



## ESPAÑA (SPAIN) : Trusted List

Tsl Id: TSL20240124

Valid until nextUpdate value: 2024-07-23T02:00:00Z

TSL signed on: 2024-01-24T10:15:21Z

## TSL Scheme Information

<b>TSL Id</b>	<i>TSL20240124</i>
<b>TSLTag</b>	<i>http://uri.etsi.org/19612/TSLTag</i>
<b>TSL Version Identifier</b>	<i>5</i>
<b>TSL Sequence Number</b>	<i>150</i>
<b>TSL Type</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric</i>

### Scheme Operator Name

<b>Name</b>	<i>[ es ]</i>	<i>MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACION DIGITAL</i>
<b>Name</b>	<i>[ en ]</i>	<i>MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION</i>

### PostalAddress

<b>Street Address</b>	<i>[ en ]</i>	<i>Poeta Joan Maragall, 41</i>
<b>Locality</b>	<i>[ en ]</i>	<i>Madrid</i>
<b>State Or Province</b>	<i>[ en ]</i>	<i>Madrid</i>
<b>Postal Code</b>	<i>[ en ]</i>	<i>28020</i>
<b>Country Name</b>	<i>[ en ]</i>	<i>ES</i>

### PostalAddress

<b>Street Address</b>	<i>[ es ]</i>	<i>Poeta Joan Maragall, 41</i>
<b>Locality</b>	<i>[ es ]</i>	<i>Madrid</i>
<b>State Or Province</b>	<i>[ es ]</i>	<i>Madrid</i>
<b>Postal Code</b>	<i>[ es ]</i>	<i>28020</i>
<b>Country Name</b>	<i>[ es ]</i>	<i>ES</i>

### ElectronicAddress

<b>URI</b>	<i>[ en ]</i>	<i>https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx</i>
<b>URI</b>	<i>[ en ]</i>	<i>mailto:sgsd@economia.gob.es</i>

### Scheme Name

**Name** [ en ] *ES:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

**Name** [ es ] *ES:Lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados que supervisa el Estado miembro de expedición, junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.*

#### Scheme Information URI

**URI** [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeinformationURI.aspx>

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeinformationURI.aspx>

**Status Determination Approach** <http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate>

#### Scheme Type Community Rules

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/ES>

**Scheme Territory** ES

#### Policy Or Legal Notice

**TSL Legal Notice** [ en ] *The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

**TSL Legal Notice** [ es ] *El marco jurídico aplicable a la presente lista de confianza es el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.*

**Historical Information Period** 65535

#### Pointer to other TSL - EUROPEAN UNION

1.EU TSL - MimeType: application/vnd.etsi.tsl+xml

**TSL Location** <https://ec.europa.eu/tools/lotl/eu-lotl.xml>

#### EU TSL digital identities

#### TSL Scheme Operator certificate fields details





Extended Key Usage

id\_kp\_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12

QCStatements - crit. = false

id\_etsi\_qcs\_QcCompliance

id\_etsi\_qcs\_QcSSCD

CRL Distribution Points

http://crl.quovadisglobal.com/qvbecag2.crl

Subject Key Identifier

2C:A6:7A:C1:D9:5A:BB:48:CF:7D:7A:0B:59:C6:CD:A3:66:FD:50:3A

Key Usage:

digitalSignature - nonRepudiation

Thumbprint algorithm:

SHA-256

Thumbprint:

F7:E8:E4:E5:54:FB:7C:7A:8F:6F:36:0E:0C:A2:F5:9D:46:6C:8F:95:39:A2:59:63:F5:ED:37:E9:05:F0:C7:97

EU TSL digital identities

TSL Scheme Operator certificate fields details

Version:

3

Serial Number:

60213747836971875367469109022676830970210644486

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHQTCCBSmgAwIBAgIU...
-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

QuoVadis Belgium Issuing CA G2

Issuer O:

QuoVadis Trustlink BVBA

Issuer 2.5.4.97:

NTRBE-0537698318

Issuer C:

BE

Subject CN:

European Commission

Subject O:

COMMISSION DE L'UNION EUROPEENNE - COMMISSIE VAN DE EUROPESE UNIE

Subject 2.5.4.97:

NTRBE-0949383342

**Subject OU:** *DG for Communications Networks, Content and Technology*

**Subject C:** *BE*

**Valid from:** *Thu Jan 21 09:48:23 CET 2021*

**Valid to:** *Sun Jan 21 09:58:00 CET 2024*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100ED0F56E73F3D2FC88D20C47F987BF504CA3B31D535B25E64F64A35FC4F4A11DFACAE  
F85BC4233601EEAE42180D89354C4A74E3E0162E0C6718FD9C7EA0C2A475F9C8CF9C9DCD7B1DC834B6420E2D16ACFB7785FAA668A3866AA6C303D24273B6FAE0D  
C7BE0581972FBE285A7A894DCE864FAA3610332797BF27DFD49538A42F902F9DE072970D7FB74EE442731C07CB0E9F0720B79BB5A7EF580400FE7E3EC7F7053EF494  
7419D67AA7C8C7E3067B42046EBF0A3DA6B4CE38BE57422AD4437469E8EC4F99714EF02821C100E4BBA96DDBB2E747B094F888EB9BF10B212376E31EA3FB9F  
BABE3AC379457E57FDB9881B4DF78FB627F837E008AC04E1E2AC6470203010001

**Authority Key Identifier** *87:C9:BC:31:97:12:7A:73:BB:7E:C0:3D:45:51:B4:01:25:95:51:AB*

**Authority Info Access**  
*http://trust.quovadisglobal.com/qvbecag2.crt*  
*http://uw.ocsp.quovadisglobal.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.8024.1.400*  
*CPS pointer: http://www.quovadisglobal.com/repository*  
*Policy OID: 0.4.0.194112.1.3*

**Extended Key Usage** *id\_kp\_clientAuth - Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_QcSSCD*

**CRL Distribution Points** *http://crl.quovadisglobal.com/qvbecag2.crl*

**Subject Key Identifier** *4A:22:89:3F:0C:59:BE:58:B9:D5:4E:F9:11:F8:5D:11:1A:C3:7F:DF*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *91:27:BC:BD:E1:58:6E:02:DB:9D:71:49:88:13:9E:A2:80:5F:21:DC:08:83:48:A7:E4:FE:62:69:89:5  
1:38:BD*

**EU TSL digital identities****TSL Scheme Operator certificate fields details**

**Version:** *3*

**Serial Number:** *15008860349683696530586013866695132338367293834*





**Issuer O:** *DigitalSign Certificadora Digital*

**Issuer C:** *PT*

**Subject CN:** *IOANNA KALOGEROPOULOU*

**Subject OU:** *RemoteQSCDManagement*

**Subject GIVEN NAME:** *IOANNA*

**Subject SURNAME:** *KALOGEROPOULOU*

**Subject E:** *ioanna.kalogeropoulou@ec.europa.eu*

**Subject OU:** *Entitlement - EC STATUTORY STAFF*

**Subject O:** *EUROPEAN COMMISSION*

**Subject 2.5.4.97:** *LEIXG-254900ZNYA1FLUQ9U393*

**Subject OU:** *Certificate Profile - Qualified Certificate - Member*

**Subject C:** *GR*

**Valid from:** *Wed Feb 22 16:36:29 CET 2023*

**Valid to:** *Sat Feb 21 16:36:29 CET 2026*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009C80E3DC4AB8118CF8E815B84FEDFDA73F8EC4F4DC42166BD1C177BE4E0F46CEBCFEFD4E1DE46949C7A8A57589D7D292218F5BAAF9F31A7CCD4196F18080F16AECDB896623773DD6D64971DC77896ADAA5A12593354FFDAFB7B3FC017C759A13A2B668270410153AEAEDCFBB53ED65F5A54AC04CBE55CSBA08FD44F10F64207EB05A229C2A4987A1A3E536166555F5480BC34AC04156C5A9412A83D35BF3C18C5CDB76B173EF78EEC6B5761B8B458221275E8F525502BEBD46EC830EB97B7C2AF843ACB55D6A4E585ED5AF6CF64B7861AA73CF976D6A55F85A1C6ABA981BA8E2B472DFB3A786501040B6E3A35820E240A02FE0723F337B0A38CC1951270250203010001

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14*

**Authority Info Access**  
*https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b*  
*https://qca-g1.digitalsign.pt/ocsp*

**Subject Alternative Name** *ioanna.kalogeropoulou@ec.europa.eu*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.25596.4.1.1*  
*CPS pointer: https://pki.digitalsign.pt*  
*Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4*  
*Policy OID: 0.4.0.194112.1.2*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl*

**Subject Key Identifier** *64:7C:64:0C:55:59:71:04:99:95:A3:42:F7:66:3B:36:9D:3A:5A:46*



**Subject O:** EUROPEAN COMMISSION

**Subject 2.5.4.97:** LEIXG-254900ZNYA1FLUQ9U393

**Subject OU:** Certificate Profile - Qualified Certificate - Member

**Subject C:** BE

**Valid from:** Fri Apr 21 17:59:43 CEST 2023

**Valid to:** Mon Apr 20 17:59:43 CEST 2026

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100E00B7B88F776FC699A960BEC1D7F4FB5FC82C6FD09761C1D088DC422F4902544A3E  
B11B7D4CF9E4C5F6C079A89FF697B224B8B707EA93D010C655A92F25E4654DE346B062239E4176A86687EDBFAEB57402E3A11E1BA9C90028EE766CFFB221253C1B84  
FE83E3736143303420CCF67BE3D004B116256A455FA8814E6D3A669127BB1ACD25DA1BDB23B12DFA998A5B328EF307EF68ED6DE42260499D7DCD0629AD829C9F6  
F7314BFFB586DF72302887FCED365738F86DF6F1D557C764D5D6965A0C1FF5048F2A3C67B0D9844BED63C69F61A7366D5D9BB1F9BCBDE5E69CF9027F66411E22B  
B5BA3D9600B8BEF41CDABB12F242784208C59AC08A1F68DAE8BB9D0203010001

**Basic Constraints** IsCA: false

**Authority Key Identifier** 73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14

**Authority Info Access**  
<https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b>  
<https://qca-g1.digitalsign.pt/ocsp>

**Subject Alternative Name** jeroen.rathe@ec.europa.eu

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.25596.4.1.1  
CPS pointer: <https://pki.digitalsign.pt>  
Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.4  
Policy OID: 0.4.0.194112.1.2

**Extended Key Usage** id\_kp\_clientAuth

**CRL Distribution Points** <https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl>

**Subject Key Identifier** 1B:EF:6E:01:67:39:13:6D:D4:3C:1B:A2:1A:C6:F2:28:2B:A9:60:B9

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_QcSSCD

**Key Usage:** nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** D3:23:8E:D2:84:DC:47:8F:86:2C:28:5B:00:5F:72:E9:BE:61:E0:76:D0:77:AE:C5:13:DA:C9:A2:BF  
:B6:93:41

EU TSL digital identities

## TSL Scheme Operator certificate fields details

**Version:** 3

Serial Number:

16575121214204686509979473323293184155782588036

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHACCBeqAwIBAgLUH0kMcmM7NMyG2SPRIC8Qs9VpoQwDOY/KoZlhveNAQENBQAwXzELMAAG... [Base64 encoded certificate data]

-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer CN:

DIGITALSIGN QUALIFIED CA GI

Issuer O:

DigitalSign Certificadora Digital

Issuer C:

PT

Subject CN:

CONSTANTIN ADRIAN CROITORU

Subject OU:

RemoteQSCDManagement

Subject GIVEN NAME:

CONSTANTIN ADRIAN

Subject SURNAME:

CROITORU

Subject E:

adrian.croitoru@ec.europa.eu

Subject OU:

Entitlement - EC STATUTORY STAFF

Subject O:

EUROPEAN COMMISSION

Subject 2.5.4.97:

LEIXG-254900ZNYAIFLUQ9U393

Subject OU:

Certificate Profile - Qualified Certificate - Member

Subject C:

RO

Valid from:

Mon Oct 02 15:29:50 CEST 2023

Valid to:

Thu Oct 01 15:29:50 CEST 2026

Public Key:

30820122304006092A86486F7D01010105004382010F003082010A02820101000C10F7DD00A2857CAA42CE8305841BC4BF93882D2F7043551AE49CD5A4434E38A2A34BD0A6FC8C3C232ECSAE2C90EA694B8623AA1339E13628ED6685CB28B6615AB84D2557A3D1B7C7C47290732ED77BF0AC2CA8309FC6B9C67DCA982446710459476F506376E913A60ACAF20487EPDA90B7F3DE16D7A3A1E9D062D82997F07944E37CCD60E9129A29316B9CA6075DD6D7262C34A57DD84332FD9A99FA45A04C96DF81F7FB6464D7B23087A87A4F842420C9237144D369E318663E469057E9489ED5E37CEDA87FA3D3DA9A89FDFD9C97AE8610A980BF1C899604DE66FA4E24845701CA874618F6A834F791726FA68F12FAA9A4BCC21175A6F37986D5CE8F790203010001

Basic Constraints

isCA: false





**Issuer CN:** DIGITALSIGN QUALIFIED CA G1

**Issuer O:** DigitalSign Certificadora Digital

**Issuer C:** PT

**Subject CN:** EUROPEAN COMMISSION

**Subject E:** digit-dmo@ec.europa.eu

**Subject O:** EUROPEAN COMMISSION

**Subject 2.5.4.97:** LEIXG-254900ZNYA1FLUQ9U393

**Subject OU:** Directorate-General for Digital Services (DIGIT)

**Subject OU:** Certificate Profile - Qualified Certificate - Organization

**Subject C:** LU

**Valid from:** Fri Nov 17 11:11:46 CET 2023

**Valid to:** Wed Nov 17 11:11:46 CET 2027

**Public Key:**  
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A5:98:78:10:3D:91:80:11:12:51:A7:1E:82:51:36:96:DB:C8:BE:06:F9:34:89:72:01:C8:F5:0B:72:5E:56:23:07:6D:F8:8:5:20:18:CN:9B:D6:FA:02:AF:A2:8C:27:82:1A:18:81:15:00:EB:63:A6:42:01:05:85:7D:F7:ES:8D:2C:07:07:F9:A5:57:A6:12:87:BD:1F:D0:23:FD:CA:53:D7:82:2A:74:1D:39:57:86:BC:F0:94:91:7D:1D:15:6B:5C:66:40:9A:C3:B0:16:56:A9:91:F1:D0:41:07:05:CB:48:17:90:63:C9:33:00:71:0C:9B:85:AF:B8:00:E2:28:B6:9D:DD:17:FE:D9:03:70:AE:E0:66:1B:37:D0:6E:43:2C:AA:7E:AA:E3:31:DB:83:CF:30:E3:57:02:82:D7:B6:84:B0:B7:AF:EB:40:BS:16:72:09:FC:55:44:75:AD:E5:25:21:A2:94:3E:49:C9:47:1E:4D:A4:5C:A2:DD:6B:C3:AR:23:2A:B3:95:87:03:FF:50:77:DE:BC:9D:C9:0A:C4:2C:B8:0C:E4:7F:B8:AF:CC:7C:DB:88:F3:CF:47:D5:2C:B1:E7:30:AF:B3:BD:E4:5A:18:C1:B3:D8:23:25:16:00:E4:E5:09:50:02:1C:63:15:5C:73:75:FF:EE:0B:1F:BE:27:76:FA:09:60:44:9C:5F:09:8D:F5:29:22:6F:78:86:E9:3A:AE:38:24:31:BC:DS:F3:1C:66:5B:F7:96:ED:0A:8A:7:56:9A:C2:9F:5E:0E:DC:25:D4:4D:93:04:2A:48:4F:B8:A5:BC:74:8E:A9:47:62:52:19:BB:53:FB:10:64:71:CD:70:61:59:54:9F:31:37:77:E6:0A:ES:24:9E:BD:44:F6:08:EC:09:33:E0:1C:8D:2A:14:69:14:C1:20:DB:03:FD:EC:C3:0E:FB:FB:BE:D6:CS:DS:77:1C:68:98:E8:08:D9:2E:AF:36:B2:4E:C3:2C:CC:60:EF:00:5D:7B:D4:B6:3A:F6:53:58:EB:22:B4:BB:3A:D2:FB:77:3F:84:41:DC:B5:76:B9:28:80:B7:3E:95:AB:04:64:39:9B:0E:F7:29:EA:D1:BE:70:21:CC:36:5E:99:5A:AE:3E:4D:43:E7:D6:89:35:F1:EB:1D:79:82:DD:54:B9:DA:B1:D6:60:EC:07:1F:ED:AA:6C:E0:DD:87:C1:A4:1F:01:D7:07:34:A9:16:2B:75:2A:0D:9B:AE:96:AF:87:3B:4D:68:69:63:E8:6B:0B:14:06:EB:F2:89:02:30:99:6:5:38:E2:D0:F1:37:F2:F5:59:E7:ES:1A:B4:FB:B5:53:75:DE:1D:03:18:3D:02:03:01:00:01

**Basic Constraints** IsCA: false

**Authority Key Identifier** 73:49:F1:40:1C:14:04:7C:9A:12:7F:FA:2F:CD:5C:67:23:18:E9:14

**Authority Info Access**  
<https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.p7b>  
<https://qca-g1.digitalsign.pt/ocsp>

**Subject Alternative Name** digit-dmo@ec.europa.eu

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.25596.4.1.1  
CPS pointer: <https://pki.digitalsign.pt>  
Policy OID: 1.3.6.1.4.1.25596.4.2.1.1.1.6  
Policy OID: 0.4.0.194112.1.3

**Extended Key Usage** id\_kp\_clientAuth

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_QcSSCD

**CRL Distribution Points** <https://qca-g1.digitalsign.pt/DIGITALSIGNQUALIFIEDCAG1.crl>

**Subject Key Identifier** 94:EE:61:C1:C9:7D:FF:AD:E2:B2:C9:B9:F6:BF:93:20:77:89:49:9C

**Key Usage:** nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** E0:A6:20:FB:B6:74:73:62:BB:93:3A:C4:41:69:D6:76:A5:53:44:47:16:CF:5F:31:60:5F:12:A2:2B:83:96:B1

**EU TSL digital identities**

**TSL Scheme Operator certificate fields details**

**Version:** 3

**Serial Number:** 21267647932559404339035760224263512027

**X509 Certificate**

```
-----BEGIN CERTIFICATE-----
MIIG7zCCBnegAwIBAgIQEAAA...
-----END CERTIFICATE-----
```

**Signature algorithm:** SHA256withRSA

**Issuer SERIAL NUMBER:** 201803

**Issuer CN:** Citizen CA

**Issuer O:** Certipost N.V./S.A.

**Issuer L:** Brussels

**Issuer C:** BE

**Subject SERIAL NUMBER:** 72020329970

**Subject GIVEN NAME:** Patrick Jean

**Subject SURNAME:** Kremer

**Subject CN:** Patrick Kremer (Signature)

**Subject C:** BE

<b>Valid from:</b>	Sat Jun 02 00:04:19 CEST 2018
<b>Valid to:</b>	Wed May 31 01:59:59 CEST 2028
<b>Public Key:</b>	30820122300D06092A864886F70D010105000382010F003082010A0282010100AFB83B56B8836386ACDD1E0B3CE83B8BF1F98A71F369530EC056FF18396FB0215307CFF5797490337332AF84B1894B83E4E8A77613E873F05951A27A7BD06BF6FA28ED90F93B65091F7B3D3272E0182D788DC764B87DC5461BD2C825A7C32600604D0B909B568354B0D0EB9DE6A91E6D00EFA011FEA5B38CD11122F7324617014ABE4BF5A8704686A4885E355005DE23D292F11EDCBBD48C5FF15C7585E1A32FA862BA9171AC79A4DC9FD8604DB71EB96D8F02212BF9E0D33CCE4C06043157C339A71853CC45ECF738D93F8C82A185AF13CA50D27C8FC5F7383B74754DE3BC910A3C87D4262C413DE8713093305B14E315B36EFC22BB849F2A4F63B54B8550203010001
<b>Authority Key Identifier</b>	D9:34:21:3E:3A:42:25:6D:E1:BB:BF:BE:47:4C:F8:02:AD:E3:2F:54
<b>Authority Info Access</b>	<a href="http://certs.eid.belgium.be/citizen201803.crt">http://certs.eid.belgium.be/citizen201803.crt</a> <a href="http://ocsp.eid.belgium.be/2">http://ocsp.eid.belgium.be/2</a>
<b>Certificate Policies</b>	Policy OID: 2.16.56.12.1.1.2.1 CPS pointer: <a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a> CPS text: [Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage soumis à des limitations de responsabilité, voir CPS - Verwendung unterliegt Haftungsbeschränkungen, gemäss CPS] Policy OID: 0.4.0.194112.1.2
<b>CRL Distribution Points</b>	<a href="http://crl.eid.belgium.be/eidc201803.crl">http://crl.eid.belgium.be/eidc201803.crl</a>
<b>Extended Key Usage</b>	id_kp_emailProtection
<b>QCStatements - crit. = false</b>	id_etsi_qcs_QcCompliance id_etsi_qcs_QcSSCD
<b>Key Usage:</b>	nonRepudiation
<b>Thumbprint algorithm:</b>	SHA-256
<b>Thumbprint:</b>	D2:06:4F:DD:70:F6:98:2D:CC:51:6B:86:D9:D5:C5:6A:EA:93:94:17:C6:24:B2:E4:78:C0:B2:9D:E5:4F:84:74
<b>TSL Type</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists">http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists</a>
<b>Scheme Territory</b>	EU
<b>Mime Type</b>	application/vnd.etsi.tsl+xml
<b>Scheme Operator Name</b>	
<b>Name</b>	[ en ] European Commission
<b>Scheme Type Community Rules</b>	
<b>URI</b>	[ en ] <a href="http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists</a>
<b>List Issue Date Time</b>	2024-01-24T02:00:00Z
<b>Next Update</b>	

**date Time**

*2024-07-23T02:00:00Z*

**Distribution Points**

**URI**

*<https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.xml>*

**URI**

*<https://sedediatid.mineco.gob.es/Prestadores/TSL/TSL.pdf>*

**1 - TSP: Banco Santander, S.A.****TSP Name**

**Name** [ en ] *Banco Santander, S.A.*

**Name** [ es ] *Banco Santander, S.A.*

**TSP Trade Name**

**Name** [ en ] *VATES-A39000013*

**Name** [ en ] *Santander*

**Name** [ es ] *Santander*

**Name** [ en ] *Banco Santander Central Hispano, S.A. CIF: A-39000013*

**Name** [ en ] *Banco Santander S.A. CIF: A-39000013*

**PostalAddress**

**Street Address** [ es ] *Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*

**Locality** [ es ] *Boadilla del Monte*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28660*

**Country Name** [ es ] *ES*

**PostalAddress**

**Street Address** [ en ] *Ciudad Grupo Santander. Avd. de Cantabria s/n, edificio Pampa, planta 1*

**Locality** [ en ] *Boadilla del Monte*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28660*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://www.gruposantander.es*

**URI** [ en ] *mailto:certificacion.universitaria@gruposantander.com*



**Subject OU:** *Direccion de Universidades*

**Subject O:** *Banco Santander Central Hispano, S.A. CIF: A-39000013*

**Subject L:** *Paseo de Pereda, 9-12*

**Subject ST:** *Santander - Spain*

**Valid from:** *Thu Nov 24 01:00:00 CET 2005*

**Valid to:** *Tue Nov 24 00:59:59 CET 2015*

**Public Key:**  
30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81 89 02 81 81 00 B4 DF D8 3E 76 FD FC 94 D3 BD 44 2D 2C 98 E0 19 AF 2E 9E EE 8E 19 3D 98 85 CD F4 13 CD 90 84 4B 8A 78 C0 3B 55 8 C 50 B8 28 97 25 9F AE AF 23 B9 26 09 43 31 EC 51 38 7E 89 9F A8 AB 8D 45 41 AB DB C9 06 77 1A C1 F3 6D 59 8E E9 4B 6A CE 16 19 46 E5 FB 6A F7 1D 3B FC AE 07 10 11 DA 81 77 D1 D0 F2 8C 09 11 D5 0 3 8A 1B 64 65 AE 95 9D FA 07 FC 16 42 3C A0 2A F3 97 2B 53 83 03 BB 7D 37 99 02 03 01 00 01

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Alternative Name** *CN=Private1-33*

**Subject Key Identifier** *20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*

**Authority Key Identifier** *20:FF:D6:D5:6F:19:BE:E1:34:B3:0A:66:6A:B6:4F:9F:77:11:07:6E*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *1C:F1:AE:29:72:6D:13:08:73:8F:07:B6:80:8A:89:AB:29:C5:CC:BF:F8:C4:19:D3:5C:71:D9:68:AE:3D:1B:D1*

**X509SubjectName**

**Subject CN:** *WG10 Qualified Identification Root CA*

**Subject OU:** *Direccion de Universidades*

**Subject O:** *Banco Santander Central Hispano, S.A. CIF: A-39000013*

**Subject L:** *Paseo de Pereda, 9-12*

**Subject ST:** *Santander - Spain*

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

**1.1.1 - Extension (critical): additionalServiceInformation**



**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**1.1.2 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA*

**Name** [ en ] *Qualified Certificates issued by CA WG10 Qualified Identification Root CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *WG10 Qualified Identification Root CA*

**Subject OU:** *Direccion de Universidades*

**Subject O:** *Banco Santander Central Hispano, S.A. CIF: A-39000013*

**Subject L:** *Paseo de Pereda, 9-12*

**Subject ST:** *Santander - Spain*

**X509SKI**

**X509 SK I** *IP/W1W8ZvuE0swpmarZPn3cRB24=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2015-11-24T01:00:00Z*

**1.1.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Reconocidos emitidos por CA WG10 Qualified Identification Root CA*

**Name** [ en ] *Qualified Certificates issued by CA WG10 Qualified Identification Root CA*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *WG10 Qualified Identification Root CA*

**Subject OU:** *Direccion de Universidades*

**Subject O:** *Banco Santander Central Hispano, S.A. CIF: A-39000013*

**Subject L:** *Paseo de Pereda, 9-12*

**Subject ST:** *Santander - Spain*

**X509SKI**

**X509 SK I** *IP/W1W8ZvuE0swpmarZPn3cRB24=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2009-04-13T00:00:00Z*

**1.2 - Service (withdrawn): Santander Digital Signature**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[en]* *Santander Digital Signature*

**Name** *[es]* *Santander Digital Signature*

**Service digital identities****Certificate fields details**

**Version:** *3*

**Serial Number:** *4828055370659501092*



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *CB:C6:89:C8:7A:63:FA:73:23:A7:60:7C:C7:C4:57:B3:B4:50:57:2B:EF:A4:74:70:B6:1C:35:BF:07:9B:60:0B*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2018-10-22T00:00:00Z*

### Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

#### 1.2.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

##### Policy Identifier:

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

##### Policy Identifier:

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

#### 1.2.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 1.2.3 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Santander Digital Signature*

**Name** *[ es ]* *Santander Digital Signature*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *Santander Digital Signature*

**Subject OU:** *Dirección de Universidades*

**Subject O:** *Banco Santander S.A. CIF: A-39000013*

**Subject L:** *Paseo de Pereda 9-12*

**Subject ST:** *Santander*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *S4y6oi6+9bMkvmbUTUiOvV3/v60=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**1.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

**1.2.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	--------	---

**1.2.4 - History instance n.2 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ en ]	<i>Santander Digital Signature</i>
-------------	--------	------------------------------------

<b>Name</b>	[ es ]	<i>Santander Digital Signature</i>
-------------	--------	------------------------------------

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>Santander Digital Signature</i>
<b>Subject OU:</b>	<i>Dirección de Universidades</i>
<b>Subject O:</b>	<i>Banco Santander S.A. CIF: A-39000013</i>
<b>Subject L:</b>	<i>Paseo de Pereda 9-12</i>
<b>Subject ST:</b>	<i>Santander</i>
<b>Subject C:</b>	<i>ES</i>

**X509SKI**

<b>X509 SK I</b>	<i>S4y6oi6+9bMkvmbUTUiOvV3/v60=</i>
------------------	-------------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>
-----------------------	---

<b>Status Starting Time</b>	<i>2016-01-24T23:00:00Z</i>
-----------------------------	-----------------------------

**1.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[ en ]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
-----------------------------------	--------	---

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdt" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.5.1

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.21.1

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.21.2

## 2 - TSP: Dirección General de la Policía

### TSP Name

**Name** [ en ] *Dirección General de la Policía*

**Name** [ es ] *Dirección General de la Policía*

### TSP Trade Name

**Name** [ en ] *VATES-S2816015H*

**Name** [ en ] *Dirección General de la Policía*

**Name** [ es ] *Dirección General de la Policía*

**Name** [ en ] *DIRECCION GENERAL DE LA POLICIA*

### PostalAddress

**Street Address** [ es ] *C/Miguel Ángel nº 5*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28010*

**Country Name** [ es ] *ES*

### PostalAddress

**Street Address** [ en ] *C/Miguel Ángel nº 5*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28010*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *http://www.dnielectronico.es*

**URI** [ en ] *mailto:dnielectronico@dnielectronico.es*

### TSP Information URI



URI	[ en ]	<a href="http://www.dnielectronico.es/PDFs/practice_statement_certification_policy.pdf">http://www.dnielectronico.es/PDFs/practice_statement_certification_policy.pdf</a>
URI	[ es ]	<a href="http://www.dnielectronico.es">http://www.dnielectronico.es</a>

## 2.1 - Service (withdrawn): Qualified Certificates issued by subordinated CA under the root CA

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service type description</b>	[ en ]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[ es ]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
<b>Service Name</b>		
<b>Name</b>	[ en ]	Qualified Certificates issued by subordinated CA under the root CA
<b>Name</b>	[ es ]	Certificados Reconocidos emitido por CAs subordinadas de la CA Root
<b>Service digital identities</b>		
<b>Certificate fields details</b>		
<b>Version:</b>	3	
<b>Serial Number:</b>	1093088852834654238833120296104474059	
<b>X509 Certificate</b>	<pre> -----BEGIN CERTIFICATE----- MIIFvzCAgeAwIBAgIQANKFcp2ap9ZIEYOVsjGlyzANBgkqhkiG9w0BAQUFAADBMQswCQYDVQQG EwJFZlUzEoMCYGA1UECgwRREISRUINDSL90EdDFkVSQWwgREUgTEgUe9MSUNJQENMAsGAIUECwwE RESjRETElMBMGAIUEFAwwMQUMeIuFjWIBETlFMBAYTAZMlOxNiEwNzYyMDZMDSw0ODYnTEI OvowXTElMAKGA1UEBBMCRVMAkDAmBGNVBAOMH0RlUKVDO0P1tBHRU5FUkFMERFIExBIFBTEID SUEdIALBgNVBAsMBEROSUUAFTATBgNVBAMMDEFEFDFjBSVogREjRTRCCAIwDQYJKoZIhvcNAQEB BQADggPAPCCAgCggIBAAAOzDovAHe2p9Z5gscq1AqAXNEBfaimuV+KcRmwe3qNPeK3W BU2EgXXHAz0JfWQ5ayJkgOgNMSAH87HrKE4esBmVCT8UswwKvLDxKESdr/BwL-CZywaHoT QMxvBwIBwgkSbrzCU40ZILexpLrEIsRROMNXY+LwAgc9NkwNLEBm7uME7Ept5pvrNB2 J4bn2nyTqRWScCMARExtHIVFKScY2dN+em99YCaQ59g20jijdGVGT999wOIdSLR0DE bHE0dNw56upPRG1WNYCJsk+syplHVBMkpv+mtInzEVfbcuJaIS487XOAU58Boj9ZZzmlv cJONLNG8BBLSPVP1+ACy849Bx4FDLzZcS8U8mbRvmdM/NZgAbBvm9LopKqR2HXr68UinWwS 95+XSDNjpr+ss8S7BwWemGIMBTANISeGWK75+Av99QHfKksczZWO04Qm0dscclUulgm LQeG+r+TLU/C9pSylw8UGAZLgNO+qWkoVYgLDNTs3CEvqu/Wi6j9VGSyprBbz0ZLvgQ uML+UklZmB04NwVaTRev6Asux7fM34Ny1vPw+DwS+Yem3Rj9nCjB4WdlDIWIEFv2zycWjCC Zk7QmkiTlpaDUsh3+AmBAAGcB5MAKGA1UdEwEwQMAAMBAIwDgYDVRlRAGIIBAQDAgEG MB0GA1UdDgQWBBSORSISX8Lxsf2wFHYB8DuoG3ujA3BgNVHSAEMDAuMCAwBGFUdIAAwDAiBger BGEFBQCARyWafHR0cDovL3d5b5kmlImVzL2RwYzANBgkqhkiG9w0BAQUFAAOCAgEAdcVzyVFR L4Zolp42Nq80R6jIatxYBm8SoCML1za1zpeJTuOmESpmgmLz33jIhSUQvg704 Q+9xao5B8VQHzLmkG8fj9mtK07alyXu5aaGvix2XoE81SZLhmWfYBnORC3s8VUJQWua5 ov+4gGfM3ZP76ZUJfOPc3zg36KJDavngLUclUfI202HqmK8XuvgeFR8958KwVWAXIMryEWBw Unk0mBIBM07Qc2vRR808dIB4TaqFpaXUErRdyJclowIyAm68b0XapT7gFvdeWShhZ xNdlgOymC2ec7WSNOtBRHS9h1V7ESDqQRKQmkbMTupwVzaDpGG4z+7dWuWgZzE7wg/03 8d4cRxxwOTw8Rz6omB1koppM91QTCagcv1WwmZy691jBdcTXV3OhBgXkHf58W9duR z4gFYk6Wlq4OMEX6NMY4k1x3kRbafJz+7Gak7E8SCYOMMMj+18ok3DZPq9+BrDw3 vk661JefqGvH8G6kMID95c7qM5aGBvUY2Y96fXoScP9a9NHTCbn7UhuJR5ANhENqY Mahy34Hp9C3BU0W82F1mwUa5jFkqEqdY35K6zKa8ub6nTH0Fuled1sc3ZofAat= -----END CERTIFICATE----- </pre>	
<b>Signature algorithm:</b>	SHA1withRSA	
<b>Issuer CN:</b>	AC RAIZ DNIE	
<b>Issuer OU:</b>	DNIE	
<b>Issuer O:</b>	DIRECCION GENERAL DE LA POLICIA	
<b>Issuer C:</b>	ES	
<b>Subject CN:</b>	AC RAIZ DNIE	
<b>Subject OU:</b>	DNIE	

Subject O: DIRECCION GENERAL DE LA POLICIA
Subject C: ES

Valid from: Thu Feb 16 11:37:25 CET 2006

Valid to: Fri Feb 08 23:59:59 CET 2036

Public Key: 30820222300D06092A864886F70D01010105000382020F003082020A0282020100800AD0C3A32007A363FF7F34A0CDDE6A5408175D8B10115A7E6B95F8A71FF0CC21D...

Basic Constraints: IsCA: true

Subject Key Identifier: 8E:45:F4:F9:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA

Certificate Policies: Policy OID: 2.5.29.32.0
CPS pointer: http://www.dnie.es/dpc

Key Usage: keyCertSign - cRLSign

Thumbprint algorithm: SHA-256

Thumbprint: 73:97:10:C5:24:5E:33:EC:8A:24:3A:1B:20:04:8F:C9:D5:F4:52:85:99:21:38:45:C1:64:D0:04:B8:B6:67:F9

Certificate fields details

Version: 3

Serial Number: 1023669171620362353858443562596147092

X509 Certificate: -----BEGIN CERTIFICATE-----
MIHvCA6egAwIAGIQAUMyW4QOJDTc1=2eIDANBqkhhkG9w0BAQSFADBDAMQswCOYDVQOQ
EwFjZ2EmYyGAIUEGwIREISRUdSU9eHedF7A5QIwREUjEteglE9MSUNQJENMAsGAUUECwE
RESJRTEVMBMGAIUEAwW4QUMgUkFJWIBETLHfMBADTA2MDhNjEwKzEzNjM2MDw0ODYNTk1
OwovXTElMAkGA1UEBmCRVMkdDAmBqNVBAOMH0RUKVVDQ0PTBHRUSUkFMiERFExBIBTTEID
SUEwDTALBgNVBAsMBEROSU1AF7A1BgNVBAMMDEFDfEBSogRESURTCcAhhDOYVkoZmwenAQEB
BQADegIPADCCAgcCzGfBAIAAqOzDovAho2P9zSgzeSVAgXxEBfAlmV+KcI8Mwh3qVpK3W
BU2EgXXHAJdUfWQA5yJkgOgNm8H877HKE4esBmVCT8UswwKvLDaKsdrBwL+CNZvwaHoT
OMX4BwBwng5wzTU4OZLZyL4EaR0MXXY+1w4gc9KwNwLLbM7uME7ep5vynB2
U4bn12ny1qRWSzGMARpxHIVFKISv2dN+ev49YCd058e20j1dGVfO59wOibgSLKQDE
bHE0Nvs5gmpRGIWNYCJnk+ypHVBM0Apvr+mfIzEVIbpaJaI87X0AU58B0YZZzmIv
c9ONEgSBSLSPV+hc489BkF4DEZzS5hmRwmdN/Zg4h5m9LwPpkqg2HIXw8LwWwS
93+X5DNjpr++zss38S7BwWcnGBM6TANIISegWK75+Av9qOHFkDkenc4Z0W4QM0hccMUlqfm
LQEG+rTLUjC9zP5ylw8UGAZLjgNO+qWkOVyglNDT53CEquW1169V9GSEYpgeBbzQZLVgQ
mIL+KULzmb04NwVtRw64ssu7fIMNv1vPe-DW5Yem3Rf9mC94WdJWIEH7k2ziwYcc
Zb7Qmki11poDXUxh3AgMBAAGcZBMA8GA1UdEwEBwQFMAMBAI8wDgYDVR0PAQHBAQADAgEG
MB0GA1UdDgQWBBSORISicXVLSxf2wFHYBsdnG3ujA3BrNVHSAEMDAuMwGBlfIdA.AwJdAibeggr
BgfE9KCAKYWalR0DovL5435y5kml11mVzL2wZ2ANBqkhhkG9w0BAQSFADBDAMQswCOYDVQOQ
Nbh1HhYEm8Wbd8NmP4UowmsjL7400DRHuRSS48Yak7kzIGFVz1AqMSCWjcw30+G30x7
bSkTzEGwngzU9aDITW66v5L0xjMwYhLOVR19hCqD9gus3cqlJNXLK0h0YR44YjP
xGW5smk3K8Xxh8P4U7bK0Vd8SloqYwzawjP9089jP900XTReEEBETyWbANA
4k1MfNKdwrVwsN418688a8EKMQ29cgHyCB4VzLfiQhVLeVQ8Ntk0zcoz1Xo2zzYy6J
DgaQZRzk6rVniSN9NalWTLAK8BzOMYh+BYFVYeXU8Wz7Lp4H78kV5E1dNvzmKB
P5m9vHS146L6U5K3S1glF79KzmbWk0ur4y10V02Y6zpp7wDR4Lr16oJLqF098F
jFQ45Nj7VAM0AsbSscpVembs58R7m3yr0BjMg0VDMQM2hFYb9aRUV0Q8L0qVFKSVodNYxh
FWT+svvMuxk520FChaLAbHuE9qhaOrYnctTW0hK29dG1HhVGR28ZEO9cccVKEvyYfoe+Q
Bx3200AGmMhFNtE30kOrua26ZQz5yKZL45hMDN4MvTNSQzB5XIII4H4vjR9Q=
-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer CN: AC RAIZ DNE

Issuer OU: DNE

Issuer O: DIRECCION GENERAL DE LA POLICIA

Issuer C: ES

**Subject CN:** AC RAIZ DNIE

**Subject OU:** DNIE

**Subject O:** DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**Valid from:** Thu Feb 16 11:37:25 CET 2006

**Valid to:** Fri Feb 08 23:59:59 CET 2036

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201008000AD0C3A32007A363FF7734A0CDDEE6A5408175DB10115A7E6B95F8A71FF0CC21D  
EA37F3DE937FD6054D84B2D5D71C0CF4C49170400E5A8C898A480E80D33C007F3B7F5AC1387AC0665424FC52CC702A2F2C3C4A12C76BF1C0BF82F19B  
F0687A1340C897BC1C2507080AB796EFCC2954E0E6652DEA B22E2B10969124E30D5D8F8BC00802F4D930FCD2E571B33BB9F304E C4A5CB79A7FB E23418B6209E1B9F5D A7C93A AD  
4564B318CE11129C6D1E554528849C57674DF9CB E28B8F5849D439FFC836D238E20C657F150E7DC107DDA922DF9100C46C713474DC39EA EA4F44697F58DB580A5271  
2BEC491D507433F9298AFAFE99F4E7CC45456DCA5A25A212E3CE D7380539F01A09F57659CE626F7A340D2C D1BC0412FC3D53C8FAD002CBCE3D21B5C5E03933A5C  
F3933C99B46F99D33F359800841BE6F4BA0FA4ACEA4761C85E2AF AF149D65AC F77F97E43349A6AFBECE2B37F12E C175059C9C604C9D300D97549E8162BBE7E02F7  
140714A97791E9DC91958ED3889033476F71C31469FAA62D011E1B EA D32E27F0BDCFE E722F0F141A30192E580D3BEA962A855880B3434ECDC2115AAEF D6225E89F  
53192132A6F8016D9B10D D92E F810B8CFE3245339C1D387C DC15693473BF A02CBB117B94CD F8372D6F3DEF835AC61E9B74498FD9C28D BE167650C83A D12516F6F6  
CC8C9C5A309E65BE D09A4893D7FA680D753187F9F70203010001

**Basic Constraints** IsCA: true

**Subject Key Identifier** 8E:45:F4:9F:73:C5:FF:2F:1B:05:DB:01:47:60:1B:03:8A:81:B7:BA

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.dnie.es/dpc>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** F5:79:21:10:81:7A:86:D4:FE:24:4A:C2:A8:B1:0B:5B:0B:F4:CE:86:26:66:1A:B9:84:47:0A:87:87:98:30:F5

**X509SubjectName**

**Subject CN:** AC RAIZ DNIE

**Subject OU:** DNIE

**Subject O:** DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2023-09-14T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt>

**URI** [es] <https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt>

URI	[ en ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt">https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt</a>
URI	[ es ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt">https://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.crt</a>
URI	[ en ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt">https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt</a>
URI	[ es ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt">https://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.crt</a>
URI	[ en ]	<a href="http://www.dnielectronico.es/PDFs/Políticas_de_Certificación_v2.1.pdf">http://www.dnielectronico.es/PDFs/Políticas_de_Certificación_v2.1.pdf</a>
URI	[ es ]	<a href="http://www.dnielectronico.es/PDFs/Políticas_de_Certificación_v2.1.pdf">http://www.dnielectronico.es/PDFs/Políticas_de_Certificación_v2.1.pdf</a>
URI	[ en ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt</a>
URI	[ es ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.crt</a>
URI	[ en ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt</a>
URI	[ es ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.crt</a>
URI	[ en ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt</a>
URI	[ es ]	<a href="https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt">https://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.crt</a>

### 2.1.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</a>
-----	--------	---

### 2.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

### 2.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:2.16.724.1.2.2.2.11
------------	-------------	-----------------------------

**Description****2.1.4 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by subordinated CA under the root CA*

**Name** *[ es ]* *Certificados Reconocidos emitido por CAs subordinadas de la CA Root*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC RAIZ DNIE*

**Subject OU:** *DNIE*

**Subject O:** *DIRECCION GENERAL DE LA POLICIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jkX0n3PF/y8bBdsBR2AbA4qBt7o=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**2.1.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

**2.1.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**2.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

### Criteria list assert=atLeastOne

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.1.2.2.2.11

#### Description

### 2.1.5 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Qualified Certificates issued by subordinated CA under the root CA

Name [es] Certificados Reconocidos emitido por CAs subordinadas de la CA Root

#### Service digital identities

##### X509SubjectName

Subject CN: AC RAIZ DNIE

Subject OU: DNIE

Subject O: DIRECCION GENERAL DE LA POLICIA

Subject C: ES

##### X509SKI

X509 SK I [jkX0n3PF/y8bBdsBR2AbA4qBt7o=](http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision)

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2006-12-11T00:00:00Z

### 2.1.5.4 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

## 2.2 - Service (withdrawn): Qualified Certificates issued by subordinated CA under the root CA for Public Administration

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.
<b>Service Name</b>		
<b>Name</b>	[en]	Qualified Certificates issued by subordinated CA under the root CA for Public Administration
<b>Name</b>	[es]	Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP
<b>Service digital identities</b>		
<b>Certificate fields details</b>		
<b>Version:</b>		3
<b>Serial Number:</b>		977112935391749175446100766159303134
<b>X509 Certificate</b>		<pre>-----BEGIN CERTIFICATE----- MIIFVjCCA6gAwIBAgIQALwvYs201YN6UsQ0i3Bx3jANBgkqhkiG9w0BAQUFADBBMQswCOYDVQ0G EwJFEzEwMCYGA1UECgwREISRUUNDSt90LEdfTRVSOwRREUgTEEgglE9MSUNJQTEEMMoGA1UECwwD Q005MR0wEgYDQ0QDABQyBSOUJERHJDAcfw0wNzAxMjA1MDEhbnV0eG5kaW50eG5kaW50eG5kaW50 MFEsCzAJBgNVBAYTAkVTMSEwJgYDVOQ0DB9ESVJFQ0NjOT04R0R0R0R0R0R0R0R0R0R0R0R0R0R0 MQwwcyYDVQQLDANDTJlaxFDASBgNVBAMMCOFDFjBSVogREaQMHCjANBgkqhkiG9w0BAQEFAAOCC AgAMIRkCgKCAgEAgEBD116eMxvoulDh069jgPmmDMF+Pyy0hAOuyaw677KwBjpmMqO qf6ae3Y83up7YF89jU02EeEeQOE+QI-B-L-X--oGLPbU5g0W1efcnXC4jznp7L2aeFAI 80As11UqmHfC7kRLN6yZZHMH4hpi5sgscxUQXw--XAZyuarbfO99TsdphXN4wQwHNlc nfTCMfesh7agG1wRUy2EYihTEGYAK2mpHIEeSpjz2WeezgWU1ha1f0180z8590hKND8s x6LVPPmst8uM1M66BRw+2scMgZmbND0HZqEAL8DNj1TzXyaz7R-X-ku59RYLwEmRQLK xyYZefbuOl5n7Uz9KANC7buCymA0+ZAE9Slz8kA6HVO+McpUBYNocJOSFXjatscOqrQ +K--gOmTubal8t7EKGs3cmkimsOHAKFO8jTfJAmzWwKj6O7BBIjpl0U4d42B4y1Nng ZW08CuBkqyl80Dx+6zaGs1o7UblNdeA4eXArJoAMUgHb77qap454WlH0ASV3qplwswuulZzWC 1cc2AWwAg6M2uchN8PWm0kXvku2h756ckwR7y22517gB9MNv7hszBMOwUwQuei3Uco IgcFz2TWC8tdXNKCAeEAAN-MHwDwYDR0TAQHBAUwAwEBZAZ0BzVH0SBAIEBAMCAQYwHQYD VR00BBYEF6cedGILokzQIjPmvtFKW9yYaOMD0GAIUdIAQzMDewLwYEVROgADANMCUGCCSGAQUF BwIBFblodIRwOs8vd3d3LnBv6GjaWEuzXmvZBjMA0GCSqS3bDQEBBQUAA4ICAQBslw3pwCj 21CceLY7Y0mINjFpTNPfNdusSsmgQjwppXCEP6MkCecUO9yXazNj1uM1VAx++997 5d7PB9+Xnu7EHR+e+54obkqplBoV9f6p9b0kO3Y8Tg9EGLM8abcUEivPIL2mQ7k78z28gp ytcZR08Jd5m+AeYPHUDefzZlnH7SlnP3Bp8mNfBnNknCYW6N8Ajo3RgqcmIbs+YgCz YVD1Q0IBRCuo3U+QFSQ79zVpTCFKBYXXKjZSokz31anY0PnaUuM8SNWwWZ5W BPqIXWkZ+deApsZXLFMSTJfclqZUOC1wRkXkdW0w4566YWhYH0w+hwK9dD6NESMA3D7 N0PCTC0x9Qs3848RjV4H+ZfmTdyTYLgkNkeB+SXVc9Lg+Twy85VyezZMSZ3PmpNzaQ xVZ9XC8SR6e+w4p91eAO8Bj1ZHY7H9ePnmasJTA6WkY0e6BMS1Gdwe+5uF1Zd9+NvOW dw+bZG6va7098EdpGWoLvyvofHFN2q1Nrtu7whKp+VsV0hZMrSpw9C-Es4yLhas5RRIvnlX 1cqwT694KID0ZlggQCbQDEdQrvCphdHdxFQ5NBz2HkhaSh8gsDd0pH451rB45Jg== -----END CERTIFICATE-----</pre>
<b>Signature algorithm:</b>		SHA1withRSA
<b>Issuer CN:</b>		AC RAIZ DGP
<b>Issuer OU:</b>		CNP
<b>Issuer O:</b>		DIRECCION GENERAL DE LA POLICIA
<b>Issuer C:</b>		ES
<b>Subject CN:</b>		AC RAIZ DGP
<b>Subject OU:</b>		CNP
<b>Subject O:</b>		DIRECCION GENERAL DE LA POLICIA
<b>Subject C:</b>		ES

Valid from: Thu Jan 25 13:05:08 CET 2007

Valid to: Sun Jan 25 13:05:08 CET 2037

Public Key: 30820222300D06092A864886F70D01010105000382020F003082020A02820201008010F5B75E... (Base64 encoded public key)

Basic Constraints: IsCA: true

Subject Key Identifier: 0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E

Certificate Policies: Policy OID: 2.5.29.32.0
CPS pointer: http://www.policia.es/dpc

Key Usage: keyCertSign - cRLSign

Thumbprint algorithm: SHA-256

Thumbprint: 97:E9:F2:C6:2C:95:F1:F0:FF:B0:A6:DF:29:C4:E7:64:7E:C9:06:FB:62:D3:62:26:FD:81:1D:41:22:74:6C:89

Certificate fields details

Version: 3

Serial Number: 1009759735754786940203842089657449054

X509 Certificate: -----BEGIN CERTIFICATE-----
MIHFiC... (Base64 encoded X.509 certificate)

Signature algorithm: SHA256withRSA

Issuer CN: AC RAIZ DGP

Issuer OU: CNP

Issuer O: DIRECCION GENERAL DE LA POLICIA

Issuer C: ES

Subject CN: AC RAIZ DGP

Subject OU: CNP



**Subject O:** *DIRECCION GENERAL DE LA POLICIA*

**Subject C:** *ES*

**Valid from:** *Thu Jan 25 13:05:08 CET 2007*

**Valid to:** *Sun Jan 25 13:05:08 CET 2037*

**Public Key:**  
3082022230D06092A864886F70D01010105000382020F003082020A02820201008010F5B75E309C6FA31B880E5CADAE97E0CCF9A67C9305BCFC88F400EC63CB1BB  
A7FBEC4FED855F931AB50AA319A7B7623F37BA9BFB605CA0ABF8D4D3611E1087904947FE409F81F8B5FEA062CF6D4E60F5B57857275C2ED98368A93FB2F6A9C  
11F035F3402C4F552A9874DCFE4448DCDEB22596621E43388698DFE8F82C0B1510B57C3E5C0658B5A45B8C53BAF6DA2D75BA5B5CDE1FBC4301CD95E9C5D46331B  
2287BB60194C11988D8455F87B10662F5EDDA6B691E2108792A75B36581C73822594D48B9F883A35F289598FCE7D0790D043D2C7A2D53CFB7FE20DB8CD4CE9A  
051C1CEFE8E5C320666232343387664A84C4BF03354893CD7633AA8E6D1FD7FA49E9E5160BC081267D140B90AC7282565E15B88E2599F853DE7F8035C4DB52E0B2980  
D3E640F44AA5AF3F2403A7C7574F9F31E3D40589E872224EE5F137FE3C6D49C3AAAD0B7E2BE8069B84E6E6DA941A0BEC4086CECD298AB67BB2387F8A14EFCABBB  
D45C619F75AA94A80EEDD054869D08FFB76BE11D9B178AF2D4D9EA65639B0AE05F2AAC88F340F1FBAACDA1A4E8ED404B35D700E2C5C0AC9A00314A876FFEFA  
EAB88E5D89221400E55DEA249C28C30B93759C02D8E736016C90EA031FDAE721349B0F596990AE45EF921B86AC8E99C2B0811E72DB6E75EEAFCT1F4C371EC89E  
C65B31B39653042E7A2DD4728220088B364D609B8711C090203010001

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *0E:9C:76:E1:A2:2E:89:33:41:F2:E3:3E:6C:5B:16:45:BD:BD:86:8E*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://www.policia.es/dpc>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *1F:30:4D:5D:DA:90:47:60:C4:B8:D6:2F:14:F5:19:62:A7:06:CD:C0:2C:5B:70:F1:50:33:A0:4F:CD:36:45:B8*

**X509SubjectName**

**Subject CN:** *AC RAIZ DGP*

**Subject OU:** *CNP*

**Subject O:** *DIRECCION GENERAL DE LA POLICIA*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-06-29T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] <http://www.policia.es/DPC/dpc.pdf>*

**URI** *[es] <http://www.policia.es/DPC/dpc.pdf>*

**URI** *[en] <https://avancedigital.mineco.gob.es/en-Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

URI	[ es ]	<a href="https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>
URI	[ en ]	<a href="https://www.policia.es/certs/AC_DGP_001-SHA1.crt">https://www.policia.es/certs/AC_DGP_001-SHA1.crt</a>
URI	[ es ]	<a href="https://www.policia.es/certs/AC_DGP_001-SHA1.crt">https://www.policia.es/certs/AC_DGP_001-SHA1.crt</a>
URI	[ en ]	<a href="https://www.policia.es/certs/AC_DGP_001-SHA2.cer">https://www.policia.es/certs/AC_DGP_001-SHA2.cer</a>
URI	[ es ]	<a href="https://www.policia.es/certs/AC_DGP_001-SHA2.cer">https://www.policia.es/certs/AC_DGP_001-SHA2.cer</a>
URI	[ en ]	<a href="https://www.policia.es/certs/AC_DGP_002-SHA1.crt">https://www.policia.es/certs/AC_DGP_002-SHA1.crt</a>
URI	[ es ]	<a href="https://www.policia.es/certs/AC_DGP_002-SHA1.crt">https://www.policia.es/certs/AC_DGP_002-SHA1.crt</a>
URI	[ en ]	<a href="https://www.policia.es/certs/AC_DGP_002-SHA2.cer">https://www.policia.es/certs/AC_DGP_002-SHA2.cer</a>
URI	[ es ]	<a href="https://www.policia.es/certs/AC_DGP_002-SHA2.cer">https://www.policia.es/certs/AC_DGP_002-SHA2.cer</a>

#### 2.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</a>
-----	--------	---

#### 2.2.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

#### 2.2.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

#### 2.2.4 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
-----	--------	---

#### 2.2.5 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by subordinated CA under the root CA for Public Administration*

**Name** [ es ] *Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *AC RAIZ DGP*

**Subject OU:** *CNP*

**Subject O:** *DIRECCION GENERAL DE LA POLICIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Dpx24aluiTNB8uM+bFsWRb29ho4=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2018-07-16T00:00:00Z*

**2.2.5.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

**2.2.5.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**2.2.5.3 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**2.2.5.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
-----	--------	---

**2.2.6 - History instance n.2 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
-------------------------	---

**Service Name**

Name	[ en ]	Qualified Certificates issued by subordinated CA under the root CA for Public Administration
------	--------	--

Name	[ es ]	Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP
------	--------	--

**Service digital identities****X509SubjectName**

Subject CN:	AC RAIZ DGP
-------------	-------------

Subject OU:	CNP
-------------	-----

Subject O:	DIRECCION GENERAL DE LA POLICIA
------------	---------------------------------

Subject C:	ES
------------	----

**X509SKI**

X509 SK I	Dpx24aIuiTNB8uM+bFsWRb29ho4=
-----------	------------------------------

Service Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
----------------	---

Status Starting Time	2016-06-30T22:00:00Z
----------------------	----------------------

**2.2.6.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</a>
-----	--------	---

**2.2.6.6 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[ en ]	undefined.
----------------------------	--------	------------

	[ es ]	undefined.
--	--------	------------

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.1.2.1.102.36

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.1.2.1.102.37

**2.2.6.7 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**2.2.7 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by subordinated CA under the root CA for Public Administration*

**Name** [ es ] *Certificados Reconocidos emitidos por CAs subordinadas de la CA Root para AAPP*

**Service digital identities****X509SubjectName**

**Subject CN:** AC RAIZ DGP

**Subject OU:** CNP

**Subject O:** DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**X509SKI**

**X509 SK I** Dpx24aIuiTNB8uM+bFsWRb29ho4=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2014-03-17T00:00:00Z

**2.2.7.8 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

2.2.7.9 - Extension (critical): Qualifiers [QCForLegalPerson]

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDAsURN ] <urn:oid:2.16.724.1.2.1.102.36>

**Policy Identifier:**

**Identifier** [ OIDAsURN ] <urn:oid:2.16.724.1.2.1.102.37>

2.3 - Service (granted): Qualified Certificates issued by subordinated CA under the root CA DNIE 2

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [ en ] *Qualified Certificates issued by subordinated CA under the root CA DNIE 2*

**Name** [ es ] *Certificados Reconocidos emitido por CAs subordinadas de la CA Root DNIE 2*

Service digital identities**Certificate fields details**

**Version:** 3

**Serial Number:** 57300804758115330416592336794492330659

X509 Certificate

-----BEGIN CERTIFICATE-----
MIFz2CAsOgAwIBAgIQKx7y2HPSCRSRV09XtivozANBqkhiG9wBQA0FADBMQewCOYDVOOG
EwFlUzEzMCYGA1UECgwREISRUINDS190IEEdFRVVSQUwREUgTEEgLTU9MSUNJOTENMASGAIUECwwE
REISREXMBUeGAIUEAwOQUMgREUwRjBETkFIDWlhcNM1MwOTJMTA1VNAJWbcNNDMmOTEMTAy
NNA1WBBMqswCOYDVOOGQwFlUzEzMCYGA1UECgwREISRUINDS190IEEdFRVVSQUwREUgTEEgLTU9MS
SUNJOTENMASGAIUECwwEREISREXMBUeGAIUEAwOQUMgREUwRjBETkFIDWlhcNM1MwOTJMTA1V
DQEAQUAAHICDwAwggKAwGAADzCIBKp01Nzm3wU3LlL2kzV3hRlocOS0y3dYFg
wVb1oNARYKdAkvUvmpX7h18zFKYhbcAnzS3M6tFwzrPHIASLHpsGjWlMDcCOMlVQcuIusEc
LXg8vzicq7FQd3ngAZE1y9DZEzNpNckJWVqspMk1tixTtOSUGK78MnlKuuB8yrsbnY7ily6
IVj6US8Y1jblFFDmIhnpRRK7CLOAmesbzPPwM1SDXtwzS4tU4+mk4K CcU/bncKm
O4+AGOWqrmLpymKGBBSESWLvODwzZLrcmsWdvsVfKcGPTL1qf0FxtsP6Mz9VJ1huTfBN
Fy3o3AC4ZwnvQUVzRtEsaufacQjBHdXjdfZQ0cOjYBUUjDGO3mWzmxXOpSDuMHaSobK
0h8DFZDZVzwnvP0WlmsYzUoypj0wGL6stZdVtUwRBR53LzLzArgf0WpWk3Op12T6h
CzLczbHTOK9SYuyxLZpvoGuzAy3ZcaZ3USOCfCYmNhaos8R69+Is0SYglzZ6cPcVt
D0BB1Lub9SOWbfHpdz6WlUd4zAumlgW9V9kerOhsWlU4hhaan3AdW3spvQ0q5wzSw49p
Z9dD7NdeRcT3++vndM1QIDAQABGSMGKMMFASGAIUEwEBwGOMBA3wDgYDR0RPAQH/
BAODAgEMBOGAIUdDzQWBBRT3G5pM4T3Gfgh6fapA+YhLwzBNBzNVHSAER/BEMEGFUDIAAw
OJA4BgggBgEgBQCARVsaHR0cDovL3BnaSsw2cpY2lhl.mvZL2RnaWlUvchV6GjYWNpb25lcj9k
cGMwDjYkKozlhcNAQELBjA1DgBACEY8v84sKfFasSimp0Zs1VSpRy1hK0jWlmsYs
vHsdH345hdByA2m8ByYotaN0KfEmJXAYWLUQT2D0Ks0fm29SpqWFW6OMpFcp9Dh0Oqsk
0qPNP0BgYz6ZcRZKcGIMDF5foov5wJw0sNFkGCTWdfdW1ksmT4kRfE43lvsGpErBuiV
QsSesH7imwua4E30l8pysLDP3UMY0zkm0909B0Ldf0+TSLJURYXy4glEIA7A5
K4pS0uYl0WlWPOZG557ehLXdkCmsSpecHBHA5v1YcAs0IPGcX++sSa9K0Kc0rPhasCT0
sZMOV3e25UGzackVVSwaGK4aPWwGc1bmGdbhdw13M2NPOKkC9QNH++Dk80gm0cH68DcYQj
JUN2QYtGcaAZ79RmCWPmMwCjHISM4PpsD5h0HtZz7122DXrTmVD00u7kTWdPa0
R1w8ghV9SE65nOBw8Z1udEi9mN2u0hLqamf63FOCZSAQ2Nv4E.Ks7GTm09214RylLnam
GAzXKSRU11OpNuZapsEY7na3Nc175++Ynm2UjIKFbnBgKwP4Z2SDVnXfgh7dgQe0g601x
VVABe08VETy3SEmvlLhkGQ3h
-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

AC RAIZ DNIE 2

Issuer OU:

DNIE

Issuer O:

DIRECCION GENERAL DE LA POLICIA

Issuer C:

ES

Subject CN:

AC RAIZ DNIE 2

Subject OU:

DNIE

Subject O:

DIRECCION GENERAL DE LA POLICIA

Subject C:

ES

Valid from:

Fri Sep 27 12:26:05 CEST 2013

Valid to:

Sun Sep 27 12:26:05 CEST 2043

Public Key:

30820222300D06092A864886F70D01010105000382020F003082020A0282020100DB642FDB45FA65FE23739FFDF052B60B7E2E7F6CE4CD5DE5691FC8A1CDF44B96B2DE2
9E23D01561D340D610160A0DA3E951594959670D4F331646287AD8089E387733A15A156736ACF1E402D48B1E9E4E27050C00E08E33452F41EB85BACT1E2D783C8F38A
BEEAA3B150779E0019133CDB0D910D8A935E925556AAACA4CB4AD7E7B714E2ACEE5418AEFC32720ABAED7DCA3B336E763B22DCBA975563EAC512B7CB58C312D
FC51436C922B6E6DA6285128508B38099E868DA43CF0C0D790D74F0B19B05694F8FAE91D1E0209E51B83E5E1B1AE43F801905AA8F1E9946A9C3C906841B3A13C58BA9
5383C3164BA4C9E8E109C9771BC529E1874CB05A87416DC6233A33B3D5758F6EE4D814D16FD18DF40D2E367309D04145738D1B0492E49AB824096C91D1D5E3B5
D1594108B1423CD8054277883B46437996CE6C573A9E43B8C1DA4A86CA2D20433FB643B586707287663D8D694CE546A8CA900EC060ECE8B65D564214BBF7516F8E5
DFCB99027804F45E56C564CADE31A9D3D93EA10B351C65BF474CE1BD498B82C75669B6F3B3BA00286397367006775123BF0837187E498D261694A8B01C7A3FE2
128B449880E49905A0A954B0D0061D4B89F6B4905A76C57C8A3D97A89651D5F877502A98981637D54A82B387616D6E4E1F868660DCD01D5B2B23A647EA4AE70C
D2C38F6867DB8314D77871846BDFEAF75AA087E7313BD0203010001

Basic Constraints

IsCA: true

Subject Key Identifier

53:DC:6E:62:A4:CE:13:1B:77:E0:87:A1:5A:A4:0F:B2:87:12:F0:9B

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://pki.policia.es/dnie/publicaciones/dpc

Key Usage:

keyCertSign - cRLSign

Thumbprint algorithm:

SHA-256

Thumbprint:

C5:C3:80:EB:92:40:FB:36:A1:6E:15:F5:D6:BA:D0:BF:61:1F:6D:03:F0:EF:24:22:99:19:E7:D2:D8:12:6C:11

X509SubjectName

Subject CN: AC RAIZ DNIE 2

Subject OU: DNIE

Subject O: DIRECCION GENERAL DE LA POLICIA

Subject C: ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

#### Scheme Service Definition URI

URI [en] <http://pki.policia.es/dnie/certs/AC004.crt>

URI [es] <http://pki.policia.es/dnie/certs/AC004.crt>

URI [en] <http://pki.policia.es/dnie/certs/AC005.crt>

URI [es] <http://pki.policia.es/dnie/certs/AC005.crt>

URI [en] <http://pki.policia.es/dnie/certs/AC006.crt>

URI [es] <http://pki.policia.es/dnie/certs/AC006.crt>

URI [en] <http://pki.policia.es/dnie/publicaciones/dpc>

URI [es] <http://pki.policia.es/dnie/publicaciones/dpc>

#### 2.3.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

#### 2.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 2.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.



[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:2.16.724.1.2.2.2.11
-------------------	------------	-----------------------------

**Description****2.3.4 - History instance n.1 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by subordinated CA under the root CA DNIE 2
-------------	------	---

<b>Name</b>	[es]	Certificados Reconocidos emitido por CAs subordinadas de la CA Root DNIE 2
-------------	------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	AC RAIZ DNIE 2
--------------------	----------------

<b>Subject OU:</b>	DNIE
--------------------	------

<b>Subject O:</b>	DIRECCION GENERAL DE LA POLICIA
-------------------	---------------------------------

<b>Subject C:</b>	ES
-------------------	----

**X509SKI**

<b>X509 SK I</b>	U9xuYqTOExt34IehWqQPsocS8Js=
------------------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>
-----------------------	---

<b>Status Starting Time</b>	2015-04-10T00:00:00Z
-----------------------------	----------------------

**2.3.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC</a>
------------	------	---

**2.4 - Service (granted): Qualified Certificates issued by AC DGP 004**

**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description***[en]*

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

*[es]*

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name****Name***[en]*

Qualified Certificates issued by AC DGP 004

**Name***[es]*

Certificados cualificados emitidos por AC DGP 004

**Service digital identities****Certificate fields details****Version:**

3

**Serial Number:**

31794812614395090018704226159857973009

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```
MIIHlCCBRXgAwIBAgIQF+HSpCwD92ZbYvIha=Cc3ETANBqkqkqG9w0BAQSFADB3M0swCOYDVOOG
Ew/FUZaM+YGAUUEc+gR/EISRUND5/90EEdfTKVSOIwgREUgTEEGU9NSI/NKTEMMAAGAUUECwWd
QOQMRgWfGyDVQRbDA9VQRfUy1TMjgxNjA5NjU3fAUeNBVAMMDUFDIFB5VogRE4IDWbHcN
MfjwODAYMTA1MDAyWbcNMeAwODAYMTA1MDAyWjB0M0swCOYDVOOGGwJfUzEoMCCYGAUUEC+gR/EIS
REIND5/90EEdfTKVSOIwgREUgTEEGU9NSI/NKTEMMAAGAUUECwWdQOQMRgWfGyDVQRbDA9VQRf
Uy1TMjgxNjA5NjU3fAUeNBVAMMDUFDIFB5VogRE4IDWbHcNMaQCCFDEIHRUCAMMDQwggIMAOGCSgSb5DOEBAQAUA4ICDwAw
ggKkoCAQCuDuWxQPywDK8o3RyXoDORMWgiVlyEnQSEIRHSuopHQEIR14eLoSkYyH0PbMRpeq
8z2Bb0A2uRGoXnmgKlHTAm98p1ALGekEz2B96OFfEsmqPbZMZSsV08ZSkZGK
CKMzLkqCgoocap2wD=ivaDoxEoMFVKLInZLHbnv9RbVdZ969RlHjoEXcslH7SgnOp0lpEiO
L2jYYSIXQyLROHQHSVP5+fj3H6oK+98Hj94uqEEXuHqLMFKJPO1VAyEsTycmzlmZzc
fOyWbc99w98Hm1HLR68OwBkS89UzOKidNinESh-dmPLkfwRwFc170I2QwYpY9A
JagKHwG9hzVJigEa+PPPSEuGOOAGXZJheEF3o8FOv6Pz3=-JnlBSly7CGWbSSEIDUajc
KOXe98GDmBpqP8bKNCrXylLdV4z2BG5CapOkp+agbDvDgWrc03EFDka76v7fWgUcCcv
NRW6RCCa2j9y90Ais0f85m9S2k1f0ow1X5T5TwOks+Odu00S0MC21MGQqEVEZ9k
i6YZOml3aS5wXb5cXv4yXwME3gd5XHmqf0CSGjX9+OmGIS0DmKacJAUhJ5Hgzpcml0Vo
JhRZg1HQIDAQABo4ICDCCABwWgHQYDVR0OBQYFA2e5MC015kdvGfL+9N4yYjK8MG6GCCSG
AOUfBwEBB9wXA3BggRgfBQwAyyYwARkdDowl29c3Auc09swWp1Y5S1zA3BggrBgEFBQcw
AoYnHR0kDowl3BraS5w2xpY2BlmVzL2NucC9XJ0cy9BQ1JhaXoyLmNydDAiBgNVHSMDGDAW
gHS7G0WrtLyPSZEOKzTOPGIWUoeGDBMBGNVHSARTEBDMEEGBFUAIAAwOTA3BggRgfBQcCARYr
aHRODowl3BraS5w2xpY2BlmVzL2NucC9wWJswWbV2hmZL2RwY2AsBgNVHRMAIFNDAIG
AQHAgEAMAAAGAUUdDwEBwQEAwIBBjCB+gYDVR0BHyMHVMIHs0HpolfmhZodHRwOi8vcGp
LnBvYyWwZuZXMyZ25wL2NyYyMmQVJmLmNybGludXUyX2V0Ly9zZGFwLnBvYyWwZuZXMyZ25w
Q1MEEOPTEfTiwkEjFwJyMEBICUyMDR089VfRrMuzAMFYwM1VE5VPUtOUcXPPURJ
UKVDQ0PtlYMEgfTRVSQwImjBERSUyMEABTUwE9MSUNJOSxDPUVTP2fidGhvcml0eVJldm9y
YXJp625MaXN0P2h2Uk2JgZWN0Y2hlc2M9Y1JMRGZldHJyYnVhW9wtUG9pbhQwDQYJKoZIhvcN
AQEIDAQggBAAv01yY1Wk8Wkepp6bmmVak8Ke3myYNSH4Zz02pHj4idL7O1kRkAcncHATz
4NdcCMCZBppIur9LNVx2RK1mYCY26QeSyl1+01UYO3OTZ2auc8LbmtosKNPwjzta99SB
Kzbn9KmfMaF2SbpQvH57NbgfQRsyR848ldh2U76yX7Td90NrtkcpkP0NYGnXpPh9R9RZ
Qm1gr7ywTKVSw9gApPwPwYk1u8QZBLZz3p1iHHCw16K4DXGFwBSPg5U0kU
wDBxds9YEE97ZuarWEcgaF0kXVCUwUWhaZnjBAW3mzZTCBJV+plw1UT0Vmsc2N9R
Qw4dU06gNRG0Ulcq8LhhBqycmOdlshsYcdko66fH6z83m5cCQRksI9+dnI2KwXBzF1
Sp7eucyDk0R6RnE2z06KpBZIMZdfjmkY1Y0kRWw0Z7z+NZyZb0f0isj2k3Tg/
LCXjA2MMfaRfRsw8WbDGH0LBBl6pM0yAMOD2BMhyJSScKizbOr0aacP2hDB43Fk92L
MSAChAAuhQT/EgQsum6QwRkfuC9PVMp3cZcKMU/IMNL5MdsUetuaBSR0uVYp9U3Ez2kCmR5
ik4pHhBZBI
```

-----END CERTIFICATE-----

**Signature algorithm:**

SHA256withRSA

**Issuer CN:**

AC RAIZ DGP 2

**Issuer 2.5.4.97:**

VATES-S2816015H

**Issuer OU:**

CNP

**Issuer O:**

DIRECCION GENERAL DE LA POLICIA

**Issuer C:**

ES

**Subject CN:**

AC DGP 004

**Subject 2.5.4.97:**

VATES-S2816015H

**Subject OU:**

CNP

**Subject O:**

DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**Valid from:** Thu Aug 02 12:50:02 CEST 2018

**Valid to:** Tue Aug 02 12:50:02 CEST 2033

**Public Key:**  
3082 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 02 0F 00 30 82 02 0A 02 82 02 01 00 AE 0E E5 97 40 F6 30 0C AF 28 DD 1C 97 A0 34 11 31 67 25 54 BC 84 9D 0F 04 21 11 D2 BA 8A 61 40 47 FC D  
7 87 BF 2E 3F 1D 61 88 48 D0 FC 9C 46 97 AA F2 8D 81 6C 9D 00 DA E1 11 14 85 E9 8A 1A 8A D6 3B 47 EC 09 94 F6 CA 75 34 BD 46 78 87 11 CF 70 7D B1 01 04 69 29 B8 A4 C9 19 33 64 AC CE 45 88 F3 FD B  
9 2A BF D9 8C 64 BF 0A 43 33 2E 4A 82 82 8A 02 6A 9D B0 0F E8 AF 9C 5A 51 12 83 05 AD 59 0B D6 76 4B 1D B9 EF F5 15 5B 75 96 7D EB D4 65 86 3A 04 5D CB 25 86 2E D2 AA 73 A9 8B 42 33 A4 48 8E B7  
68 EF 8D 8D 52 25 74 1D C8 B4 74 1D 01 D2 54 FA F9 F9 F8 F7 1E 0E A2 2B EF 7C 96 9C F8 AA EB 5E 34 4C 62 B8 78 AA 2C C1 4A 24 F3 B5 54 0C 84 B1 3B 58 72 0C E5 99 76 5C 21 0C 96 6D C2 3D F6 FE 3C  
20 82 26 D4 82 DF E8 17 5B 1B 0B 41 B1 AF 12 F3 46 50 82 57 7E B4 DD 67 1F 98 7E 76 6A 54 2E DE 88 73 04 70 15 CD 5C FC ED 36 42 EC 58 A4 4F 40 B5 A8 0A 1F 01 B0 86 BC D5 D6 38 04 6A 2F AB 3E F2 7  
9 12 E1 8E 39 7A CR 19 76 49 85 E1 05 DE 8F 05 3A F8 44 7E SC F7 F8 97 E7 7C 1E 48 CB B1 82 58 1B 39 12 D0 D4 6A 3B 82 28 E5 DE F7 C1 83 98 13 EA 7C FB 01 28 D0 91 B5 78 F2 2E 47 55 E1 AD B3 04 6E 7  
F 09 AA 4E 92 2A 7E 6A 06 C3 BC 38 16 CA 2A 37 10 50 C9 B1 AE ED EA FE C5 5A 05 1C 80 27 2F 35 15 9D EB 60 B1 03 68 EB F3 2F 4E 02 2B 34 06 B8 F9 7D AB 7D E6 4D 9C D6 21 68 B3 0F E2 5C 9E 53 D3  
04 21 AA 5F 90 77 1B B4 94 EE 50 30 2D B5 F2 F1 8E A8 45 44 43 3F 71 8B A6 19 3A 6B 77 CD 2E 70 5D BF F2 E5 C5 EF E3 25 F0 30 4D E0 8D DE 57 1F 89 AA 17 A0 B9 19 F8 D7 27 DF 8E 98 67 D2 F3 40 E6 29  
A7 25 80 0B 87 8F 91 ED DA BA 5C 9B 45 68 26 14 59 CE 0D 7F 1D 02 05 01 00 01

**Subject Key Identifier** 0D:A7:E4:C0:B4:D7:97:E4:74:DC:86:7C:52:FE:F4:DE:32:62:32:BC

**Authority Info Access**  
<http://ocsp.policia.es>  
<http://pki.policia.es/cnp/certs/ACRaiz2.crt>

**Authority Key Identifier** 93:80:EB:56:AD:4B:CF:B1:91:0E:2B:34:CE:3C:62:16:1E:87:BF:80

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://pki.policia.es/cnp/publicaciones/dpc>

**Basic Constraints**  
IsCA: true - Path length: 0

**CRL Distribution Points**  
<http://pki.policia.es/cnp/crls/ARL.crl>  
ldap://ldap.policia.es/CN=CRL,CN=AC%20RAIZ%20DGP%202,OI=VATES-S2816015H,OU=CNP,O=DIRECCION%20GENERAL%20DE%20LA%20POLICIA,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 6A:D4:3C:81:5C:D8:47:AF:82:B1:80:A2:A0:BD:39:02:B3:52:0E:19:CF:0E:D2:10:D8:00:99:E5:97:42:99:00

**X509SubjectName**

**Subject CN:** AC DGP 004

**Subject 2.5.4.97:** VATES-S2816015H

**Subject OU:** CNP

**Subject O:** DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**X509SKI**

**X509 SK I** DafkwLTXI+R03IZ8Uv703jJiMrw=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

<b>Service status description</b>	[en]	undefined.
	[es]	undefined.

**Status Starting Time** 2019-01-15T01:00:00Z

#### 2.4.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

#### 2.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
------------	------	---

#### 2.4.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
------------	------	---

### 2.5 - Service (granted): OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>

<b>Service type description</b>	[en]	A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.
	[es]	A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.

#### **Service Name**

<b>Name</b>	[en]	OCSP Responses issued by Autoridad de Certificación AC RAIZ DNIE 2
-------------	------	--

<b>Name</b>	[es]	Respuestas OCSP emitidas por Autoridad de Certificación AC RAIZ DNIE 2
-------------	------	--

#### Service digital identities

#### **Certificate fields details**

**Version:** 3

**Serial Number:** 57300804758115330416592336794492330659



**Subject CN:** AC RAIZ DNIE 2

**Subject OU:** DNIE

**Subject O:** DIRECCION GENERAL DE LA POLICIA

**Subject C:** ES

**X509SKI**

**X509 SK I** U9xuYqTOExt34IehWqQPsocS8Js=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2021-04-21T00:00:00Z

**2.5.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 3 - TSP: Agencia Notarial de Certificación S.L. Unipersonal

#### TSP Name

**Name** [ en ] *Agencia Notarial de Certificación S.L. Unipersonal*

**Name** [ es ] *Agencia Notarial de Certificación S.L. Unipersonal*

#### TSP Trade Name

**Name** [ en ] *VATES-B83395988*

**Name** [ en ] *ANCERT - Agencia Notarial de Certificación*

**Name** [ es ] *ANCERT - Agencia Notarial de Certificación*

**Name** [ en ] *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Name** [ en ] *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

#### PostalAddress

**Street Address** [ en ] *Calle Campezo, nº 1, Edificio 6, pl. 2ª*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28022*

**Country Name** [ en ] *ES*

#### PostalAddress

**Street Address** [ es ] *Calle Campezo, nº 1, Edificio 6, pl. 2ª*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28022*

**Country Name** [ es ] *ES*

#### ElectronicAddress

**URI** [ en ] *mailto:ancert@ancert.com*

**URI** [ en ] *http://www.ancert.com*





**Subject O:** Agencia Notarial de Certificacion S.L.U. - CIF B83395988

**Subject L:** Paseo del General Martinez Campos 46 6a planta 28010 Madrid

**Subject C:** ES

**Valid from:** Tue Jun 21 12:09:32 CEST 2016

**Valid to:** Sat May 25 02:01:00 CEST 2030

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100AF1C82F732F3D5C616D47997802121A1F4455094BBB8E5FF1E07E97F050031A66DE9C  
D73FB9B1E0125AD31C1AE2205A425377C3F5A3FC9D99FA03231225866769CC8C36C4720E0F7547C6E344F3FA0F5A840370B69214D6739E4C721601A9FFDE701BEC  
E81B6F25186CA4D72E8B023AB5D8A0302940992F642F4F9CF76CB4D6961F36C05A6F0F8F99292762373C25D9FDA6A6BEA5E3299880FC2907E896AD8D87FE1CEA2B4  
A870725A77A994AD1A8A7C2365C20914365F6A58A169BEA3758E293ACC2F21CC727C44BD050CB0EC8A2DF6EC5521E4F390B575F89E9BA5C18AFE9B832A8B18753  
6BB948C1DFBAF122FA3BAF359F57670C33147D71D2622349657F0CC603499F8984101A0A32994D804286DD2B8B8CA6C40B8C4FF89E8943878EA15619A1B40CA  
89DBE77E70D5563DCA77C42803133CA7A25D0C13D7E00B75E0BDFE4E957906741686584DD2189F2CFBB7A7B6EE4D77C2E398009FCDE312F1E798277F5607016DC67  
B520C84FEDCD4DD21294D146280AB79DECB8A86337EBCA38B43169423B266C252D64820F1FE8F9E08AD1204E2EC66475889133F79A5AC6E7FC38C4F1F82061AF  
689B563264E1EA40AECB1620DA45F65FEC4F78A479D8E65F4F577FB1EB80F2B61C5BF49AA19B415470C2646DCB26A16DEB4F58EB8C2B2AFC0D211CB9BF892098CF  
D00B27698D6B9C7E18CB46D965D901725561F8E10550203010001

**Authority Info Access**  
<http://ocsp.ac.ancert.com/ocsp.xuda>  
[http://www.ancert.com/pki/v2/certs/ANCERTPRIV\\_V2.crt](http://www.ancert.com/pki/v2/certs/ANCERTPRIV_V2.crt)

**Authority Key Identifier**  
FD:3C:6A:79:66:15:3C:00:BB:D2:36:A2:62:A6:58:E6:1A:E0:33:AF

**Basic Constraints**  
IsCA: true - Path length: 0

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.18920.2.1  
CPS pointer: <https://www.ancert.com/cps>

**CRL Distribution Points**  
[http://www.ancert.com/crl/ANCERTPRIV\\_V2.crl](http://www.ancert.com/crl/ANCERTPRIV_V2.crl)  
[http://www2.ancert.com/crl/ANCERTPRIV\\_V2.crl](http://www2.ancert.com/crl/ANCERTPRIV_V2.crl)  
[http://www3.ancert.com/crl/ANCERTPRIV\\_V2.crl](http://www3.ancert.com/crl/ANCERTPRIV_V2.crl)

**Subject Key Identifier**  
5F:EE:DD:29:03:01:43:69:C8:1E:3D:5B:81:7E:A5:F3:A1:76:AC:F8

**Subject Alternative Name**  
pki.explotacion@ancert.com

**Key Usage:**  
digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
AE:9E:FF:CD:7B:83:0D:9A:7A:6D:F0:90:7E:DF:CE:FE:5D:C8:8A:A5:CC:B7:04:5F:03:FD:67:1C:  
BD:E5:B4:B7

**Certificate fields details**

**Version:**  
3

**Serial Number:**  
151806557225635609738953006987710450500

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH0CCBSggAwIBAgIQjThlmVlg1wyzv9Bipl.RDANBgkqhkiG9w0BAQsFAgCgDELMAKGA1UEB...

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

ANCERT Certificados Redes Privadas V2

Issuer O:

Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Issuer C:

ES

Subject CN:

ANCERT Corporativos Personales V2

Subject O:

Agencia Notarial de Certificacion S.L.U. - CIF B83395988

Subject L:

Paseo del General Martinez Campos 46 6a planta 28010 Madrid

Subject C:

ES

Valid from:

Thu May 27 09:46:34 CEST 2010

Valid to:

Wed May 27 09:46:34 CEST 2020

Public Key:

30820222300D06092A864886F70D01010105000382020F003082020A0282020100AF1C82F732F3D5C616D47997802121A1F4455094BBB5E5FF1E07E97F050031A66D0E9C...

Authority Key Identifier

FD:3C:6A:79:66:15:3C:00:BB:D2:36:A2:62:A6:58:E6:1A:E0:33:AF

Basic Constraints

IsCA: true - Path length: 0

Certificate Policies

Policy OID: 1.3.6.1.4.1.18920.2.1
CPS pointer: https://www.ancert.com/cps

CRL Distribution Points

http://www.ancert.com/crl/ANCERTPRIV\_V2.crl
http://www2.ancert.com/crl/ANCERTPRIV\_V2.crl
http://www3.ancert.com/crl/ANCERTPRIV\_V2.crl

Subject Key Identifier

5F:EE:DD:29:03:01:43:69:C8:1E:3D:5B:81:7E:A5:F3:A1:76:AC:F8

Subject Alternative Name

pki.explotacion@ancert.com

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *8A:C2:CF:DE:0B:8A:60:12:51:8A:A3:BC:EF:89:55:26:B1:A5:29:B4:F6:39:54:4B:23:2C:DD:62:8D:81:5D:71*

### **X509SubjectName**

**Subject CN:** *ANCERT Corporativos Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2018-02-15T01:00:00Z*

### **3.1.1 - Extension (critical): additionalServiceInformation**

#### **AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### **3.1.2 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

### **Service Name**

**Name** *[es] Certificados Corporativos Personales v.2*

**Name** *[en] Personal Corporate Certificate v2*

### **Service digital identities**

### **X509SubjectName**

**Subject CN:** *ANCERT Corporativos Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** ES

### X509SKI

**X509 SK I** X+7dKQMBQ2nIHj1bgX6l86F2rPg=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

#### 3.1.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 3.1.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ es ] *Certificados Corporativos Personales v.2*

**Name** [ en ] *Personal Corporate Certificate v2*

#### Service digital identities

#### X509SubjectName

**Subject CN:** *ANCERT Corporativos Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** ES

### X509SKI

**X509 SK I** X+7dKQMBQ2nIHj1bgX6l86F2rPg=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2010-11-16T00:00:00Z





**Signature algorithm:** *SHA256withRSA*

**Issuer CN:** *ANCERT Corporaciones de Derecho Publico V2*

**Issuer O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Issuer C:** *ES*

**Subject CN:** *ANCERT Corporaciones de Derecho Publico Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**Valid from:** *Thu May 27 10:04:55 CEST 2010*

**Valid to:** *Wed May 27 10:04:56 CEST 2020*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201009D2D4309E6656B83A6CB97A20343B1BFCA24746FE83AF64568AB720C4D567711E565C  
4B4940011D16456F69EA683A636423F3212F3271261A250A2E71C651BCK89E3EEC62A151CAE25EFD4EE58B88F9D1309F44E4EE73116D0C538A8407950C2FB8471A664A  
922BC408A3B511F9CD3B1A8FA2109D6405B21D90FF30CB2E9B11F1F38B0E03DB5FE92661D0216A93D94D16278A694138CEBE88F5B19A34E747BCD6A4B6AD93775  
37D2F6593EC416D61FE22C6CB7C775F3CB0F66A21A668E56957C02D35F43FE942AEA6E6FE0B3D58A7C99A75FCYCA30CEA53A5A935CD12030794B55E19806  
405ACD9CDA759F1229C4768B84CD63F3B781E5C750AB339D4B0F8B4A382D2B1B2A1F00899F94E7B3C06776E174F86DD8C798B89B04C175AD2ED73AF057323066  
49BEE369E.CF8F38F5864700C427CB5636606DA3D74EEBA775C59F39AC.C5B1FEA760CFD1F93BA2FBC7AF090A8D7A014758CE9095E3307AFC30555F44BB4B4645  
41E924C289BF28F43271973D7067F66E0F60DBE56F5FE9AF2E2CEAD0ABE9EC9CD24A9C71D85615EE2E1CAA221A4419F78B1E44E5A603B2B975E7544F54A8C568C95  
599622416BF2E7BCC264E273BA7279B6929523FA08902F3948E8DDA38EE33C9B8FE89E59413F5F2C537D6BBFA17B17631C70CCB9D6F7C5C2416A62894D7F0A3012  
B3366CD3588EF371F89D3BF4A1A1E44BFD8C27350203010001

**Authority Key Identifier** *40:C8:73:80:39:5C:42:7F:08:43:C3:DC:C7:F5:EE:80:EC:ED:FE:D9*

**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.3.1*  
*CPS pointer: <https://www.ancert.com/cps>*

**CRL Distribution Points** *[http://www.ancert.com/crl/ANCERTPUB\\_V2.crl](http://www.ancert.com/crl/ANCERTPUB_V2.crl)*  
*[http://www2.ancert.com/crl/ANCERTPUB\\_V2.crl](http://www2.ancert.com/crl/ANCERTPUB_V2.crl)*  
*[http://www3.ancert.com/crl/ANCERTPUB\\_V2.crl](http://www3.ancert.com/crl/ANCERTPUB_V2.crl)*

**Subject Key Identifier** *C0:BA:BA:37:3B:43:72:09:BC:5B:3B:36:D6:B2:DE:2D:F6:4B:7C:C8*

**Subject Alternative Name** *pki.explotacion@ancert.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *26:18:A9:AC:8D:B2:5F:36:4F:DB:37:C3:9D:B3:93:AC:00:11:1A:BE:57:64:8F:EF:65:7D:75:1C:66  
:02:21:D2*

**X509SubjectName**

**Subject CN:** *ANCERT Corporaciones de Derecho Publico Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2018-02-15T01:00:00Z*

### 3.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 3.2.2 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** *[es] Certificados Personales de Corporaciones de Derecho Público v.2*

**Name** *[en] Qualified Personal Certificates for Public Corporations v2*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *ANCERT Corporaciones de Derecho Publico Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *wLq6NztDcgm8Wzs21rLeLfZLfMg=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*



**3.2.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.2.3 - History instance n.2 - Status: undersupervision**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ es ] *Certificados Personales de Corporaciones de Derecho Público v.2*

Name [ en ] *Qualified Personal Certificates for Public Corporations v2*

**Service digital identities****X509SubjectName**

Subject CN: *ANCERT Corporaciones de Derecho Publico Personales V2*

Subject O: *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

Subject C: *ES*

**X509SKI**

X509 SK I *wLq6NztDcgm8Wzs21rLeLfZLfMg=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2010-11-16T00:00:00Z*

**3.3 - Service (granted): Certificados Notariales Reconocidos para personas físicas v.2**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
 [ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

Name [ es ] *Certificados Notariales Reconocidos para personas físicas v.2*



**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.1.1*  
*CPS pointer: https://www.ancert.com/cps*

**CRL Distribution Points** *http://www.ancert.com/crl/ANCERTNOT\_V2.crl*  
*http://www2.ancert.com/crl/ANCERTNOT\_V2.crl*  
*http://www3.ancert.com/crl/ANCERTNOT\_V2.crl*

**Subject Key Identifier** *6F:1B:B8:64:97:1D:3C:F5:87:BA:05:A8:FF:EC:F8:E8:F7:94:D8:63*

**Subject Alternative Name** *pki.explotacion@ancert.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *C4:47:25:08:C3:BC:68:9F:C5:9E:8B:F7:7A:6D:DE:DF:BB:29:A4:33:16:BD:09:46:D5:44:E5:4D:F  
C:00:15:35*

**X509SubjectName**

**Subject CN:** *ANCERT Certificados Notariales Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

**3.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**3.3.2 - History instance n.1 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** [ es ] *Certificados Notariales Reconocidos para personas físicas v.2*

**Name** [ en ] *Qualified Notarial Certificates for individuals v.2*

### Service digital identities

#### X509SubjectName

**Subject CN:** *ANCERT Certificados Notariales Personales V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *bxu4ZJcdPPWHugWo/+z46PeU2GM=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2010-11-16T00:00:00Z*

### 3.4 - Service (granted): Certificados Notariales Reconocidos para personas jurídicas v.2

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** [ es ] *Certificados Notariales Reconocidos para personas jurídicas v.2*

**Name** [ en ] *Qualified Notarial Certificates for legal person v.2*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *80355812110946286783278297140241042538*



**Subject Key Identifier** 08:A1:2C:68:35:80:A4:FF:9C:AB:11:6C:0B:33:99:2D:71:19:AA:30

**Subject Alternative Name** pki.explotacion@ancert.com

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 0C:A8:B7:A0:15:06:CA:FA:A1:87:9E:74:91:C6:62:F8:26:4E:B3:A2:F1:F0:E0:65:7D:A3:D6:A9:12:FF:14:87

**X509SubjectName**

**Subject CN:** ANCERT Certificados Notariales Corporativos V2

**Subject O:** Agencia Notarial de Certificacion S.L.U. - CIF B83395988

**Subject L:** Paseo del General Martinez Campos 46 6a planta 28010 Madrid

**Subject C:** ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2019-10-28T01:00:00Z

**3.4.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1

**3.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>**3.4.4 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

<b>Name</b>	[ es ]	Certificados Notariales Reconocidos para personas jurídicas v.2
-------------	--------	---

<b>Name</b>	[ en ]	Qualified Notarial Certificates for legal person v.2
-------------	--------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	ANCERT Certificados Notariales Corporativos V2
--------------------	--

<b>Subject O:</b>	Agencia Notarial de Certificacion S.L.U. - CIF B83395988
-------------------	--

<b>Subject L:</b>	Paseo del General Martinez Campos 46 6a planta 28010 Madrid
-------------------	---

<b>Subject C:</b>	ES
-------------------	----

**X509SKI**

<b>X509 SK I</b>	CKEsaDWApP+cqxFsCzOZLXEZqjA=
------------------	------------------------------

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2016-06-30T22:00:00Z

**3.4.4.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1
-------------------	-------------	-------------------------------------

**3.4.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**3.4.5 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [ es ] *Certificados Notariales Reconocidos para personas jurídicas v.2***Name** [ en ] *Qualified Notarial Certificates for legal person v.2***Service digital identities****X509SubjectName****Subject CN:** *ANCERT Certificados Notariales Corporativos V2***Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988***Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid***Subject C:** *ES***X509SKI****X509 SK I** *CKEsaDWApP+cqxFsCzOZLXEZqjA=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time***2010-11-16T00:00:00Z***3.4.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[ es ] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier** [ OIDsURN ] *urn:oid:1.3.6.1.4.1.18920.1.3.1.2.1*



**3.5 - Service (granted): Certificados Reconocidos para empleados del Consejo General del Notariado v.2****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name****Name**

[es]

Certificados Reconocidos para empleados del Consejo General del Notariado v.2

**Name**

[en]

Qualified Certificates for the Spanish Notarial Council employees v.2

**Service digital identities****Certificate fields details****Version:**

3

**Serial Number:**

5238340232474032902941577877953496595

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIHhjjCCBAkAwwIBAgIAAeIRUUCjYVb66WCDGEzANBkshkG9w0BA0sFADBIMQovCOYDVQOQ
EWJFZzFBMDRGA1UUCM4QWdlbmNpYSB0b3RhemllbCBEZSBZDZlbnVzZjFjaW9uMFMuTCVSLA1
IENRiBCCODMzOTU0ODg5LzA3bGpNVAAMTGRFQQ0VSVCEBZDZlbnVzZjFjaW9uMFMuTCVSLA1
MDYyMTFwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
byBkZWVwR2VzZXh0bCByeX0wW5leBDBYwIw3MgNDYyGnMfgeCubhRhDDIAMDwE1EzHhZDFB
MDRGA1UUCM4QWdlbmNpYSB0b3RhemllbCBEZSBZDZlbnVzZjFjaW9uMFMuTCVSLA1IENRiB
ODMzOTU0ODg5LzA3bGpNVAAMTGRFQQ0VSVCEBZDZlbnVzZjFjaW9uMFMuTCVSLA1IENRiB
ggHMAOGC5gSIB3DQEAQAUA4ICDwAwggKAAoCAQDA8Ubb8LzME60xVuFDzQPIC6ICIAQ
q165Xh0e+rW40yYv2R9glEFMaPOHhXppXyAATUxkcdNMaMullHQuFE+vmHhVMN+F
pu51A8w76LTFJdXpC2h2hWZpYXm3FYXU0IBwK8Bz1TBImsAQBkRqo66McM
CEZFMgM0Ww2TRNaRMUxL3JApkQO5rNckRPKDE7ro020XFnLnpUhtj3eWwKwbHJEK
3vz6k6KorSb3aDwyP0CtLgk27BRXMD-190ULAZBtwHemLEOkmCwQSKVe+dyUAICh8idsTXW
Pr-4HTH6s6HfcXGpVc1eV608TGu0ufez8XopJlMefYceL4nd9IzmQQHr+Ks9Bw
hzw5a56tA1MukH61BUd1c95nHaj9pm50avVwTpw6TDolq2CGGxUYNIWAD08JHJVMWkcsbR
+9pzdDw1Sw68QCUCYvexXtEkwv3CtYluzcb0F9HB9kYgV8Xg-c-jpWzjBt1b+UPuVL
EW4HkO8W8wmlRCjmlNFEEZr2rNYUUYXJKER-3BaTPA5p808BzJpge8uMauKd2pw
XUUpstPk37B9qz2MGKLFmc24gojA4EiaofaWwIDAQAB0IB8jCCAc4wYAGCSGAOUFBwEB
BHQwJAvBggBgEFAQwAyyaHR0cDovL29jc3AuYWMuYW5zXj00LnV5b39yY3NlLnR1ZGUwPwY1
KwYBR0UHMARGM2b0dHA6Ly93d3cuYW5zXj00LnV5b39yY3NlLnR1ZGUwPwY1Q080X1Yy
LmNyYDAwMjE0MDg5LzA3bGpNVAAMTGRFQQ0VSVCEBZDZlbnVzZjFjaW9uMFMuTCVSLA1
MEEGA1UdIAQ6MDgwNyYKkYyBBAAGB2EgAjoMcyGCcSQAOUFBwIBFpoddHRwcz01L3d3dy5hbWNI
c30y29U2NwccBmgYDVR0BBGMCPHGM0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0G0
Y3JlL0FOQQVSVENH1P9WM5cmYgK2b0dHA6Ly93d3cuYW5zXj00LnV5b39yY3NlLnR1ZGUwPwY1
1P9WM5cmYgK2b0dHA6Ly93d3cuYW5zXj00LnV5b39yY3NlLnR1ZGUwPwY1Q080X1Yy
VREPAQIBAQDAgGCM0G0A1UdIgcQWBER0mim23GpCJ35VOYKkK0kAIBgNVIRHhEAgRpw
a2kuZXhw690YWVp25AYW5zZX00LnV5b39yY3NlLnR1ZGUwPwY1Q080X1YyLmNyYDAwMjE0
aZ21bE0S7eW0Rkn31JsuSeER5WYmMdsB7KSGTLRS7G7HQLOITRAV+qAF+Es44Ve1u
g08csmL08c8Ppnl3508c1ZAwWnhZgZ2h0GgrKk0vVez2leyoY8q85vmlJQuerpN
hjTgyvX0b8kkydWVGUMhuAUzR7xbW0+HGwT+RAEYBEfmX19RHZFE4KL934Yd3HQ-W
imBq+GBAMmNavQAYS1kdrOWZL0gemEszllmLkRlBspFun1B19v5c54AMPNI1Xp7p2pWc
mIBH72LkLk1T5E2U9AMy7L7PmbE+V46d8314W4eCOIT122R1816D8d0E520q
W9KnrDh3ZqZwptZagXSlAHmgSireLkzNqQYxyj+qg403jodT0J1msj2eMsb2xGud9
lyCg0H0z7VLLSTNH4DvLxT3WbEkg9lyChzBwHessyEXRRGDpbfJFzaothHmHGrv0QA
JvcZdgR8kG7DhJEIBabancwv2YFufn5CACBZJXK0QPCJNDNjms8eZLcs57WMDm68
JTwYpsn1SswVf0q6d16Fmm0CNskQeup2x+-WDLZyZpYyG5DPCCVU=

```

-----END CERTIFICATE-----

**Signature algorithm:**

SHA256withRSA

**Issuer CN:**

ANCERT Certificados CGN V2

**Issuer O:**

Agencia Notarial de Certificacion S.L.U. - CIF B83395988

**Issuer C:**

ES

**Subject CN:**

ANCERT Certificados para empleados V2

**Subject O:**

Agencia Notarial de Certificacion S.L.U. - CIF B83395988

**Subject L:**

Paseo del General Martinez Campos 46 6a planta 28010 Madrid

**Subject C:**

ES

**Valid from:** Tue Jun 21 12:27:52 CEST 2016

**Valid to:** Sat May 25 02:01:00 CEST 2030

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C0FFC51B06CE8BCC781EA8C55B850F37D03C80B A202B65010AB5E B3B17FE1D1EF A2  
479E34972606BF646CF402C414C68F5977ED5E CA097178C0AD4FD723C70334CB8CBA51D072E144FAF9E21E3C9530DF85A6EE7303CC09B7882D34455E306F0B787  
66E5168672617988DC56145F5D0E265062C8AF01CFEFD530759B7010F6A111A9CA29FFAA8A08C72B0A011ECC53203345A7D9344D6913145C BD C9029290950E6B35E29  
C44F72C0C4E EB A34B76B4E5C9CB9E951B7EB8E1DDE696B682B06DD1E3124DD5CFA DA4E8A A2B4A1DDAD F0C8FD027F12C62B6E C145731D F89F68B4BE33048B701  
D998B10CA49F00B04122957B E77230650887C25DB135D63F881D31E532CB3A1DFB3FD663EF55CD3E55ED3C B131AE02E75EACT371A29265304745CA319E2F8C6  
D765F5FE7BD041F887F88912F4137087FCF0E5A49EA2D03532E907B3505477573DE671DA8FDA66E4E6AF5704E9FE0E930E896A9F6186CS460D230900F4F3C2631E4  
54C5A472C6D1FBDA73B830F0D52CA F10FED09462F831C5F7442B1BE15C24DB8D4C1971B385F4707D2732A3560541B5783E73E2695B38DF062D5BF943EE54B116F F8  
1CA3A1156B9CA72D10A929C345133276AE25C D6253255D88CA27947EDC19D33E90378DE F3D701B99D6981E0675CC69F34A760DB8A6F5E2514A6C4CF C4ADFB07D  
B6AAF670C18A2E2166736E20A230381226BA25A5B0203010001

**Authority Info Access**  
<http://ocsp.ac.ancert.com/ocsp.xuda>  
[http://www.ancert.com/pki/v2/certs/ANCERTCGN\\_V2.crt](http://www.ancert.com/pki/v2/certs/ANCERTCGN_V2.crt)

**Authority Key Identifier**  
05:6E:E1:A1:9A:EE:07:AF:CE:F5:B4:D3:65:3D:04:50:E2:D0:9B:44

**Basic Constraints**  
IsCA: true - Path length: 0

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.18920.4.2  
CPS pointer: <https://www.ancert.com/cps>

**CRL Distribution Points**  
[http://www.ancert.com/crl/ANCERTCGN\\_V2.crl](http://www.ancert.com/crl/ANCERTCGN_V2.crl)  
[http://www2.ancert.com/crl/ANCERTCGN\\_V2.crl](http://www2.ancert.com/crl/ANCERTCGN_V2.crl)  
[http://www3.ancert.com/crl/ANCERTCGN\\_V2.crl](http://www3.ancert.com/crl/ANCERTCGN_V2.crl)

**Subject Key Identifier**  
74:9A:49:8D:DA:48:C6:80:28:D3:48:9B:CE:57:72:91:2A:EB:03:93

**Subject Alternative Name**  
pki.explotacion@ancert.com

**Key Usage:**  
digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
E7:18:F6:7C:8B:1F:8E:1F:C0:17:6A:36:1C:98:E6:29:9F:D3:F4:39:CF:A4:6E:DD:B4:6A:57:B4:AC  
:08:B4:43

**X509SubjectName**

**Subject CN:**  
ANCERT Certificados para empleados V2

**Subject O:**  
Agencia Notarial de Certificacion S.L.U. - CIF B83395988

**Subject L:**  
Paseo del General Martinez Campos 46 6a planta 28010 Madrid

**Subject C:**  
ES

**Service Status**  
<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**  
[en] undefined.  
[es] undefined.

**Status Starting Time**  
2019-08-08T00:00:00Z

**3.5.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	--------	---

**3.5.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.18920.4.2.1.3.1">urn:oid:1.3.6.1.4.1.18920.4.2.1.3.1</a>
-------------------	-------------	---

**Description****3.5.3 - History instance n.1 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ es ]	<i>Certificados Reconocidos para empleados del Consejo General del Notariado v.2</i>
-------------	--------	--

<b>Name</b>	[ en ]	<i>Qualified Certificates for the Spanish Notarial Council employees v.2</i>
-------------	--------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>ANCERT Certificados para empleados V2</i>
<b>Subject O:</b>	<i>Agencia Notarial de Certificacion S.L.U. - CIF B83395988</i>
<b>Subject L:</b>	<i>Paseo del General Martinez Campos 46 6a planta 28010 Madrid</i>
<b>Subject C:</b>	<i>ES</i>

**X509SKI**

<b>X509 SK I</b>	<i>dJpJjdpIxoAo00ibzldykSrrA5M=</i>
------------------	-------------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---

<b>Status Starting Time</b>	<i>2016-06-30T22:00:00Z</i>
-----------------------------	-----------------------------

**3.5.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.5.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados Reconocidos para empleados del Consejo General del Notariado v.2*

**Name** [en] *Qualified Certificates for the Spanish Notarial Council employees v.2*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANCERT Certificados para empleados V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *dJpJdpIxoAo00ibzldykSrrA5M=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2010-11-16T00:00:00Z*

**3.6 - Service (granted): Certificados Reconocidos de Notario v.2**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [es] *Certificados Reconocidos de Notario v.2*



**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.4.1*  
*CPS pointer: https://www.ancert.com/cps*

**CRL Distribution Points** *http://www.ancert.com/crl/ANCERTCGN\_V2.crl*  
*http://www2.ancert.com/crl/ANCERTCGN\_V2.crl*  
*http://www3.ancert.com/crl/ANCERTCGN\_V2.crl*

**Subject Key Identifier** *5F:93:40:B5:38:08:24:CE:F0:BF:23:4E:B9:2F:95:13:68:AE:84:FB*

**Subject Alternative Name** *pki.explotacion@ancert.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A8:85:EC:82:18:B1:C9:67:30:B0:26:4E:CF:BB:DE:E0:6C:97:B7:01:FA:F8:0D:CC:B2:69:20:F5:E7:27:AD:73*

**X509SubjectName**

**Subject CN:** *ANCERT Certificados FERN V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time***2019-08-08T00:00:00Z***3.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**3.6.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.4.1.1.3.1

**Description****3.6.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Reconocidos de Notario v.2*

**Name** [ en ] *Spanish Notaries Qualified Certificates v.2*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANCERT Certificados FERN V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *X5NAtTgIJM7wvyNOuS+VE2iuhPs=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**3.6.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.6.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Reconocidos de Notario v.2*

**Name** [ en ] *Spanish Notaries Qualified Certificates v.2*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANCERT Certificados FERN V2*

**Subject O:** *Agencia Notarial de Certificacion S.L.U. - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46 6a planta 28010 Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *X5NAfTgIJM7wvyNOuS+VE2iuhPs=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time**

*2010-11-16T00:00:00Z*

**3.7 - Service (withdrawn): Certificados Notariales Reconocidos para personas físicas****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [ es ] *Certificados Notariales Reconocidos para personas físicas*

**Name** [ en ] *Qualified Notarial Certificates for individuals*

**Service digital identities****Certificate fields details**

**Version:** *3*

**Serial Number:** *222481592478305966459721756209740642910*





**Subject Key Identifier** *A5:12:7F:B7:43:DB:51:29:67:C6:76:95:EA:EF:D9:E3:75:C5:C1:35*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *D7:90:51:96:05:C9:5A:B0:01:18:BD:98:62:29:0A:E9:AF:02:47:3F:22:33:76:B8:EA:33:D3:1A:60:FE:9F:C5*

**X509SubjectName**

**Subject CN:** *ANCERT Certificados Notariales Personales*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2016-06-30T22:00:00Z*

**3.7.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

**Qualifier type description** *[en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

*[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.1.1.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.1.2.1*

**3.7.2 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

3.7.3 - History instance n.1 - Status: supervisionceased

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

Name [ es ] *Certificados Notariales Reconocidos para personas físicas*

Name [ en ] *Qualified Notarial Certificates for individuals*

Service digital identities

## X509SubjectName

Subject CN: *ANCERT Certificados Notariales Personales*

Subject O: *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

Subject L: *Paseo del General Martinez Campos 46-6a planta*

Subject ST: *Madrid*

Subject C: *ES*

## X509SKI

X509 SK I *pRJ/t0PbUSlnxnaV6u/Z43XFwTU=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time *2015-03-09T23:00:00Z*

3.7.3.1 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [ en ] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[ es ] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

Criteria list assert=**atLeastOne**

Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.1.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.1.2.1

### 3.7.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Notariales Reconocidos para personas físicas*

**Name** [ en ] *Qualified Notarial Certificates for individuals*

### Service digital identities

**X509SubjectName**

**Subject CN:** *ANCERT Certificados Notariales Personales*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *pRJ/t0PbUSlnxnaV6u/Z43XFwTU=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2004-11-25T00:00:00Z*

### 3.7.4.2 - Extension (critical): Qualifiers [QCStatement]

**Qualifier type description** [ en ] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[ es ] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne**



**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Valid from:** *Tue Feb 22 11:34:42 CET 2011*

**Valid to:** *Mon Feb 22 11:34:43 CET 2021*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100AC665D46B2DA194B6D27C9E8518ACB3C8C5B1A3DDC8AF5E7C9FA5C3AED3C6382ED  
A1EEAF8F125586E08D046020EE53D0E703316C7331E88E34D572E0C734D995D9C8CEC07A16177B8068037911ACD77D343E620420E8D2831F575D7123123D43D752ABA  
6A302263D4D29BFC6A65F386F30B3FC72B47C803402CA7D187A6B4904251F5C8009DE93E89203F925149FC5ABD1A3B6E6EEDF8FC891549C01A848F64A30342378AA  
43103487DEFF63519830F24657BFA8B3E9D6E31C9E3193B3797D3D453E1FC53BE2CB117C6F28747E34D54C707922E15056E996C88DEA828254FDC7119A45ED375  
6FD979C01C8B1E9CB8746EC27724E04F16C2CDB389AC6DEB5590203010001

**Authority Key Identifier** *84:F7:FA:72:5E:88:64:66:1D:28:8C:B0:77:BD:0C:6A:9F:4C:4D:62*

**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.1.3*  
*CPS pointer: <http://www.ancert.com/cps>*  
*CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certificacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]*

**CRL Distribution Points**  
*<http://www.ancert.com/crl/ANCERTNOT.crl>*  
*<http://www2.ancert.com/crl/ANCERTNOT.crl>*  
*<http://www3.ancert.com/crl/ANCERTNOT.crl>*

**Subject Alternative Name** *ancert@ancert.com*

**Subject Key Identifier** *51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *39:35:94:82:D2:AE:7D:F8:48:A1:E5:6D:E1:84:EB:9B:FA:B9:D9:83:09:C3:CD:2E:D0:97:A1:8C:B  
E:07:F2:40*

**Certificate fields details**

**Version:** *3*

**Serial Number:** *126356436681186619492921660190540379841*



**Subject Key Identifier** 51:1A:2B:6E:2F:CE:4A:38:5E:74:08:B6:51:EE:8C:37:5D:13:8C:AD

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 13:77:15:68:2F:A1:69:5F:25:EA:BC:C0:21:60:B7:2E:34:ED:9A:D3:E9:68:9E:17:7E:2A:E4:3F:83:3E:FC:13

**X509SubjectName**

**Subject CN:** ANCERT Certificados Notariales Corporativos

**Subject O:** Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

**Subject L:** Paseo del General Martinez Campos 46-6a planta

**Subject ST:** Madrid

**Subject C:** ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2018-02-15T01:00:00Z

**3.8.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

**3.8.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

**Qualifier type description** [en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.

[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne**



**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.3.2.1

**3.8.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

**3.8.4 - History instance n.1 - Status: granted**

**Service Type Identifier** http://uri.etsi.org/TrstSvc/Svctype/CA/QC

**Service Name**

**Name** [ en ] Qualified Notarial Certificates for legal person

**Name** [ es ] Certificados Notariales Reconocidos para personas jurídicas

**Service digital identities****X509SubjectName**

**Subject CN:** ANCERT Certificados Notariales Corporativos

**Subject O:** Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

**Subject L:** Paseo del General Martinez Campos 46-6a planta

**Subject ST:** Madrid

**Subject C:** ES

**X509SKI**

**X509 SK I** URorbi/OSjhedAi2Ue6MN10TjK0=

**Service Status** http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

**Status Starting Time** 2016-06-30T22:00:00Z

**3.8.4.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [ en ] undefined.

[ es ] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

**3.8.4.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18920.1.3.2.1

**3.8.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.8.5 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Notarial Certificates for legal person*

**Name** [ es ] *Certificados Notariales Reconocidos para personas jurídicas*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANCERT Certificados Notariales Corporativos*

**Subject O:** *Agencia Notarial de Certificación S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

Subject ST: Madrid

Subject C: ES

X509SKI

X509 SK I URorbi/OSjhedaI2Ue6MN10TjK0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2004-11-25T00:00:00Z

#### 3.8.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

#### 3.8.5.5 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in "Service digital identity" and further identified by the above (filters) information used to further identify under the "Sdi" identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.1.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.1.3.2.1

### 3.9 - Service (withdrawn): Qualified Certificates for the Spanish Notarial Council employees





**Subject CN:** *ANCERT Certificados para empleados*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Valid from:** *Thu Feb 12 16:03:47 CET 2004*

**Valid to:** *Sun Feb 12 16:03:39 CET 2012*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D7A084CCF50317B724936B4A7D802218E1524B014204E9353F6F1325A10D3A8E9B7768  
4005BF0E7D153028ABD94B816E2F85B2FC0246E0E057D127413C2BF8BA528009D2A5442723C8D0897874263936231C4CAF331D295850641D34D45E875C338830  
00418555A8932A13F2746BC960B156A3BF07232F58A6052457CECD91F59F08C275B46C38F96D51CC4CF50084A5A560FA80038618E4B17B47630F0E5B6707F0432D  
17EBBC092375C6BE5AEE3B99E911A4479EC5287E5B030AECFD95DE340C9A875D5B6A63303D29779559E9EC0832C6A89C792B080C44ED072D172BF7DC2E68CF4868  
E5B4E1854C332B6E5E3B64D31E031E1D1F8E1B6E2B43B01D90203010001

**Authority Key Identifier** *EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*

**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.4.2*  
*CPS pointer: <http://www.ancert.com/cps>*  
*CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]*

**CRL Distribution Points**  
*<http://www.ancert.com/crl/ANCERTCGN.crl>*  
*<http://www2.ancert.com/crl/ANCERTCGN.crl>*  
*<http://www3.ancert.com/crl/ANCERTCGN.crl>*

**Subject Alternative Name** *ancert@ancert.com*

**Subject Key Identifier** *56:3D:DB:0E:C5:F0:3D:D3:54:B0:03:A0:E1:FD:DB:67:9F:7D:09:AF*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *56:3D:81:58:24:D9:1A:E6:BA:83:AE:08:6A:B5:29:59:80:7D:51:09:8C:25:75:93:38:A3:7D:28:0E:7D:8B:A1*

**X509SubjectName**

**Subject CN:** *ANCERT Certificados para empleados*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2018-02-15T01:00:00Z

### 3.9.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.2.1.1

### 3.9.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 3.9.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] *Qualified Certificates for the Spanish Notarial Council employees*

**Name** [es] *Certificados Reconocidos para empleados del Consejo General del Notariado*

#### Service digital identities

##### X509SubjectName

**Subject CN:** ANCERT Certificados para empleados

**Subject O:** Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

### 3.9.3.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

<b>Qualifier type description</b>	<i>[en]</i>	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	<i>[es]</i>	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

#### **Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

### 3.9.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 3.9.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en]* *Qualified Certificates for the Spanish Notarial Council employees*

**Name** *[es]* *Certificados Reconocidos para empleados del Consejo General del Notariado*

### Service digital identities



**X509SubjectName**

**Subject CN:** *ANCERT Certificados para empleados*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Vj3bDsXwPdNUsAOg4f3bZ599Ca8=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2004-11-24T23:00:00Z*

**3.9.4.3 - Extension (critical): Qualifiers [QCStatement]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.</i>
	<i>[es]</i>	<i>está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.18920.4.2.1.1*

**3.10 - Service (withdrawn): Qualified Certificates for Public Corporations**

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

<b>Service type description</b>	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

**Service Name**

<b>Name</b>	<i>[ en ]</i>	<i>Qualified Certificates for Public Corporations</i>
<b>Name</b>	<i>[ es ]</i>	<i>Certificados Reconocidos para Corporaciones de Derecho Público</i>

Service digital identities

## Certificate fields details

Version:	3
Serial Number:	28596344023930227605525191007477744754
X509 Certificate	<pre>-----BEGIN CERTIFICATE----- MIIGPCCBSezAwIBAgIQFYNoVlMh8RutABCSTeajANBgkqhkiG9w0BAQsFADCBDELAAKAIE BHMCRVMsZSBJBgNVBAAOTkFnZW5uWzEgIm90YXpYVWZGZG9QZVdGImaWNBvY2l2b2hBTLkwaIFVn aXBkcnVmbmFsc0g0OGEHMLzMSNTk4ODRwMC4GA1UEAxMrQU5DRVJUIEUENvenBvenmFjaW9uZXMg ZGllZGVzZWNoY29kaWJsaWNBKDYwMDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0 BgNVBAYTAkVMO8wDQYzVWV0QWUwZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u cnRpbmV6IENhbnVycyADNjQyY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw Q2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw QU5DRVJUIEUENvenBvenmFjaW9uZXMgZGllZGVzZWNoY29kaWJsaWNBKDYwMDM0MjE0MDM0MjE0 MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0MjE0MDM0 MIIBIjANBgkqhkiG9w0BAQsFAAOCAQEAQ8AMIBGcKCAQEAxtUz5oF1QeggnwPAZP1OPMDdlvE 1JnaX7H2hu8S7D1m9Y4cK6Q7m5iIhmMg5o4bz2Maf6oXfYEXdzBYL8W7D01KmszZWR8N/ 11Ry1Nc-u7EAsWQesMc3VqBSuNstFHLHpmK8p7urVPk7nauLcWdatdaA1Eszab8YpQ 6abblhMgSV3MGNdaVm6C+7Fov1Sd3M7gZJQYIBuZb2TymVkwHfBPyoqpb1rvLxWzWQomms SYODAndz1hwclmZLanKoyUs4dITP1c8AQD1smDEIwTw5Bkw4Inlq59qhz1SSU13NLN dIBMQDAQABohfCPTCCAJkwHwYDVR0BBgwEwAUJEncwys9K8KAsogLFS90ZpUwEgYDVR0T AOHBAgwBgEwIBADCAQEA1UdlASCArweggEUMIBBEAYKkwYBBAGB2gDA1CCAAQAJQYKwYB BOHBAgwBgEwIBADCAQEA1UdlASCArweggEUMIBBEAYKkwYBBAGB2gDA1CCAAQAJQYKwYB VDAADAGBGoG3WdlbmNpYSB0b3RhcmlhbnCBKZSBDZXBkZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u biBKZSbWcmFjdGijYXMGZGllZGVzZWNoY29kaWJsaWNBKDYwMDM0MjE0MDM0MjE0MDM0MjE0 IGRIRchIBZANBmIUR1d09wWkZCZSBJbmVJZW50cmFzZG9uWzZSb2hBbHRw O8wD43LmFuY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw Y2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw O0VSFBV05cmGKChdHAGL9y3d3cyLmFuY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw VROPQHBAAQDAGGMBwGA1UdEQQVAMBOEwFuY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2VwY2Vw N6S0zpa2CBohl69lrkDANBgkqhkiG9w0BAQsFAAOCAQEAARlw1h2jwDGArzgdPiqob7XFp0 HwFpVz1NS1ElaRq5LnsqwkPBNcXKZDdJfBHV2ny0b409wWeyNstEz0zK4enTSI pWEMSiW-6V-XzkTg61bNp-NvVGHINBc5Pvcr5SH6K-NugTev8W1VovBZVWRc7agCqWtGnK0j 4Y+6B33DYtpa9+MyqWnJ+ModLcteg0fjG6vQTNOSBaT5GmKclF1k0a61AEJrWdEdM0z/T ZLNGp6808SLgXuUnlRAC++WA02FN4h157n25V8NvCDBq52y2gkLppwCx2D38n8IGTKIDq cXlqWAG0E= -----END CERTIFICATE-----</pre>
Signature algorithm:	SHA1withRSA
Issuer CN:	ANCERT Corporaciones de Derecho Publico
Issuer O:	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988
Issuer C:	ES
Subject CN:	ANCERT Certificados para Corporaciones de Derecho Publico
Subject O:	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988
Subject L:	Paseo del General Martinez Campos 46-6a planta
Subject ST:	Madrid
Subject C:	ES
Valid from:	Thu Feb 12 15:44:34 CET 2004
Valid to:	Wed Feb 12 15:44:26 CET 2014
Public Key:	<pre>30820122300D06092A8648867FD01010105000382010F003082010A028201010006C6D49333E6814842881C9F03ED03B8F33F540F30765BC4D75A6E017EE51D96EE052C CF0D39BD558A02E904E99FE657C798C824CA8A01BA9931A7FAA1715811795DC1614F16A3D3590A9B6C595B37F975472D4D73E8B140C56E907AC331DE355D23 CFE1271EAEAC51CB1E9B8E420B3BBA854F91B77BA9A51C59D6ADAD1D6BF05312C66E6E8D18A90E9A6DB5213204954C18D75A566E82FB168BD449DDCCEEE819F C94182017E1663B8764F99324C0715B3D8A2AE98754EEF2F15B35904209AC1656E6C09DD7F3D61C1C2DE309DB56A4E2A8C94B387F57533D40712500F5A1B5032372 16B70481930FE452752AE7DC606F3D79F12B4DCD2CD8647C1310203010001</pre>
Authority Key Identifier	8C:4C:1E:37:0C:B1:9F:D2:AC:44:0B:3A:BE:02:CF:F4:8D:2D:66:95
Basic Constraints	IsCA: true - Path length: 0

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.18920.3.1

CPS pointer: <http://www.ancert.com/cps>CPS text: *[[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certificacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]***CRL Distribution Points**<http://www.ancert.com/crl/ANCERTPUB.crl><http://www2.ancert.com/crl/ANCERTPUB.crl><http://www3.ancert.com/crl/ANCERTPUB.crl>**Subject Alternative Name**

ancert@ancert.com

**Subject Key Identifier**

90:8C:75:66:37:AE:74:23:3A:5A:D8:27:C1:A2:56:CB:EB:D5:2B:90

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

60:66:75:6C:46:17:4D:9A:4F:CB:86:86:73:35:86:51:87:F8:A4:96:BD:EF:A4:6A:FB:DA:B2:9A:18:70:B6:B4

**X509SubjectName****Subject CN:**

ANCERT Certificados para Corporaciones de Derecho Publico

**Subject O:**

Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988

**Subject L:**

Paseo del General Martinez Campos 46-6a planta

**Subject ST:**

Madrid

**Subject C:**

ES

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2016-06-30T22:00:00Z

**3.10.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]****Qualifier type description**[en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.***Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.3.1.1.1

**3.10.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**3.10.3 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates for Public Corporations*

**Name** [es] *Certificados Reconocidos para Corporaciones de Derecho Público*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANCERT Certificados para Corporaciones de Derecho Publico*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *kIx1ZjeudCM6WtgnwaJWy+vVK5A=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2015-03-09T23:00:00Z*

**3.10.3.1 - Extension (critical): Qualifiers [QCStatement]**

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es]

está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.3.1.1.1

### 3.10.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] *Qualifed Certificates for Public Corporations*

**Name** [es] *Certificados Reconocidos para Corporaciones de Derecho Público*

#### Service digital identities

#### X509SubjectName

**Subject CN:** *ANCERT Certificados para Corporaciones de Derecho Publico*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *kIx1ZjeudCM6WtgnwaJWy+vVK5A=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2004-11-25T00:00:00Z*

### 3.10.4.2 - Extension (critical): Qualifiers [QCStatement]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*



**Subject CN:** *ANCERT Certificados FERN*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Valid from:** *Thu Feb 12 15:53:10 CET 2004*

**Valid to:** *Wed Feb 12 15:53:02 CET 2014*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100924F8214E3C1789257AA0E42899D6483CC90B2E75ADCB1A5DF2FA35C3F1745E66A69  
30F401D3BA8AA23D6C334B62CF0A7D95B87A175A719FA05D196C6620F249AB8568A5DF3E9423B3C209CA9ACAB2B59BD767DCD3B332E742F9EC3F579EE508453C9  
6BEE89B2DE3F32DE07053C4BE23A9629E26C5DF3098A88B4A572E90E3EAI7AC792C5B13171AC4F0C424FB477FB0E0981CB8744B038BCBE888C22371EB7B75F17  
251A937BC48638D2B5F9FBBE833AB994BD4AFC17507FB38FB0616E531BE50965AF63CF316EC7A0A421CAFC069F1F1403DAEF984488101EFC38F2CBBAS1E25F0  
5B55F38D4AF7866487BAF820623D576144C9ECF3BD8328ACBD11950203010001

**Authority Key Identifier** *EC:57:9F:C8:76:22:6F:CC:3A:AE:5B:F0:2D:A1:62:58:D1:8D:02:CC*

**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18920.4.1*  
*CPS pointer: <http://www.ancert.com/cps>*  
*CPS text: [[ANCERT, [1]], Agencia Notarial de Certificacion. La declaracion de practicas de certifiacion que rige el funcionamiento de la presente autoridad se encuentra disponible en <http://www.ancert.com/cps>]*

**CRL Distribution Points**  
*<http://www.ancert.com/crl/ANCERTCGN.crl>*  
*<http://www2.ancert.com/crl/ANCERTCGN.crl>*  
*<http://www3.ancert.com/crl/ANCERTCGN.crl>*

**Subject Alternative Name** *ancert@ancert.com*

**Subject Key Identifier** *99:E5:5C:82:BA:18:E5:8C:F7:88:1B:DE:D0:C2:AD:6D:46:B2:B8:A6*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *76:C5:27:32:7D:E2:A2:E3:CD:8C:1B:A8:58:2E:EB:C7:18:88:E1:13:06:01:9F:D8:7F:18:D7:7E:55:FC:85:4E*

**X509SubjectName**

**Subject CN:** *ANCERT Certificados FERN*

**Subject O:** *Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988*

**Subject L:** *Paseo del General Martinez Campos 46-6a planta*

**Subject ST:** *Madrid*

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

### 3.11.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

#### Criteria list assert=atLeastOne

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.1.1.1

### 3.11.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 3.11.3 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Spanish Notaries Qualified Certificates

**Name** [es] Certificados Reconocidos de Notario

#### Service digital identities

##### X509SubjectName

**Subject CN:** ANCERT Certificados FERN

**Subject O:** Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988



**Subject L:** Paseo del General Martinez Campos 46-6a planta

**Subject ST:** Madrid

**Subject C:** ES

**X509SKI**

**X509 SK I** meVcgroY5Yz3iBve0MKtbUayuKY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** 2015-03-09T23:00:00Z

### 3.11.3.1 - Extension (critical): Qualifiers [QCStatement]

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.1.1.1

### 3.11.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Spanish Notaries Qualified Certificates

**Name** [es] Certificados Reconocidos de Notario

### Service digital identities

#### X509SubjectName

**Subject CN:** ANCERT Certificados FERN

**Subject O:** Agencia Notarial de Certificación S.L. Unipersonal - CIF B83395988

**Subject L:** Paseo del General Martinez Campos 46-6a planta

**Subject ST:** Madrid

**Subject C:** ES

**X509SKI**

**X509 SK I** meVcgroY5Yz3iBve0MKtbUayuKY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2004-11-25T00:00:00Z

### 3.11.4.2 - Extension (critical): Qualifiers [QCStatement]

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18920.4.1.1.1

### 3.12 - Service (granted): Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [es] Sellos cualificados de tiempo emitidos por «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»

**Name** [en] Qualified Time Stamp issued by «ANCERT Qualified Time-stamp Authority G2 (TSA/TSU)»

**Service digital identities**

**Certificate fields details**

**Version:** 3

**Serial Number:** 1030803513657198470690908184875233618



**CRL Distribution Points**

*http://www.ancert.com/crl/ANCERTCS\_V2.crl*  
*http://www2.ancert.com/crl/ANCERTCS\_V2.crl*  
*http://www3.ancert.com/crl/ANCERTCS\_V2.crl*

**Subject Key Identifier**

*5A:A8:47:D1:6F:86:F3:86:AF:CD:FB:B1:9D:87:41:78:15:C0:E1:95*

**Subject Alternative Name**

*pki.explotacion@ancert.com*

**Key Usage:**

*digitalSignature*

**Thumbprint algorithm:**

*SHA-256*

**Thumbprint:**

*26:AE:01:6C:AC:51:81:94:43:93:AC:4E:06:0E:44:FD:AE:A1:34:7A:0C:18:D8:CC:B1:65:BF:80:EF:A5:80:AE*

**X509SubjectName****Subject CN:**

*ANCERT Qualified Time-stamp Authority G2*

**Subject 2.5.4.97:**

*VATES-B83395988*

**Subject O:**

*Agencia Notarial de Certificación S.L. Unipersonal*

**Subject C:**

*ES*

**X509SKI****X509 SK I**

*WqhH0W+G84avzfuxnYdBeBXA4ZU=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description**

*[en]*

*undefined.*

*[es]*

*undefined.*

**Status Starting Time**

*2020-10-23T02:00:00Z*

**4 - TSP: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)****TSP Name**

**Name** [ en ] *Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*

**Name** [ es ] *Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*

**TSP Trade Name**

**Name** [ en ] *VATES-Q2826004J*

**Name** [ en ] *CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*

**Name** [ es ] *CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM)*

**Name** [ en ] *FNMT*

**Name** [ es ] *FNMT*

**Name** [ en ] *FNMT-RCM*

**Name** [ es ] *FNMT-RCM*

**Name** [ en ] *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

**Name** [ es ] *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

**PostalAddress**

**Street Address** [ en ] *C/ Jorge Juan, 106*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28009*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ Jorge Juan, 106*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28009*

**Country Name** [ es ] ES

## ElectronicAddress

**URI** [ en ] http://www.cert.fnmt.es

**URI** [ en ] mailto:ceres@fnmt.es

## TSP Information URI

**URI** [ en ] http://www.cert.fnmt.es/en/home

**URI** [ es ] http://www.cert.fnmt.es

## 4.1 - Service (withdrawn): Qualified certificates for individuals issued by FNMT-RCM

### Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

**Service type description** [ en ] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[ es ] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

**Name** [ en ] Qualified certificates for individuals issued by FNMT-RCM

**Name** [ es ] Certificados reconocidos para personas físicas emitidos por la FNMT-RCM

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 921770777

#### X509 Certificate

-----BEGIN CERTIFICATE-----

```
MIC+TCCAmKgaW1BAglENvEGTANBekpkhG9w0BAQUFADA2M0swCQYDVQQGEwJFUzENMAAUAUIC
CHMERkSNVDEYMBYGAUUECmPRkSNVCBDBGZSAyIENBMB4XDTSMDMkxODE0NTYxOVVXDTESMDMx
ODEIMYxOVVwNjE1MAKGA1UEBmMCRVMAKDTALBgNVBAoTBEZ01VQzGDAWBgNVBAsTD0Z01VQzG2xh
c21gaMR0QzCBInANBgkqhkiG9w0BAQEFAAOBwwgwYCC2YEAmdPwGTePTT-dUUTV88qitmpY
40bQxcZa-WlhpFcrQwIbblNadHeBxkadfBj9cQusBvIwahfJC1uXJA7ly7GIM8quazK
08QeU/GdlUYyKz5JDBWkaodsQJCDU3zb07jD03M6GvYh0H0cCbrbrxm0AnVImfCAQOggEU
MIIBEDARBkphkgBwwCQEIBAMCAAcuWAYDVDR0BFEwTzBNoi0sgNRIMEUxZzAIBgNVBAYTAkVT
MQ0wCwYDVQQKEwRGTkRUMRgWfSYDVQQLAw9GTkRUIEUsYXN0IDg0OEJDTALBgNVBAMTBENSTDEw
KwYDVROBQCQwtoAPMTLS0TAAZMTG9uZDUMTgQ8MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5
MBRGAAUJdnQYMBR0FEcud8SxgI8EFTLHhIP0kVXMD8MBRGA1UEJ0gQWBRRAmZzE3gkxwI3y6N
TzpfDDXYTAMBgNVHRMERTADAQHMBGCSqGSIb2QJBAQMMAobbFY0LADAgSQAAGCqGSIb3
DQEBBQUAAAGBAGFmohZyYImm+0SIE8SDgEeSjXy1THa3NgRc8dN531jW5=agyuP9Q5wvolkF
sUly8Coc41dptPYXm2yZgXv0R86qzY-s1rT6o5ZjZlUwVMZGACok0eb4GozVU0ZEN8pdx
PqNHPcgr0W2nSIMlntLVsV=RIG3whd
```

-----END CERTIFICATE-----

**Signature algorithm:** SHA1withRSA

**Issuer OU:** FNMT Clase 2 CA

**Issuer O:** FNMT

**Issuer C:** ES

**Subject OU:** *FNMT Clase 2 CA*

**Subject O:** *FNMT*

**Subject C:** *ES*

**Valid from:** *Thu Mar 18 15:56:19 CET 1999*

**Valid to:** *Mon Mar 18 16:26:19 CET 2019*

**Public Key:** *30819D300D06092A864886F70D019101050003818B0030818702818100983FAD1936933D3EFE764214FD356F01FAAD227A58E346D05DC65AF9622D8F315EFE8430FE5074ACD69D1DED62C649DD14127D710BAC06C13FD70687ED9089D6E5E303B2F227B19F33C8AA6B364AA3C43F79419D89462F2B3E63D4383691AA1D810D42754DF3874E30F4DC8B46CBF621387EAD09B8EB6E2FF19F49409D59661020103*

**CRL Distribution Points** *C=ES,O=FNMT,OU=FNMT Clase 2 CA,CN=CRL1*

**Authority Key Identifier** *40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*

**Subject Key Identifier** *40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61*

**Basic Constraints** *IsCA: true*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *62:B9:26:72:66:21:28:32:A8:E2:2D:AB:93:3D:91:C7:01:12:74:AC:F7:17:03:F9:CC:97:83:37:51:A6:E9:4F*

## X509SubjectName

**Subject OU:** *FNMT Clase 2 CA*

**Subject O:** *FNMT*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2017-09-12T00:00:00Z*

## Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

## TSP Service Definition URI

URI [ en ] <http://www.ceres.fnmt.es/dpc>

URI [ es ] <http://www.ceres.fnmt.es/dpc>

#### 4.1.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.1.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

Name [ en ] *Qualified certificates for individuals issued by FNMT-RCM*

Name [ es ] *Certificados reconocidos para personas físicas emitidos por la FNMT-RCM*

##### Service digital identities

##### X509SubjectName

Subject OU: *FNMT Clase 2 CA*

Subject O: *FNMT*

Subject C: *ES*

##### X509SKI

X509 SK I *QJp2RJd0B8SsFMsejU86RXww12E=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

#### 4.1.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.1.3 - History instance n.2 - Status: undersupervision



<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service Name</b>		
<b>Name</b>	[ en ]	Qualified certificates for individuals issued by FNMT-RCM
<b>Name</b>	[ es ]	Certificados reconocidos para personas físicas emitidos por la FNMT-RCM

**Service digital identities****X509SubjectName**

<b>Subject OU:</b>	FNMT Clase 2 CA
<b>Subject O:</b>	FNMT
<b>Subject C:</b>	ES

**X509SKI**

<b>X509 SK I</b>	QJp2RJd0B8SsFMsejU86RXww12E=
------------------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>
-----------------------	---

<b>Status Starting Time</b>	2004-11-25T00:00:00Z
-----------------------------	----------------------

**4.2 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service type description</b>	[ en ]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[ es ]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

<b>Name</b>	[ es ]	Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes
<b>Name</b>	[ en ]	Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities

**Service digital identities****Certificate fields details**

<b>Version:</b>	3
<b>Serial Number:</b>	16



**Subject OU:** AC APE

**Subject O:** FNMT-RCM

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

#### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### TSP Service Definition URI

**URI** [es] <http://www.ceres.fnmt.es/dpc>

**URI** [en] <http://www.ceres.fnmt.es/dpc>

#### 4.2.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.13

#### 4.2.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.2.3 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ es ] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*

**Name** [ en ] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

### Service digital identities

#### X509SubjectName

**Subject OU:** AC APE

**Subject O:** FNMT-RCM

**Subject C:** ES

#### X509SKI

**X509 SK I** Y0t0Wwe/6GbRWixfy/15bqCMric=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** 2016-05-29T22:00:00Z

#### 4.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

**Qualifier type description** [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[ es ] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA/ CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.5734.3.13

#### 4.2.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ es ] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes*

**Name** [ en ] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities*

Service digital identities**X509SubjectName**

Subject OU: AC APE

Subject O: FNMT-RCM

Subject C: ES

**X509SKI**

X509 SK I Y0t0Wwe/6GbRWixfy/15bqCMric=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2010-06-07T00:00:00Z

**4.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.5734.3.13

**4.3 - Service (withdrawn): Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

Name [ es ] Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles

Name [ en ] Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones



**X509SubjectName**

**Subject OU:** *AC FIRMA MOVIL*

**Subject O:** *FNMT*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2016-06-30T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**TSP Service Definition URI**

**URI** *[en]* *http://www.ceres.fnmt.es/dpc*

**URI** *[es]* *http://www.ceres.fnmt.es/dpc*

**4.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**4.3.2 - History instance n.1 - Status: supervisionceased****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[es]* *Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles*

**Name** *[en]* *Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones*

**Service digital identities****X509SubjectName**

**Subject OU:** *AC FIRMA MOVIL*

**Subject O:** *FNMT*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *89gczFvt/UcPQuPA3IRz1JlvSO8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

**Status Starting Time** *2015-02-24T23:00:00Z*

#### 4.3.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### Service Name

**Name** *[ es ]* *Certificados reconocidos para personas físicas emitidos en soporte tarjeta SIM para dispositivos y teléfonos móviles*

**Name** *[ en ]* *Qualified certificates for individuals issued in SIM smart-card for mobile devices and phones*

#### Service digital identities

#### X509SubjectName

**Subject OU:** *AC FIRMA MOVIL*

**Subject O:** *FNMT*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *89gczFvt/UcPQuPA3IRz1JlvSO8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2010-06-07T00:00:00Z*

#### 4.4 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*







**Issuer C:** ES  
**Subject CN:** AC Administración Pública  
**Subject SERIAL NUMBER:** Q2826004J  
**Subject OU:** CERES  
**Subject O:** FNMT-RCM  
**Subject C:** ES  
**Valid from:** Fri May 21 11:26:24 CEST 2010  
**Valid to:** Sat May 21 11:57:08 CEST 2022  
**Public Key:** 30820122300D06092A864886F70D01010105000382010F003082010A02820101009CA4FC375DCCE83D561E9BF2A7094DBE9F200BF2D2457D99A0D7C2F81F53FA0948C9  
F44D701F08077021460DF2DD08A1F45156FE8E8400F5955834E2C37E79E2BA5A997BF3B39288279E10F90608CBDF2D2F398F3C592D8677D1A0C432E317BF7CA7114F  
62FAD37B4F8B791E1E1A2CA8B6793B4815925919C1F4DD9BC872A6C7BE351EC3B1E2DC3CAE304DD989716C7037ECS516533D487077AB8BAB44FA92C365A7BA1C  
964798AC2785098E026AC08E0DF4D7F04863988BE59F500008EF2C7E7EA78A29054B17BD875792BC349863D01F5A31CF92880489A3F4338B85961021717E460A1F0A12  
397D67D39B02F91D099AE1EC41C9FDBF3D9E2D69BF3BACT0203010001  
**Basic Constraints** IsCA: true - Path length: 0  
**Subject Key Identifier** 14:11:E2:B5:2B:B9:8C:98:AD:68:D3:31:54:40:E4:58:5F:03:1B:7D  
**Authority Key Identifier** F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D  
**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.cert.fnmt.es/dpcs/>  
CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/ Jorge Juan, 106-28009-Madrid-España)]  
**Authority Info Access** <http://ocspape.cert.fnmt.es/ocspape/OcspResponder>  
<http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt>  
**CRL Distribution Points** <ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>  
<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>  
**Key Usage:** keyCertSign - cRLSign  
**Thumbprint algorithm:** SHA-256  
**Thumbprint:** 83:0F:F2:05:AE:69:48:50:59:C3:FB:23:76:A7:F2:F9:EE:1C:2A:61:DE:25:9D:D0:9D:0B:B6:AD:69:F8:88:32  
**X509SubjectName**  
**Subject CN:** AC Administración Pública  
**Subject SERIAL NUMBER:** Q2826004J  
**Subject OU:** CERES

**Subject O:** FNMT-RCM

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2022-10-10T00:00:00Z

#### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### TSP Service Definition URI

**URI** [en] <http://www.ceres.fnmt.es/dpc>

**URI** [es] <http://www.ceres.fnmt.es/dpc>

#### 4.4.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.3.2

#### 4.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.4.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**4.4.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.10.1

**Description****4.4.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**4.4.6 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

**Name** [en] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

**Service digital identities****X509SubjectName**

**Subject CN:** AC Administración Pública

**Subject SERIAL NUMBER:** Q2826004J

**Subject OU:** CERES

**Subject O:** FNMT-RCM

**Subject C:** ES

**X509SKI**

**X509 SK I** FBHitSu5JitaNMxVEDkWF8DG30=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2019-07-15T00:00:00Z

#### 4.4.6.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.  
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.3.2

#### 4.4.6.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.4.6.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 4.4.6.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.  
[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.3.10.1

Description

#### 4.4.6.5 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**4.4.7 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ es ]* *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

**Name** *[ en ]* *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Administración Pública*

**Subject SERIAL NUMBER:** *Q2826004J*

**Subject OU:** *CERES*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *FBHitSu5jJitaNMxVEDkWF8DG30=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2017-09-27T10:00:00Z*

**4.4.7.6 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.5734.3.3.3.2*

**4.4.7.7 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.4.7.8 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 4.4.7.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [ en ] undefined.  
[ es ] undefined.

##### Criteria list assert=atLeastOne

###### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.5734.3.3.10.1

###### Description

#### 4.4.8 - History instance n.3 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

Name [ es ] *Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)*

Name [ en ] *Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)*

##### Service digital identities

##### X509SubjectName

Subject CN: AC Administración Pública

Subject SERIAL NUMBER: Q2826004J

Subject OU: CERES

Subject O: FNMT-RCM

Subject C: ES

##### X509SKI



**X509 SK I**

FBHitSu5jJitaNMxVEDkWF8DG30=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2016-06-30T22:00:00Z

**4.4.8.10 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.5734.3.3.3.2
------------	------------	----------------------------------

**4.4.8.11 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	------	---

**4.4.9 - History instance n.4 - Status: undersupervision****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

Name	[es]	Certificados reconocidos para su uso en el ámbito de organización y funcionamiento de las Administraciones Públicas, sus organismos y entidades vinculadas o dependientes (nueva AC)
------	------	--

Name	[en]	Qualified certificates issued for the use in public administrations, government bodies and dependent or bound entities (new CA)
------	------	---

**Service digital identities****X509SubjectName**

Subject CN:	AC Administración Pública
-------------	---------------------------

Subject SERIAL NUMBER:	Q2826004J
------------------------	-----------

Subject OU:	CERES
-------------	-------

Subject O:	FNMT-RCM
------------	----------

Subject C:	ES
------------	----

**X509SKI****X509 SK I**

FBHitSu5JitaNMxVEDkWF8DG30=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2011-07-27T00:00:00Z

**4.4.9.12 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier**

[ OIDsURN ]

urn:oid:1.3.6.1.4.1.5734.3.3.3.2

**4.5 - Service (withdrawn): Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name****Name**

[ es ]

Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.

**Name**

[ en ]

Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.

**Service digital identities****Certificate fields details****Version:**

3

**Serial Number:**

4



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *05:2B:EB:BD:CD:5C:84:7B:FA:0F:6F:B0:EA:22:46:B5:5B:A9:EE:55:E0:2A:2D:48:0B:87:FC:2F:34:2C:84:43*

#### X509SubjectName

**Subject CN:** *ISA CA*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

#### Service Status

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

#### TSP Service Definition URI

**URI** *[en] http://www.ceres.fnmt.es/dpc*

**URI** *[es] http://www.ceres.fnmt.es/dpc*

#### 4.5.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 4.5.2 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### Service Name

**Name** *[es] Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

**Name** *[ en ]* *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

### Service digital identities

#### X509SubjectName

**Subject CN:** *ISA CA*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *R+34Y/CZr17+fg5cWMv+4jU3pr0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

**Status Starting Time** *2016-05-29T22:00:00Z*

### 4.5.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### Service Name

**Name** *[ es ]* *Certificados reconocidos para su uso en el ámbito de competencias de las organizaciones establecidas en el marco de la Comisión Europea.*

**Name** *[ en ]* *Qualified certificates to be used in the area of competence of the organizations established in the framework of the European Commission.*

### Service digital identities

#### X509SubjectName

**Subject CN:** *ISA CA*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *R+34Y/CZr17+fg5cWMv+4jU3pr0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2011-07-27T00:00:00Z*



<b>Valid to:</b>	<i>Sun Oct 28 12:48:58 CET 2029</i>	
<b>Public Key:</b>	<pre> 30820122300D06092A864886F70D010105000382010F003082010A02820101009D2004262DFB2D6930CB09937FAS5EAE47072EF94BE456BE58FB20BF9BA538625AF 86F1C0D8DB063FB8E71BE8905A6FD0321E192D5522016BE7626217EC14C5955A090E952CCD20FA933CA3A68D8B4BD0426EA16DC06E90CD6491151601289640A8E75 C1728C8CEECE427C9C08037895D9F6DE791E1800E9ACFF59AA9B42D292B5A3C3095817D567F1AAA8FDE0274FF77C29D602E59FFD31CD5ACD61D637BCC9E8C4D DB99F4F7158CC9BBDD22E21DAA2180452E7F7BF5BCB6DDA731E8DABBA8B3E31E46281A17F67EDD6D42A6268ECF62720C0F868CCBCB2D73CD7632D07A1E167B38 6E2D8DF8C0539A97F8BC1D938AE81CB7312D94942B235E11E1CDAA9B0470203010001 </pre>	
<b>Basic Constraints</b>	<i>IsCA: true - Path length: 0</i>	
<b>Subject Key Identifier</b>	<i>B1:D4:4F:C4:23:79:FA:44:05:09:C6:EB:39:CF:E8:35:B0:B8:20:64</i>	
<b>Authority Info Access</b>	<i>http://ocspfnmtcmca.cert.fnmt.es/ocspfnmtcmca/OcspResponder</i> <i>http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt</i>	
<b>Authority Key Identifier</b>	<i>F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D</i>	
<b>Certificate Policies</b>	<i>Policy OID: 2.5.29.32.0</i> <i>CPS pointer: http://www.cert.fnmt.es/dpcs/</i> <i>CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/ Jorge Juan, 106-28009-Madrid-España)]</i>	
<b>CRL Distribution Points</b>	<i>ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint</i> <i>http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl</i>	
<b>Key Usage:</b>	<i>keyCertSign - cRLSign</i>	
<b>Thumbprint algorithm:</b>	<i>SHA-256</i>	
<b>Thumbprint:</b>	<i>60:12:93:CA:20:B0:9A:03:29:5D:19:62:56:C6:95:3F:F9:EB:A8:11:DB:8E:3C:E1:40:41:3C:1B:FF:E9:A8:69</i>	
<b>Service Status</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>	
<b>Service status description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>
<b>Status Starting Time</b>	<i>2016-06-30T22:00:00Z</i>	
<b>Scheme Service Definition URI</b>		
<b>URI</b>	<i>[en]</i>	<i>https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
<b>URI</b>	<i>[es]</i>	<i>https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</i>
<b>TSP Service Definition URI</b>		
<b>URI</b>	<i>[en]</i>	<i>https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion</i>
<b>URI</b>	<i>[es]</i>	<i>https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion</i>

**4.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**4.6.2 - History instance n.1 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates for individuals issued by AC FNMT Usuarios*

**Name** [ es ] *Certificados Reconocidos para personas físicas emitidos por AC FNMT Usuarios*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC FNMT Usuarios*

**Subject OU:** *Ceres*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *sdRPxCN5+kQFCcbrOc/oNbC4IGQ=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2015-01-01T23:00:00Z*

**4.7 - Service (granted): Qualified certificates issued by AC Representación**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [ en ] *Qualified certificates issued by AC Representación*





**Authority Key Identifier** *F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://www.cert.fnmt.es/dpcs/>*  
*CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/ Jorge Juan, 106-28009-Madrid-España)]*

**CRL Distribution Points** *ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint*  
*<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *8F:D1:6A:17:99:44:D5:D1:D4:20:AF:09:40:5E:DA:7A:BF:2A:9C:74:28:83:E8:C2:F8:9E:0D:90:A  
F:AF:75:4B*

**X509SubjectName**

**Subject CN:** *AC Representación*

**Subject OU:** *CERES*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time***2023-02-06T00:00:00Z***Scheme Service Definition URI**

**URI** *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**4.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**4.7.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**4.7.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates issued by AC Representación*

**Name** [ es ] *Certificados Reconocidos emitidos por AC Representación*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Representación*

**Subject OU:** *CERES*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *3FCWn9cxickR5O+WX/ZfglJGYIM=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**4.7.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**4.7.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by AC Representación*

**Name** *[ es ]* *Certificados Reconocidos emitidos por AC Representación*

### Service digital identities

#### X509SubjectName

**Subject CN:** *AC Representación*

**Subject OU:** *CERES*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *3FCWn9cxickR5O+WX/ZfgIJGYIM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2015-08-30T22:00:00Z*

## 4.8 - Service (granted): Qualified Certificates issued by AC Componentes Informáticos

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[ en ]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[ es ]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** *[ en ]* *Qualified Certificates issued by AC Componentes Informáticos*

**Name** *[ es ]* *Certificados cualificados emitidos por AC Componentes informáticos*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *70151399191966231374477229323776743104*



**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F0:38:42:1F:07:F2:0D:63:A2:0D:36:91:E5:A1:78:AB:84:59:EB:E5:70:C1:64:7B:76:90:55:4E:F2:38:76:AB*

#### X509SubjectName

**Subject OU:** *AC Componentes Informáticos*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *GfhYLxTWpsybBJgIDUzXqwCng2U=*

#### Service Status

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-02-28T00:00:00Z*

#### Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

#### 4.8.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

#### 4.8.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

#### 4.8.3 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** [ en ] *Qualified Certificates issued by AC Componentes Informáticos*

**Name** [ es ] *Certificados cualificados emitidos por AC Componentes informáticos*

**Service digital identities****X509SubjectName**

**Subject OU:** *AC Componentes Informáticos*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *GfhYLxTWpsybBJgIDUzXqwCng2U=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time**

*2017-09-12T00:00:00Z*

**4.8.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**4.9 - Service (withdrawn): Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** [ en ] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[ es ] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.*

**Service Name**

**Name** [ en ] *Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

**Name** [ es ] *Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

**Service digital identities****Certificate fields details**

Version:

3

Serial Number:

28295960146001875498465664804547762024

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIH5jCCB6gAwIBAgIQFVma8U48sYOCYXcCaDANBgkqhkiG9w0BAQsFAADBMQswCjYwMDQ...
-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer OU:

AC Componentes Informáticos

Issuer O:

FNMT-RCM

Issuer C:

ES

Subject CN:

AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016

Subject 2.5.4.97:

VATES-Q2826004J

Subject OU:

CERES

Subject O:

FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA

Subject C:

ES

Valid from:

Fri Nov 25 13:04:39 CET 2016

Valid to:

Fri Nov 25 13:04:39 CET 2022

Public Key:

30:82:01:A2:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:8F:00:30:82:01:8A:02:82:01:81:00:AC:06:08:99:CC:43:32:0A:6A:5A:CS:56:2F:7A:44:07:25:DF:B6:F9:C4:F4:9F:3F:16:46:FD:EE:0E:79:2E:45:9D:A9:...

Basic Constraints

IsCA: false

Authority Info Access

http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder

http://www.cert.fnmt.es/certs/ACCOMP.cert



**Certificate Policies** Policy OID: 1.3.6.1.4.1.5734.3.9.20  
 CPS pointer: <http://www.cert.fnmt.es/dpcs/>  
 CPS text: [Certificado para el Servicio Cualificado de Sellado de Tiempo de la FNMT-RCM. Sujeto a las condiciones de uso expuestas en la DPC de la FNMT-RCM (C/Jorge Juan 106-28009-Madrid-España)]

**Extended Key Usage** id\_kp\_timeStamping

**Subject Key Identifier** A1:F6:70:6D:CC:7E:8D:3B:CC:3C:93:E2:DE:94:9B:B1:45:9F:1F:9F

**QCStatements - crit. = false** id\_etsi\_qcs\_QcCompliance  
 id\_etsi\_qcs\_RetentionPeriod: 15

**Authority Key Identifier** 19:F8:58:2F:14:D6:A6:CC:9B:04:98:08:0D:4C:D7:AB:00:A7:83:65

**CRL Distribution Points** ldap://ldapcomp.cert.fnmt.es/CN=CRL1,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint  
<http://www.cert.fnmt.es/crlscomp/CRL1.crl>

**Key Usage:** digitalSignature - nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 08:F2:93:4C:39:4D:89:DD:B0:CF:C3:86:AA:F5:C5:2E:4F:17:AF:BB:BE:1C:67:A0:36:11:13:2F:80:BE:B7:A9

**X509SubjectName**

**Subject CN:** AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016

**Subject 2.5.4.97:** VATES-Q2826004J

**Subject OU:** CERES

**Subject O:** FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA

**Subject C:** ES

**X509SKI**

**X509 SK I** ofZwbcx+jTvMPJPi3pSbsUWfH58=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2023-02-28T00:00:00Z

**4.9.1 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

### Service Name

**Name** [en] *Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

**Name** [es] *Sellos de tiempo cualificados emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2016*

### Service digital identities

#### X509SubjectName

**Subject CN:** *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2016*

**Subject 2.5.4.97:** *VATES-Q2826004J*

**Subject OU:** *CERES*

**Subject O:** *FÁBRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *ofZwbcx+jTvMPJPi3pSbsUWfH58=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2017-09-12T00:00:00Z*

## 4.10 - Service (granted): Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

### Service Name

**Name** [en] *Qualified Certificates issued by AC SERVIDORES SEGUROS TIPO1*

**Name** [es] *Certificados cualificados emitidos por AC SERVIDORES SEGUROS TIPO1*

### Service digital identities

#### Certificate fields details

**Version:** 3



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *1E:DB:6B:D9:12:74:88:2D:B7:95:BF:C5:14:F8:AA:BE:10:AD:95:5C:BC:CF:D3:FD:5A:5B:5F:EB  
:B2:CE:5B:68*

**X509SubjectName**

**Subject CN:** *AC SERVIDORES SEGUROS TIPO1*

**Subject 2.5.4.97:** *VATES-Q2826004J*

**Subject OU:** *Ceres*

**Subject O:** *FNMT-RCM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jEIyQPI5P2sTwXXGXe6GIkQ5b3c=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2019-07-15T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**4.10.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**4.11 - Service (granted): Servicio Cualificado de certificados de sello emitidos por “AC Unidades de Sellado de Tiempo”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*



**Public Key:**

30820222300D06092A864886F70D01010105000382020F003082020A0282020100C846B418214B778FE418DD1F0B82C5C1196C821263ACA E64D06CA3BD3EF34717A435  
96D06773CEECDD0C530B781FE8C20655B6E00D2A2338F72A9CA BF924E4F80116B1F EA521832A8280A79329B08A2D6DF91042D3F0F4DD48606C9C3614186A5DC436  
E8FB9063B579D6978A C2404078FE47A688E1ED A1E8382170C9C39EF142BF EFBD771EFCBED010D88B9A3F3C57836421D9E1A3A1D0B8DBCB396FC7F7C8E C276E56  
A3B6047608F84E28936CBED7960CE6860D99543D83478B8676BAD26F2DD864401321C19AD873F63BAF58DE7519B8895E74E20A0775B5852A11ABB85905787FD9AE72  
01296CC21308CD1F7CC08DEA8A3BE26E49F1990D97CF2CF4B40C2A5BFC952F46396169DD9CBF55C7E8F3A3C4ACAEFBEB346455BB629169B8A669E35578A20854  
3AF905C0CB1B0A920F5576DABC04FAC334C6F4BE1DD6E3187B6DA5D8B1BBA33886B01B46067280561501E2E2C65DEA849D56D30D71C72E0034804075A00C03F7  
D887C8ED7593C6A26E378A07DC5C9AE10AEF2AE4E7B8B3F969B0BA21889668E0E44A81CF A7F00E2E65C31E59798923960D24D429E2D86D0F994584F9783293DB56  
E9869B53C634C10C441BBE5EA3795CB58D7F4032B00DE36E42A9D928FE2144B87F92B784A4273A5FE B4D946218F FD8A2523C508627084D49DD91310200C68E8267F  
E1B5178D735B46766BF9533480E223E3B1CCEA30203010001

**Basic Constraints**

IsCA: true - Path length: 0

**Authority Info Access**

<http://ocspfnmtcmca.cert.fnmt.es/ocspfnmtcmca/OcspResponder>

<http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt>

**Subject Key Identifier**

40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5

**Authority Key Identifier**

F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS pointer: <http://www.cert.fnmt.es/dpcs/>

CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/ Jorge Juan, 106-28009-Madrid-España)]

**CRL Distribution Points**

<ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>

<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

9C:E6:30:B3:5F:8A:E2:C6:41:9E:73:4A:D9:D2:FA:30:47:6D:D9:E7:39:4B:1E:93:B2:7F:83:F7:76:A0:24:EA

**X509SubjectName****Subject CN:**

AC Unidades de Sellado de Tiempo

**Subject 2.5.4.97:**

VATES-Q2826004J

**Subject OU:**

Ceres

**Subject O:**

FNMT-RCM

**Subject C:**

ES

**X509SKI****X509 SK I**

QLIVBKhpF2CQ7RGVJcMI+lr0hdU=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2020-06-15T22:00:00Z



**Issuer OU:** AC RAIZ FNMT-RCM

**Issuer O:** FNMT-RCM

**Issuer C:** ES

**Subject CN:** AC Sector Público

**Subject 2.5.4.97:** VATES-Q2826004J

**Subject OU:** Ceres

**Subject O:** FNMT-RCM

**Subject C:** ES

**Valid from:** Thu Nov 28 09:48:09 CET 2019

**Valid to:** Wed Nov 28 09:48:09 CET 2029

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201008897B53908F91C10B4BBE3C4A523248E869DF860AFEDC73D64108C1DFA95A32495D11  
F406B15C80E4965D41F5B0610A8D116E4EA89ED7C4C904C4556DEB2F7F1893897D338F172CA CED39BB8F330E0B0934632F94299839E846B771242D45C9BEA923F9  
58FA0D6FC8014C5F3C1BBD67D3D0F8D94939EF7E9D5D4ADBE2040E343C2CC14E9C741650119A3AE6FC95E9999CC78644E0585C458DAE68F2DF01235703715AF693  
7D8C51C3D49B1EA7E0387A0B9002E432C84D33A0821909C795D1811FD3CAFBEC45D3F5C76F79EFAB619690186A5FC70BB43B381A0694A204BE0C73A3C325A  
A1E94FC41FE66B789C0FE68036206B776C77CC29624D4C5E1C0F2FC88F9A757618A72D003011DD811C38E3C22578E7E5039D3434268C704B0988BC18BE6E5E278  
3595D4885E742C1DC8A8A00F75E3906D2F9C58D9EB3E642388B18AFC2FDSF99254EEAC03F994A2E57A846B61B5277CBA852D592919A38EDB0CCCA83AD7D60425E  
680F29BA79CF2398D22B99F7248B157AC7D8D1FBEAD0389AE15DCD2EF633E73A66AD6E57509A753FB0B8A1B4655CA8334E73C4E46E01F831F85567D9CB4FA  
5B388E7385DF41C4E27CC93D85C64458F230E56C651A252E5847CEBD58B5AD82338C97779D745237BEBEBC5C1DS972EAC772F48D7B0CC38330B2E1AA7F2F4752C96B  
05CCEFEF35B98D86CE4671EC7685E78E87AC81A4DA210203010001

**Basic Constraints** IsCA: true - Path length: 0

**Authority Info Access**  
<http://ocspfnmtcmca.cert.fnmt.es/ocspfnmtcmca/OcspResponder>  
<http://www.cert.fnmt.es/certs/ACRAIZFNMT.crt>

**Subject Key Identifier** E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C

**Authority Key Identifier** F7:7D:C5:FD:C4:E8:9A:1B:77:64:A7:F5:1D:A0:CC:BF:87:60:9A:6D

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.cert.fnmt.es/dpcs/>  
CPS text: [Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de la FNMT-RCM ( C/ Jorge Juan, 106-28009-Madrid-España)]

**CRL Distribution Points**  
<ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint>  
<http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 82:65:75:6D:D5:CD:8A:37:EE:61:E4:03:51:28:8E:4B:16:A8:9D:D2:48:C1:EC:4E:BA:25:AA:F1:61:AB:F4:98

**X509SubjectName**



Subject CN: AC Sector Público

Subject 2.5.4.97: VATES-Q2826004J

Subject OU: Ceres

Subject O: FNMT-RCM

Subject C: ES

**X509SKI**

X509 SK I 5wTucJERkkT5DpKPVvkMeBx2/BJw=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

**Status Starting Time**

2020-07-28T00:00:00Z

**Scheme Service Definition URI**

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**4.12.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.17.5

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.5734.3.17.6

**Description****4.12.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 4.12.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 4.12.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

Name [ es ] *Servicio Cualificado de certificados emitidos por “AC Sector Público”*

Name [ en ] *Qualified Certificates issued by “AC Sector Público”*

##### Service digital identities

##### X509SubjectName

Subject CN: *AC Sector Público*

Subject 2.5.4.97: *VATES-Q2826004J*

Subject OU: *Ceres*

Subject O: *FNMT-RCM*

Subject C: *ES*

##### X509SKI

X509 SK I *5wTucJERkkT5DpKPVkMeBx2/BJw=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2020-06-15T22:00:00Z*

#### 4.12.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [ en ] *undefined.*

[ es ] *undefined.*

Criteria list assert=**atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.5734.3.17.5

**Description****4.12.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**4.12.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**4.13 - Service (granted): Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [ en ] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[ es ] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [ es ] Sellos cualificados de tiempo emitidos por Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020

**Name** [ en ] Qualified timestamps issued by Autoridad de Sellado de Tiempo FNMT-RCM TSU 2020

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 106110774237859830093543854131413521392



**Authority Key Identifier** *40:B9:55:04:A8:4F:7F:60:90:ED:11:95:25:C3:25:FA:5A:F4:85:D5*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://www.cert.fnmt.es/crlsacst/CRL.crl*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.5734.3.18.1*  
*CPS pointer: http://www.cert.fnmt.es/dpcs/*  
*CPS text: [Certificado cualificado de sello electrónico para TSU. Sujeto a las condiciones de uso expuestas en DPC de FNMT-RCM, NIF: Q2826004-J (C/Jorge Juan 106-28009-Madrid-España)]*  
*Policy OID: 0.4.0.194112.1.1*

**Authority Info Access**  
*http://www.cert.fnmt.es/certs/ACST.crt*  
*http://ocspst.cert.fnmt.es/ocspst/OcspResponder*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *88:15:87:C2:7E:44:DC:07:DA:A3:92:D2:5B:CC:81:38:53:F2:03:63:46:31:65:86:86:87:EE:BC:DB:71:D7:55*

**X509SubjectName**

**Subject CN:** *AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020*

**Subject 2.5.4.97:** *VATES-Q2826004J*

**Subject OU:** *CERES*

**Subject O:** *FNMT-RCM*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *8Q53TQoy52mlkAAa5KAVz7uJANI=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2020-07-28T00:00:00Z*

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

## 5 - TSP: Consorci Administració Oberta de Catalunya - CAOC

### TSP Name

**Name** [ en ] *Consorci Administració Oberta de Catalunya - CAOC*

**Name** [ es ] *Consorci Administració Oberta de Catalunya - CAOC*

### TSP Trade Name

**Name** [ en ] *VATES-Q0801175A*

**Name** [ en ] *Consorci AOC (CATCert)*

**Name** [ es ] *Consorci AOC (CATCert)*

**Name** [ en ] *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Name** [ es ] *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Name** [ en ] *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

### PostalAddress

**Street Address** [ en ] *Calle Salvador Espriu, 45-51*

**Locality** [ en ] *L'Hospitalet del Llobregat*

**State Or Province** [ en ] *Barcelona*

**Postal Code** [ en ] *08908*

**Country Name** [ en ] *ES*

### PostalAddress

**Street Address** [ es ] *Calle Salvador Espriu, 45-51*

**Locality** [ es ] *L'Hospitalet del Llobregat*

**State Or Province** [ es ] *Barcelona*

**Postal Code** [ es ] *08908*

**Country Name** [ es ] *ES*

### ElectronicAddress

**URI** [ en ] *<http://www.aoc.cat>*

URI [en] mailto:info@aoc.cat

TSP Information URI

URI [en] http://www.aoc.cat

URI [es] http://www.aoc.cat

5.1 - Service (withdrawn): Qualified certificates issued by CA IdCAT

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en]

Qualified certificates issued by CA IdCAT

Name

[es]

Certificados Reconocidos emitidos por CA idCAT

Service digital identities

Certificate fields details

Version:

3

Serial Number:

149207157159073437715447019610265252046

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIHhDCCBpigaAwIBAgIQEBA0P3KPbKoywnYpwozjANBqkqhkiG9w0BAQUFADCB8zELMAGAIUE
BIMCRVMAZzA5bGVhbnRlbnRlLnVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
ODAxMjc2LURpMScwZDQ0Lm5ldCZ2ZjZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
CkMsbnVjYXNldGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
BKVUFDQ0eAefwMzEwMzZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
OzA5bGVhbnRlbnRlLnVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
LURpMTUyMDAwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDEwMDE
MSw4LmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
EyaWzWldSBodHRwczovLjM3ZDcyYXZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
RjU0eXNlbnRlbnRlLnVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
LUIEQF0MIIBjANBgkqhkiG9w0BAQEFAAOCAQMIBGCAOEAu99Aw9QEXkzypU83y67eE
RM1LSEGeAUcaA0GAYDFpya7Ka6p76wX30opXcldYdlVSVIZKZCpStVJWNBBMtrBezAPIX59p1cbH
4CvXsImaCvXUtkl0ppvc2yO490magp2cXak=7mKqkplp740RkRvozcJPF30YA
dgrSoLaOGDGIG+0maNbx+ydDVgMjphoO7Gxau9FALEZfsscg7FpkoXMR306lvaA63GAEmPeSs
0StJEW6hkZzRfPulMAG2h99XyF+lmpDzP6NwIHEP4g1S0mb6HFBxTicX1S6U/QkAs5hRROD
7XkCzr2Wk+rwQIDAQABoICTCAswIQDYDROSBBYwFlESZWNyWVw/QGNbG9NenQuhMvM0B9G
A1UdEQQYMBAwBgNVX2RyZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
AOhBAQDAgCMB0GA1UdDgQWB7TksBFRjR2dDldW60havPblYLiTCCATEGA1UdhwSCASggEGk
qB8g=HdggRb=YgFRKrim+gqB+8p89KTBzSLMAKGA1UdBHBMCRVMAZzA5bGVhbnRlbnRlLnVud
ZW5jaWw0ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
EyaWzWldSBodHRwczovLjM3ZDcyYXZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
LXNlbnRlbnRlLnVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
YXRzZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
ZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
gqE893EATCBEgYDVR0gBHMhMHPHMHMgsrlEAV4QMDDKBvDAsGggrgEFBQCARYgaHRO
+hM6L9y8Eca2F0Y2VudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
aWZpY2F0IH0SZWlKDEdbmJySBpIGV4Y2xlc2lyZWlbnQeYSBFbnRpdGF0cyBKZSBZDj0aWZp
Y2FjaMzGZGJgQzVhc3NlIDdlZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
MGGA1UdBHBMCRVMAZzA5bGVhbnRlbnRlLnVudGVudGVudGVudGVudGVudGVudGVudGVudGVud
bY0aHR0cDovL2Vwe2NmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
AAOCAAQEAgl7bMDZt19HLVyezaEH4KazVHUjRuyxwStFDBHw0006KAIEKbykww8SX-n
fwGvZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZmZm
iLD430G+JNgwEXFA9n3noXR2Hmi+EqLEbz=soT10Gbhj5qAg7DbAyh2DQ02D9fSIS/
Y5KXwEypesNqTj8dvwFGeBEUv2jgKbc76skulO3rdSo6np0dkZPRbdK10+scpp91B8tgbBNW
ZRtXsvgl0vRaudfQCxY4PF3WSWq7GaM.m2nzNqws9pmnA=
-----END CERTIFICATE-----
```

Signature algorithm:

SHA1withRSA

Issuer CN:

EC-ACC

Issuer OU:

Jerarquia Entitats de Certificacio Catalanes

Issuer OU:

Vegeu <https://www.catcert.net/verarrel> (c)03



**Issuer OU:** *Serveis Publics de Certificacio*

**Issuer O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Issuer C:** *ES*

**Subject CN:** *EC-IDCat*

**Subject OU:** *Entitat publica de certificacio de ciutadans*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Valid from:** *Fri Oct 31 11:40:39 CET 2003*

**Valid to:** *Thu Oct 31 11:40:39 CET 2019*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100BDFE40C3D41C117922CF2A54B3CDF2EBB78444CD4B48419E014780D1E180603169C9AEED29AE49EFA8D760ED29DC01274B57957564A0B33EC8525634104CB6B03CCC03C85F69D5C6C7902717BF12260025E34D422420FA69CB80B68EF48077FD0D89A83C3E04829E4FB8EE6B0A22A9DC97FA7BEE1F408F24CAB9C8C93C3E5F7D8B00760AD2A0B03A1831881BEED2668DD31FB274354CA9FA6178EEC63E7BAFF4500B11B65F9EC7AAEC5A64A1733CDF46D4967C40EB71801263DE4ACD12D49116EA5864DB346C3EE24C5F687DF57C9FFA5527A43CCFE883567ED10FE20D52D2C99BE891C3041C5322B3C8DFA5102646ACE617D1385ED78429BFD96ACABEB590203010001

**Issuer Alternative Name** *ec\_acc@catcert.net*

**Subject Alternative Name** *ec\_idcat@catcert.net*

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *CD:92:C0:45:46:34:76:0D:D2:F4:5B:A2:74:1D:AB:CF:6C:B6:0B:B9*

**Authority Key Identifier** *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*  
*CPS pointer: <https://www.catcert.net/verCIC-2>*  
*CPS text: [Aquest certificat semet única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-acc.crl>*  
*<http://epsd2.catcert.net/crl/ec-acc.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *95:4B:88:92:23:49:8A:ED:51:AA:7A:29:B6:2E:ED:24:BE:03:CD:48:1D:18:2E:03:EB:83:BA:E8:D  
D:7B:D7:1B*

**X509SubjectName**

**Subject CN:** *EC-IDCat*

**Subject OU:** *Entitat publica de certificacio de ciutadans*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2018-03-15T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es]* *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**5.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**5.1.2 - History instance n.1 - Status: granted****Service Type Identifier**

*<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service Name**

**Name** *[en]* *Qualified certificates issued by CA IdCAT*

**Name** *[es]* *Certificados Reconocidos emitidos por CA idCAT*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *EC-IDCat*

**Subject OU:** *Entitat publica de certificacio de ciutadans*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SKI** *zZLARUY0dg3S9FuidB2rz2y2C7k=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

**5.1.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**5.1.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by CA IdCAT*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA idCAT*

**Service digital identities****X509SubjectName**

**Subject CN:** *EC-IDCat*

**Subject OU:** *Entitat publica de certificacio de ciutadans*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *zZLARUY0dg3S9FuidB2rz2y2C7k=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2006-01-23T00:00:00Z*

## 5.2 - Service (withdrawn): Certificados Reconocidos emitidos por CA AL

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

### Service Name

**Name** *[es] Certificados Reconocidos emitidos por CA AL*

**Name** *[en] Qualified certificates issued by CA AL*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *81871235804792199700514938710945526542*



**Subject Key Identifier** *4C:EC:8D:49:D4:2B:02:03:9A:D0:48:30:0A:4B:6B:BD:31:7A:A6:34*

**Authority Key Identifier** *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*  
*CPS pointer: <https://www.catcert.net/verCIC-2>*  
*CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-acc.crl>*  
*<http://epsd2.catcert.net/crl/ec-acc.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *59:2C:50:8E:39:D7:66:5F:84:45:86:C3:B9:E7:65:AF:D5:D8:0B:BE:05:F9:28:9C:B0:DE:D5:71:1A:C9:C1:0A*

**X509SubjectName**

**Subject CN:** *EC-AL*

**Subject OU:** *Administracions Locals de Catalunya*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time***2018-03-15T01:00:00Z***Scheme Service Definition URI**

**URI** *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**5.2.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

### 5.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 5.2.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [es] *Certificados Reconocidos emitidos por CA AL*

**Name** [en] *Qualified certificates issued by CA AL*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *EC-AL*

**Subject OU:** *Administracions Locals de Catalunya*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**5.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

**5.2.3.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**5.2.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*



**Service Name**

**Name** [ es ] *Certificados Reconocidos emitidos por CA AL*

**Name** [ en ] *Qualified certificates issued by CA AL*

**Service digital identities****X509SubjectName**

**Subject CN:** *EC-AL*

**Subject OU:** *Administracions Locals de Catalunya*

**Subject OU:** *Vegeu https://www.catcert.net/verCIC-2 (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *TOyNSdQrAgOa0EgwCktrvTF6pjQ=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time**

*2010-05-05T00:00:00Z*

**5.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[ en ]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[ es ]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.2*

**Policy Identifier:**

**Identifier** [ OIDsURN ] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.2*



**Issuer OU:** *Serveis Publics de Certificacio ECV-1*

**Issuer O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Issuer C:** *ES*

**Subject CN:** *EC-SAFP*

**Subject OU:** *Secretaria d'Administracio i Funcio Publica*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Valid from:** *Wed Jan 08 14:01:10 CET 2003*

**Valid to:** *Mon Jan 07 23:59:59 CET 2019*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009923C6CA0B612EFFF0C1866464D449D75B9B7666500949BAAFCD E4228D1F2C3416978113  
51B090FB D4860E2177ED8F1B9E3D94B3FCAD5F4408094E339D8E27F84809717343AFEDD4AE020E96340A94C84E7A4A7F093E07FE921F923DB2590D19C5B F2D199  
3B9EA684FF0A34B59A3C3111864B309116FB20E4286A5FDA7E610939F95FA02D4BF75FD5E339153B0FD2113C4768A7B7F89C8237BB0A5AE5C709D8A37AD95D75  
1DB50141478F7F9F7C7E0B705F17EAA23373755E0EB634650CE093CAE432640C46E7DCE9E1FACCE2856E7812CACD553304058619518C75A879F42A718615A81FD24  
6136C583A6D42992166CE1313808B19BC1289A360D61B86890203010001

**Issuer Alternative Name** *ec\_gencat@catcert.net*

**Subject Alternative Name** *ec\_safp@catcert.net*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *05:B7:ED:4F:16:52:DD:FA:E6:92:C0:A2:72:79:56:60:54:C2:24:13*

**Authority Key Identifier** *31:6A:5C:0A:46:4E:37:AF:42:E3:B0:60:2B:0C:0F:2D:2F:93:DF:14*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*  
*CPS pointer: <https://www.catcert.net/verCIC-2>*  
*CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2.  
Vegeu <https://www.catcert.net/verCIC-2>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-gencat.crl>*  
*<http://epsd2.catcert.net/crl/ec-gencat.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *20:7C:EC:E0:38:B9:82:6A:12:0A:91:9D:4B:41:BC:A8:F3:7F:2E:99:46:21:BF:5A:99:3A:04:08:7D:  
55:6D:C6*

**X509SubjectName**

**Subject CN:** *EC-SAFP*

**Subject OU:** *Secretaria d'Administracio i Funcio Publica*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2018-03-15T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es]* *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**5.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en]* *undefined.*

*[es]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

**Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

**Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

### 5.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 5.3.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [es] *Certificados Reconocidos emitidos por CA SAFP*

**Name** [en] *Qualified certificates issued by CA SAFP*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *EC-SAFP*

**Subject OU:** *Secretaria d'Administracio i Funcio Publica*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *BbftTxZS3fmksCicnIWYFTCJBM=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

### 5.3.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1**Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1**Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1**Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2**5.3.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**5.3.4 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [es] *Certificados Reconocidos emitidos por CA SAFP***Name** [en] *Qualified certificates issued by CA SAFP***Service digital identities****X509SubjectName****Subject CN:** *EC-SAFP***Subject OU:** *Secretaria d'Administracio i Funcio Publica***Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03***Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *BbftTxZS3fkmksCicnIWYFTCJBM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2010-05-05T00:00:00Z*

#### 5.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

#### 5.4 - Service (withdrawn): Certificados Reconocidos emitidos por CA PARLAMENT

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

<b>Service type description</b>	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name [ es ] *Certificados Reconocidos emitidos por CA PARLAMENT*

Name [ en ] *Qualified certificates issued by CA PARLAMENT*

Service digital identities

Certificate fields details

Version: 3

Serial Number: 49921083824290425381953941137842983617

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHhmzCCBoOgAwIBAgIQY5zsdgDmG9A4oBuzdSwTANBgkqhkiG9w0BAQUFA...
-----END CERTIFICATE-----

Signature algorithm: SHA1withRSA
Issuer CN: EC-ACC
Issuer OU: Jerarquia Entitats de Certificacio Catalanes
Issuer OU: Vegeu https://www.catcert.net/verarrel (c)03
Issuer OU: Serveis Publics de Certificacio
Issuer O: Agencia Catalana de Certificacio (NIF Q-0801176-I)
Issuer C: ES
Subject CN: EC-PARLAMENT
Subject OU: Parlament de Catalunya
Subject OU: Vegeu https://www.catcert.net/verCIC-2 (c)03
Subject OU: Serveis Publics de Certificacio
Subject L: Passatge de la Concepcio 11 08008 Barcelona



**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Valid from:** *Wed Jun 30 10:57:35 CEST 2004*

**Valid to:** *Mon Jun 29 23:59:59 CEST 2020*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100BC0997D707DE74B6A7F45F9C9E71952262972F9236750C9CB69CD811EBDAAGIES-EC-  
TBAB8D75FD85B97C0516C8F3F60B9D35DESAG6D047049AA3411AC99E82ED7E9E9837F1C2D688A16DBE4FEB2154B507CA7C2E6492C92642D009241D15BA2B25055  
C4E8EB81FAA281F693B8E8DF2B5CB7341467F3DD580AFF5CBA9B8E8F85FA544FD766718E81B04298A7F2B66D78D00811D6E739E4D198ADE12405A780C2C5512C893  
0BE0FD0DC1FB3DAF265FDS43FB1E45B9D359F17FD910D7B35CFC1E79E241C2C110400296C216B3AD6B58670B07B8E50F922619BFC7A71A3E38E354FB3FD05F8  
FB42F44046FC42DDC3B965F1D0D7B51A21BEB8EAB62874E41399AEF0203010001

**Issuer Alternative Name** *ec\_acc@catcert.net*

**Subject Alternative Name** *ec-parlament@catcert.net*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *1E:13:98:EA:C2:42:59:55:B6:DE:2F:3E:CA:9F:C9:EA:CB:2E:2C:14*

**Authority Key Identifier** *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*  
*CPS pointer: <https://www.catcert.net/verCIC-2>*  
*CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-acc.crl>*  
*<http://epsd2.catcert.net/crl/ec-acc.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *44:C5:0A:C8:0E:DB:E9:E5:52:E3:C9:6C:E5:BD:11:C8:37:C7:0F:56:A3:3A:CA:BC:F1:8D:8D:7A:9B:35:0E:07*

**X509SubjectName**

**Subject CN:** *EC-PARLAMENT*

**Subject OU:** *Parlament de Catalunya*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2018-03-15T01:00:00Z

#### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 5.4.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

#### 5.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 5.4.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[es]* *Certificados Reconocidos emitidos por CA PARLAMENT*

**Name** *[en]* *Qualified certificates issued by CA PARLAMENT*

### Service digital identities

#### X509SubjectName

**Subject CN:** *EC-PARLAMENT*

**Subject OU:** *Parlament de Catalunya*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 5.4.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en]* *undefined.*

*[es]* *undefined.*

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4*

##### **Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4*

##### **Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

##### **Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

#### 5.4.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 5.4.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

**Name** [ es ] *Certificados Reconocidos emitidos por CA PARLAMENT*

**Name** [ en ] *Qualified certificates issued by CA PARLAMENT*

##### Service digital identities

##### X509SubjectName

**Subject CN:** *EC-PARLAMENT*

**Subject OU:** *Parlament de Catalunya*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *HhOY6sJCWVW23i8+yp/J6ssuLBQ=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2010-05-05T00:00:00Z*

#### 5.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.4

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.4

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

## 5.5 - Service (withdrawn): Certificados Reconocidos emitidos por CA UR

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

**Name** [ es ] Certificados Reconocidos emitidos por CA UR

**Name** [ en ] Qualified certificates issued by CA UR

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 8834028594214827114689084859419303276



**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*

**Authority Key Identifier** *A0:C3:8B:44:AA:37:A5:45:BF:97:80:5A:D1:F1:78:A2:9B:E9:5D:8D*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.12*  
*CPS pointer: <https://www.catcert.net/verCIC-2>*  
*CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de Classe 2. Vegeu <https://www.catcert.net/verCIC-2>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-acc.crl>*  
*<http://epsd2.catcert.net/crl/ec-acc.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *87:00:D0:47:E5:07:11:16:F6:75:51:A4:39:39:98:D6:29:E6:6F:02:C7:B5:2E:61:8E:F4:F9:49:6E:73:47:56*

**X509SubjectName**

**Subject CN:** *EC-UR*

**Subject OU:** *Universitats i Recerca*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2018-03-15T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**5.5.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3

**5.5.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**5.5.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados Reconocidos emitidos por CA UR*

**Name** [en] *Qualified certificates issued by CA UR*

**Service digital identities****X509SubjectName**

**Subject CN:** *EC-UR*

**Subject OU:** *Universitats i Recerca*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*



**Subject OU:** *Serveis Publics de Certificacio ECV-2*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *SJ+NhtHL8daKUnt/FaIKUfiX/gs=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 5.5.3.1 - Extension (critical): Qualifiers [NotQualified]

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

#### **Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2</i>
-------------------	--------------------	---

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1</i>
-------------------	--------------------	---

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.15096.1.3.1.161.3</i>
-------------------	--------------------	--

#### 5.5.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	<i>[ en ]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	---------------	--

#### 5.5.4 - History instance n.2 - Status: undersupervision

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service Name</b>		
<b>Name</b>	[ es ]	Certificados Reconocidos emitidos por CA UR
<b>Name</b>	[ en ]	Qualified certificates issued by CA UR
<b><u>Service digital identities</u></b>		
<b>X509SubjectName</b>		
<b>Subject CN:</b>		EC-UR
<b>Subject OU:</b>		Universitats i Recerca
<b>Subject OU:</b>		Vegeu <a href="https://www.catcert.net/verCIC-2">https://www.catcert.net/verCIC-2</a> (c)03
<b>Subject OU:</b>		Serveis Publics de Certificacio ECV-2
<b>Subject L:</b>		Passatge de la Concepcio 11 08008 Barcelona
<b>Subject O:</b>		Agencia Catalana de Certificacio (NIF Q-0801176-I)
<b>Subject C:</b>		ES
<b>X509SKI</b>		
<b>X509 SK I</b>		SJ+NhtHL&daKUnt/FaIKUfiX/gs=
<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>	
<b>Status Starting Time</b>	2010-05-05T00:00:00Z	

#### 5.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[ en ]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[ es ]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.3

**Policy Identifier:**



**Issuer OU:** *Vegeu <https://www.catcert.net/verCIC-2> (c)03*

**Issuer OU:** *Serveis Publics de Certificacio ECV-2*

**Issuer L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Issuer O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Issuer C:** *ES*

**Subject CN:** *EC-URV*

**Subject OU:** *Universitat Rovira i Virgili*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-3> (c)05*

**Subject OU:** *Serveis Publics de Certificacio*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

**Valid from:** *Fri Apr 17 11:47:19 CEST 2009*

**Valid to:** *Tue Apr 16 23:59:59 CEST 2019*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100EB9F6AFFFA423FEFA76FD97C92422EF3CE39EB13D1F5113800B0DD0E66029CE1F0AF03582D0D01B77C2B07803450E230273EBA0F0093079AA090D070802E613D428D97BFC7EAEF7D36E728265D942A177BD4AF01D15D68DF41632F04BF56678431694BE69A79A1BF45BBD089925D4CDEE1BA70C1D0C85331530ED4011AC2B6640276B007E166EB60A08BE8842DD6B20EA3AC3AE9A58D86D82BC7B1FA83C539DCB9140A9E9DAA0690BEED1228E34214A3E9C0FA0C4A7687AA6D08F7378D81FFBC7A1B2F313DE6DF001CFD64C06700316D76A93C82E7E49A516CF92960B28E5C0D61E2544D3F31C4863D6DA30CE52D9BCA89877CA32557C484A6D646AA822E05E90203010001

**Issuer Alternative Name** *ec\_ur@catcert.net*

**Subject Alternative Name** *ec-urv@catcert.net*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E*

**Authority Key Identifier** *48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.15096.1.3.1.13*  
*CPS pointer: <https://www.catcert.net/verCIC-3>*  
*CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3. Vegeu <https://www.catcert.net/verCIC-3>]*

**CRL Distribution Points**  
*<http://epsd.catcert.net/crl/ec-ur.crl>*  
*<http://epsd2.catcert.net/crl/ec-ur.crl>*

**Key Usage:** *keyCertSign - cRLSign*



**Subject C:** ES

**Valid from:** Tue May 03 11:36:18 CEST 2005

**Valid to:** Fri May 03 11:36:18 CEST 2013

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100EB9F6AFFFA423FEFA76FD97C92422E3CE39EB13D1F5113800B0DD0E66029CE1FD4F03582DD0DB1B7FC2B37803450E230273EBA8F0093079A009D070882E613DA28D97BFC7EAEF7D36E728265D942A17FBD4AF01D15D68DF41632F00B566764316948E69A79A1BF45BBD0C89925D4CD0E1B7A70C1DDC85331530ED4011AC2B6640276B007E166EB60A08BE8842DD6B20EA3AC3AE9A58D86D82BC7B1FA83C559DCB9140A9EC9DAA0690BEED1228E34214A3E9C0FA0C4A7687AA6D08F7378D81FFBC7A1B2F313DE6DF001CFD64C06700316D76A93C82E7E49A516CF92960B28E5C0D61E2544D3F31C4863D6DA30CE52D9BCA898F7CA32557C484A6D646AA822E05E90203010001

**Issuer Alternative Name** ec\_ur@catcert.net

**Subject Alternative Name** ec-urv@catcert.net

**Basic Constraints** IsCA: true

**Subject Key Identifier** BB:2E:A9:2E:30:D4:9C:10:73:B5:FD:A9:77:C2:3E:C3:51:97:B9:3E

**Authority Key Identifier** 48:9F:8D:86:D1:CB:F1:D6:8A:52:7B:7F:15:A2:0A:51:F8:97:FE:0B

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.15096.1.3.1.13  
 CPS pointer: <https://www.catcert.net/verCIC-3>  
 CPS text: [Aquest certificat és emès única i exclusivament a Entitats de Certificació de nivell 3.  
 Vegeu <https://www.catcert.net/verCIC-3>]

**CRL Distribution Points**  
<http://epsd.catcert.net/crl/ec-ur.crl>  
<http://epsd2.catcert.net/crl/ec-ur.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 88:33:D0:A9:1F:26:45:EF:EF:C3:B4:E0:0F:B8:97:C5:20:65:7E:BC:88:EA:F7:3B:9E:F0:F1:9A:2C:7B:A1:53

**X509SubjectName**

**Subject CN:** EC-URV

**Subject OU:** Universitat Rovira i Virgili

**Subject OU:** Vegeu <https://www.catcert.net/verCIC-3> (c)05

**Subject OU:** Serveis Publics de Certificacio

**Subject L:** Passatge de la Concepcio 11 08008 Barcelona

**Subject O:** Agencia Catalana de Certificacio (NIF Q-0801176-I)

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svstatus/withdrawn>

<b>Service status description</b>	[en]	undefined.
	[es]	undefined.

**Status Starting Time** 2018-03-15T01:00:00Z

### Scheme Service Definition URI

<b>URI</b>	[es]	<a href="https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>
<b>URI</b>	[en]	<a href="https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>

### 5.6.1 - Extension (critical): Qualifiers [NotQualified]

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

### 5.6.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 5.6.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [es] *Certificados Reconocidos emitidos por CA URV*

**Name** [en] *Qualified certificates issued by CA URV*

### Service digital identities

#### X509SubjectName

**Subject CN:** *EC-URV*

**Subject OU:** *Universitat Rovira i Virgili*

**Subject OU:** *Vegeu <https://www.catcert.net/verCIC-3> (c)05*

**Subject OU:** *Serveis Publics de Certificacio*

**Subject L:** *Passatge de la Concepcio 11 08008 Barcelona*

**Subject O:** *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *uy6pLjDUnBBztf2pd8I+w1GXuT4=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 5.6.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5*

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2*

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5*

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*



**5.6.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**5.6.4 - History instance n.2 - Status: undersupervision**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ es ] *Certificados Reconocidos emitidos por CA URV*

Name [ en ] *Qualified certificates issued by CA URV*

**Service digital identities****X509SubjectName**

Subject CN: *EC-URV*

Subject OU: *Universitat Rovira i Virgili*

Subject OU: *Vegeu <https://www.catcert.net/verCIC-3> (c)05*

Subject OU: *Serveis Publics de Certificacio*

Subject L: *Passatge de la Concepcio 11 08008 Barcelona*

Subject O: *Agencia Catalana de Certificacio (NIF Q-0801176-I)*

Subject C: *ES*

**X509SKI**

X509 SK I *uy6pLjDUUnBBztf2pd8I+w1GXuT4=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2010-05-05T00:00:00Z*

**5.6.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.5

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.2

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.5

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

## 5.7 - Service (granted): Qualified certificates issued by CA Ciutadania

### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

#### Name

[en]

Qualified certificates issued by CA Ciutadania

#### Name

[es]

Certificados Reconocidos emitidos por CA Ciutadania

### Service digital identities

#### Certificate fields details

#### Version:

3

#### Serial Number:

154100517041182570311467181176543273551



**CRL Distribution Points** <http://epsd.catcert.net/crl/ec-acc.crl>  
<http://epsd2.catcert.net/crl/ec-acc.crl>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6*

**X509SubjectName**

**Subject CN:** *EC-Ciudadania*

**Subject OU:** *Serveis Públics de Certificació*

**Subject O:** *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

**Subject C:** *ES*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en]* *undefined.*  
*[es]* *undefined.*

**Status Starting Time**

*2016-06-30T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**5.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**5.7.2 - History instance n.1 - Status: undersupervision****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[en]* *Qualified certificates issued by CA Ciudadania*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA Ciudadania*

### Service digital identities

#### X509SubjectName

**Subject CN:** *EC-Ciudadania*

**Subject OU:** *Serveis Públics de Certificació*

**Subject O:** *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *C2hZPofIoxUa4ECCII+fHbLFNxU=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2014-11-17T23:00:00Z*

## 5.8 - Service (granted): Qualified certificates issued by CA SectorPublic

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[ en ]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[ es ]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** *[ en ]* *Qualified certificates issued by CA SectorPublic*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA SectorPublic*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *151118660848720701053205649823964411794*



**CRL Distribution Points** <http://epsd.cacert.net/crl/ec-acc.crl>  
<http://epsd2.cacert.net/crl/ec-acc.crl>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3*

**X509SubjectName**

**Subject CN:** *EC-SectorPublic*

**Subject OU:** *Serveis Públics de Certificació*

**Subject O:** *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

**Subject C:** *ES*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en]* *undefined.*  
*[es]* *undefined.*

**Status Starting Time**

*2022-06-29T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**5.8.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en]* *undefined.*  
*[es]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

### 5.8.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 5.8.3 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 5.8.4 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### **Service Name**

**Name** [en] *Qualified certificates issued by CA SectorPublic*

**Name** [es] *Certificados Reconocidos emitidos por CA SectorPublic*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *EC-SectorPublic*

**Subject OU:** *Serveis Públics de Certificació*

**Subject O:** *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2018-03-15T01:00:00Z*

### 5.8.4.1 - Extension (critical): Qualifiers [NotQualified]



Qualifier type description	[en]	undefined.
	[es]	undefined.

### Criteria list assert=atLeastOne

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

#### 5.8.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 5.8.4.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 5.8.4.4 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

#### 5.8.5 - History instance n.2 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Qualified certificates issued by CA SectorPublic

Name [es] Certificados Reconocidos emitidos por CA SectorPublic

**Service digital identities****X509SubjectName**

Subject CN: *EC-SectorPublic*

Subject OU: *Serveis Públics de Certificació*

Subject O: *CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA*

Subject C: *ES*

**X509SKI**

X509 SK I *RzzeFHe7ak9HkakC/9QG4XPc4tk=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2016-06-30T22:00:00Z*

**5.8.5.5 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	<i>undefined.</i>
	[es]	<i>undefined.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1*

**Policy Identifier:**

Identifier *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1*

**Policy Identifier:**

Identifier *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1*

**5.8.5.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**5.8.6 - History instance n.3 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service Name</b>		
<b>Name</b>	[ en ]	Qualified certificates issued by CA SectorPublic
<b>Name</b>	[ es ]	Certificados Reconocidos emitidos por CA SectorPublic
<b>Service digital identities</b>		
<b>X509SubjectName</b>		
<b>Subject CN:</b>	EC-SectorPublic	
<b>Subject OU:</b>	Serveis Públics de Certificació	
<b>Subject O:</b>	CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA	
<b>Subject C:</b>	ES	
<b>X509SKI</b>		
<b>X509 SK I</b>	RzzeFHe7ak9HkakC/9QG4XPc4tk=	
<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>	
<b>Status Starting Time</b>	2014-11-17T23:00:00Z	

#### 5.8.6.7 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[ en ]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[ es ]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDAsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.161.1

##### Policy Identifier:

**Identifier** [ OIDAsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.91.1

##### Policy Identifier:

**Identifier** [ OIDAsURN ] urn:oid:1.3.6.1.4.1.15096.1.3.1.121.1

**6 - TSP: ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC****TSP Name**

**Name** [ en ] ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

**Name** [ es ] ANF AUTORIDAD DE CERTIFICACIÓN ASOCIACIÓN ANF AC

**TSP Trade Name**

**Name** [ en ] VATES-G63287510

**Name** [ en ] ANF AC

**Name** [ es ] ANF AC

**Name** [ en ] ANF Autoridad de Certificacion

**PostalAddress**

**Street Address** [ en ] Gran Vía de les Corts Catalanes, 996

**Locality** [ en ] Barcelona

**State Or Province** [ en ] Barcelona

**Postal Code** [ en ] 8018

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] Gran Vía de les Corts Catalanes, 996

**Locality** [ es ] Barcelona

**State Or Province** [ es ] Barcelona

**Postal Code** [ es ] 8018

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ en ] <http://www.anf.es>

**URI** [ en ] <mailto:info@anf.es>

**TSP Information URI**



**Issuer C:** ES

**Subject CN:** ANF Server CA

**Subject SERIAL NUMBER:** G-63287510

**Subject OU:** ANF Clase 1 CA

**Subject O:** ANF Autoridad de Certificacion

**Subject L:** Barcelona (see current address at <https://www.anf.es/address/>)

**Subject ST:** Barcelona

**Subject C:** ES

**Valid from:** Tue Apr 05 16:29:05 CEST 2005

**Valid to:** Fri Apr 03 16:29:05 CEST 2015

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100BFEA48A79A88396B2C48400704937CF7B82D7EA537E261D621FC9037CB693E5E8B37D  
F3BF3B7886C3884090F49D0C5C1032B1B3E55F9110E6FD8A80145F038BD5C8D0F23920937E372D266940B5C79942F5E124EDK03C6B3CE56A51C1D97BFD4F074C1D4  
B7DA5F294D75F21F55CF32231C4609271D45ECF18C3489DE7B16A7435E8A2BE994431E073E936D6F893D3C8EEB1C8B7FFC97D4E35F0D6F7778F52A2E8DC48B989730  
B1465A0B6370D478C786B37FF242AA9F8A6E6DA194CAEC87021CD6544BFD8C899BA66338668C16898997C350E8F64201A7777D10199203E85D45C815C5871B0D91  
F2C6399C7B73C00A99F8EE836F7E4277118EC31F1C722F3D1B0205010001

**Subject Key Identifier** BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C

**Basic Constraints** IsCA: true

**Certificate Policies** Policy OID: 1.3.6.1.4.1.18332.1.8  
CPS pointer: <https://www.anf.es/AC/documentos>  
CPS text: [Antes de aceptar este certificado, compruebe:  
-Condicionen, limitaciones y usos autorizados segun CP a la que se somete.  
-Estado de vigencia]

**Authority Key Identifier** BE:3B:F6:B4:31:B7:73:24:48:39:C5:57:13:94:75:AA:9F:81:3F:2C

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 71:D9:41:36:C6:0F:F5:74:6E:8D:93:23:27:A9:AE:D5:BE:6A:31:F4:2C:7F:55:B0:5A:37:4F:9B:6F:4D:27:27

**X509SubjectName**

**Subject CN:** ANF Server CA

**Subject SERIAL NUMBER:** G-63287510

**Subject OU:** ANF Clase 1 CA

**Subject O:** ANF Autoridad de Certificacion

**Subject L:** *Barcelona (see current address at <https://www.anf.es/address/>)*

**Subject ST:** *Barcelona*

**Subject C:** *ES*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 6.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.2.4*

#### 6.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

**Qualifier type description** *[en] it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

*[es] está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.2.4*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.3.4*

#### 6.1.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**6.1.4 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ en ]* *Qualified certificate issued by ANF Server CA*

**Name** *[ es ]* *Certificado reconocido emitido por la CA ANF Server CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANF Server CA*

**Subject SERIAL NUMBER:** *G-63287510*

**Subject OU:** *ANF Clase 1 CA*

**Subject O:** *ANF Autoridad de Certificación*

**Subject L:** *Barcelona (see current address at <https://www.anf.es/address/>)*

**Subject ST:** *Barcelona*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *vjv2tDG3cyRIOcVXE5R1qp+BPYw=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time**

*2015-05-11T00:00:00Z*

**6.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** *[ en ]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

*[ es ]* *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**



**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.2.4

### 6.1.4.2 - Extension (critical): Qualifiers [QCStatement]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.2.4

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.18332.3.4

### 6.1.5 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] *Qualified certificate issued by ANF Server CA*

**Name** [es] *Certificado reconocido emitido por la CA ANF Server CA*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *ANF Server CA*

**Subject SERIAL NUMBER:** *G-63287510*

**Subject OU:** *ANF Clase 1 CA*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona (see current address at <https://www.anf.es/address/>)*

**Subject ST:** *Barcelona*

**Subject C:** *ES*

X509SKI

X509 SK I

vjv2tDG3cyRIOcVXE5R1qp+BPYw=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2004-11-25T00:00:00Z

**6.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[ OIDsURN ]

urn:oid:1.3.6.1.4.1.18332.2.4

**6.1.5.4 - Extension (critical): Qualifiers [QCStatement]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in "Service digital identity" and further identified by the above (filters) information used to further identify under the "Sdi" identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier

[ OIDsURN ]

urn:oid:1.3.6.1.4.1.18332.2.4

Policy Identifier:

Identifier

[ OIDsURN ]

urn:oid:1.3.6.1.4.1.18332.3.4

**6.2 - Service (granted): Qualified certificate issued by ANF Assured ID CA1**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.



**Subject CN:** ANF Assured ID CA1

**Subject SERIAL NUMBER:** G63287510

**Subject E:** info@anf.es

**Subject OU:** ANF Autoridad Intermedia de Identidad

**Subject O:** ANF Autoridad de Certificacion

**Subject L:** Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)

**Subject ST:** Barcelona

**Subject C:** ES

**Valid from:** Mon Mar 03 12:17:23 CET 2014

**Valid to:** Thu Feb 29 12:17:23 CET 2024

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201009C7BF4896DFC7D980CEA24F9EE8CADC4E0A7EC8157FA0A954B7F7C85C74449E2C9D  
A3A34141E2B994002D682032BB19708501583E6447EB5F3B5897BD9A457547DC31E57805115990D7B5FAC16A472A0C6C2E537BCB7B7FDDDE19658BFD08C589498SE1  
046D718E7FF7B7CSAD958B60550EB2EE73E59786F0FA25B6C337DDCC2A388F14461A088B405D920D7E0272C11DFF6FF53FAE798AF1A575B7082B4EE18EE56D92B.D147  
540044DC31B8B9E2B4CB4EB7579F594735B4A01A06A2187D933D2E26CFD796F23C62B4A04909A9BEBE72E2C0314992B0E07B4A8C71095173BDB303E7FFE4E0C9BA  
E24A26ED52EB43SE19C4C24204C02A81462D3C3EFA020707C487D00D77FD5CD0D90F89449961BD948C32F7413A0F5599A983A20E12835F736837D60E8CB718139B1C  
23928BD42174A50F6F6F464DB0A187A5D02A19AC1E263AE81843F392939B8509F746D085F222C13E0D66A7DB794C2E6FBD49D7AE9B7893B2F076EB2SA728EC  
3FA8ADD543080D0E3171407EBFD4B8623963AB44F69E9B2AA39A9ABD2076CE29F9A9CFB48C96441847E11E37446EBE4D48EA3E76245C4DA21669F462CE18E0A8  
409D3F53D5A7E5788B1A0F7391A273554933C48B5388C8C8ED43DE5E8C035E6B0BB7F9CF69B2D1A.D11D871BB56BA26C04194C38F69B62E6F87E.B6BB44B134BF54  
A409E2C2D476FB472A36B27C.CACE8624A36F3962D30203010001

**Subject Key Identifier** 35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Basic Constraints** IsCA: true

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003 España. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]  
CPS pointer: <https://www.anf.es/es/documentos>

**CRL Distribution Points**  
[https://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_arl.crl](https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl)  
[https://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_arl.crl](https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl)  
ldap://ldap.anf.es:389/cn=ANF\_Global\_Root\_CA\_arl.crl,ou=ANF\_Global\_Root\_CA,dc=anf  
DC=anf,CN=ANF\_Global\_Root\_CA\_arl.crl,OU=ANF\_Global\_Root\_CA

**Authority Info Access** <http://ocsp.anf.es/spain/AV>

**Subject Alternative Name**  
<http://www.anf.es>  
info@anf.es  
OU="Inscrita en el Ministerio del Interior de España con el numero nacional 171.443",  
SERIALNUMBER="G63287510", O=ANF Autoridad de Certificacion, L=Barcelona,  
STREET=Gran Via de les Corts Catalanes. 996. 08018

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** FB:E0:EC:01:17:9E:8F:99:CC:58:BF:D2:53:8A:B1:1E:75:7D:18:C6:43:7A:8D:C9:65:19:10:F4:45:3C:D4:C5

## X509SubjectName

**Subject CN:** ANF Assured ID CA1

**Subject SERIAL NUMBER:** G63287510

**Subject E:** info@anf.es

**Subject OU:** ANF Autoridad Intermedia de Identidad

**Subject O:** ANF Autoridad de Certificacion

**Subject L:** Barcelona (see current address at <http://www.anf.es/es/address-direccion.html> )

**Subject ST:** Barcelona

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2019-10-28T01:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 6.2.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22

**6.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**6.2.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**6.2.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22">urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22</a>
------------	-------------	---

**Policy Identifier:**

Identifier	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.18332.2.5.1.13">urn:oid:1.3.6.1.4.1.18332.2.5.1.13</a>
------------	-------------	---

**Policy Identifier:**

Identifier	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.18332.2.5.1.14">urn:oid:1.3.6.1.4.1.18332.2.5.1.14</a>
------------	-------------	---

**Policy Identifier:**

Identifier	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.18332.2.5.1.15">urn:oid:1.3.6.1.4.1.18332.2.5.1.15</a>
------------	-------------	---

**Description****6.2.5 - History instance n.1 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
-------------------------	---

**Service Name**

Name	[ en ]	Qualified certificate issued by ANF Assured ID CA1
------	--------	--

Name	[ es ]	Certificado reconocido emitido por la CA ANF Assured ID CA1
------	--------	---

Service digital identities**X509SubjectName**

Subject CN: ANF Assured ID CA1

Subject SERIAL NUMBER: G63287510

Subject E: info@anf.es

Subject OU: ANF Autoridad Intermedia de Identidad

Subject O: ANF Autoridad de Certificacion

Subject L: Barcelona (see current address at <http://www.anf.es/es/address-direccion.html> )

Subject ST: Barcelona

Subject C: ES

**X509SKI**

X509 SK I NS4t5ikcv4vZSnyeK+CVR9HGTz0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-03-15T01:00:00Z

6.2.5.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22

6.2.5.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**6.2.5.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**6.2.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [ en ] undefined.  
[ es ] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] <urn:oid:1.3.6.1.4.1.18332.3.4.1.5.22>

**Policy Identifier:**

**Identifier** [ OIDsURN ] <urn:oid:1.3.6.1.4.1.18332.2.5.1.13>

**Policy Identifier:**

**Identifier** [ OIDsURN ] <urn:oid:1.3.6.1.4.1.18332.2.5.1.14>

**Policy Identifier:**

**Identifier** [ OIDsURN ] <urn:oid:1.3.6.1.4.1.18332.2.5.1.15>

**Description****6.2.6 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificate issued by ANF Assured ID CA1*

**Name** [ es ] *Certificado reconocido emitido por la CA ANF Assured ID CA1*

**Service digital identities****X509SubjectName**

**Subject CN:** *ANF Assured ID CA1*

**Subject SERIAL NUMBER:** *G63287510*



**Subject E:** *info@anf.es*  
**Subject OU:** *ANF Autoridad Intermedia de Identidad*  
**Subject O:** *ANF Autoridad de Certificacion*  
**Subject L:** *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html> )*  
**Subject ST:** *Barcelona*  
**Subject C:** *ES*

**X509SKI**

**X509 SK I** *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

**6.2.6.5 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*

**6.2.6.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**6.2.7 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service Name**

**Name** [en] *Qualified certificate issued by ANF Assured ID CA1*

**Name** [es] *Certificado reconocido emitido por la CA ANF Assured ID CA1*

## Service digital identities

### X509SubjectName

**Subject CN:** *ANF Assured ID CA1*

**Subject SERIAL NUMBER:** *G63287510*

**Subject E:** *info@anf.es*

**Subject OU:** *ANF Autoridad Intermedia de Identidad*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html>)*

**Subject ST:** *Barcelona*

**Subject C:** *ES*

### X509SKI

**X509 SK I** *NS4t5ikcv4vZSnyeK+CVR9HGTz0=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2014-09-15T00:00:00Z*

### 6.2.7.7 - Extension (critical): Qualifiers [QCForLegalPerson]

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

### **Criteria list assert=atLeastOne**

#### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.11*

#### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.18332.2.4.1.2.22*



**Subject C:** ES

**Subject CN:** ANF High Assurance AP CA1

**Subject SERIAL NUMBER:** G63287510

**Valid from:** Fri May 20 17:08:29 CEST 2016

**Valid to:** Mon May 18 17:08:29 CEST 2026

**Public Key:**  
3082 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 02 0F 00 30 82 02 0A 02 82 02 01 00 84 93 2F 7E 53 18 FA 3D F1 06 E2 CD E7 F2 3B 02 C2 64 EE E5 1E B6 F8 0D BD 5B B5 9A F4 0F A3 D7 92 CD 5A 03 75 91 2F 0F EF 50 85 B0 2C FE 7E 45 65 71 C1 16 AD E6 F8 42 7A 19 99 C7 0E DB 4A 89 5C 03 1A 0A BE DC E6 82 82 94 3E DD 4A CE AB 81 FD 43 25 45 33 9C 04 65 4A 26 7E 9B A1 2A 45 24 84 4E D4 16 3 C 84 5 FE BD 80 8E 0C DF 3E F9 C7 E3 FF 6B 8A F7 0A 90 EF C1 7D E9 E2 66 59 B2 85 AB E9 A5 4F A5 C2 AC ED 01 BB 4E 7D 9D 58 FB A8 2D 0F BD 64 DF D4 43 68 98 D7 D4 01 BD F1 55 E0 9B C1 05 6A 8 E 73 D2 F6 B3 42 37 9A F5 86 43 A0 C4 F2 62 BE 9C 86 8D 14 44 E3 B6 F5 DE 0C F5 29 03 03 80 54 F9 5C 1A 1E D6 AF D0 2B 63 73 5E BC C9 88 E6 A8 90 ED CA 33 1F 4E 50 85 03 6E A6 47 57 27 78 1F 31 83 8 D 28 C9 33 30 00 87 10 9A 62 C5 48 E7 16 B4 2A EA 5B 37 42 CB F4 13 CC 5F C9 1A E0 85 01 EF 6A 6B 18 24 DE 21 95 A4 8D 10 C7 2D D9 7C 5D B3 93 F1 23 03 3D 4E AD 5E 13 20 0A C9 6C 5A E9 5B 66 87 1 9 B3 84 39 97 97 3B 1A D9 21 C8 FB F1 43 40 EC D1 D1 8B AF AB A5 DA AF C1 49 43 6C 2B 95 E9 1B 1C 7E 6D BB 00 26 C3 AA 8C AE D6 58 3A 7B 6C 55 F2 5F 0F 20 F5 72 FA 74 39 77 22 77 E5 05 3E D7 72 D8 75 3E 36 67 BA E5 49 FB 8C E4 4D BB C1 42 6E 79 CD 07 A0 4D 02 3F AB 77 ED D4 C7 ED 01 01 69 58 39 30 A8 13 D9 8E 4A 68 4B 3E 4F 43 3B 20 5D D8 F8 BE 77 DB 8F 79 5A 36 56 59 0A 0C B2 77 C9 35 A6 AD D2 B9 13 65 64 2B E5 7D 29 51 D7 22 0C 25 C2 DA 15 CF 6D 6C 10 51 ED 82 C7 6E F2 85 CE A1 8C FF F8 FA 6D AB 96 6C 03 9D 4E 80 9D 9C 44 93 73 84 90 AD 04 71 B2 AB C0 83 9C 1E 04 0C 1A BA 2 2 D2 DC CB 9E 0B F3 FA 6F EC A1 83 5C 19 A6 CC 89 48 95 A1 D5 1B 8E 71 02 03 01 00 01

**Subject Key Identifier** 92:47:FD:D2:C3:61:2B:A9:C7:09:A7:3D:3E:35:27:51:31:08:6C:35

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Basic Constraints** IsCA: true

**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS text: [ANF AC emisor de certificados reconocidos conforme la Ley 59/2003. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]  
 CPS pointer: <http://www.anf.es/es/documentos>

**CRL Distribution Points** [https://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_arl.crl](https://www.anf.es/crl/ANF_Global_Root_CA_arl.crl)  
[https://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_arl.crl](https://crl.anf.es/crl/ANF_Global_Root_CA_arl.crl)

**Authority Info Access** <http://ocsp.anf.es/spain/AV>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 4D:C5:4F:4C:5B:DA:C1:95:57:06:6E:32:F6:2F:8C:48:6B:15:5B:00:F5:3D:10:2D:E7:8C:98:EE:61:A2:C3:17

**X509SubjectName**

**Subject O:** ANF Autoridad de Certificacion

**Subject OU:** ANF Autoridad Intermedia PKde API

**Subject C:** ES

**Subject CN:** ANF High Assurance AP CA1

**Subject SERIAL NUMBER:** G63287510

**X509SKI**

**X509 SK I** *kkf90sNhK6nHCac9PjUnUTEIbDU=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2022-01-11T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**6.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**6.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**6.3.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified certificates issued by ANF High Assurance AP CA1*

**Name** *[es] Certificados cualificados emitidos por ANF High Assurance AP CA1*

**Service digital identities****X509SubjectName**

**Subject O:** *ANF Autoridad de Certificacion*

**Subject OU:** *ANF Autoridad Intermedia PKde API*

**Subject C:** ES

**Subject CN:** ANF High Assurance AP CA1

**Subject SERIAL NUMBER:** G63287510

**X509SKI**

**X509 SK I** kkf90sNhK6nHCac9PjUnUTEIbDU=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2018-03-15T01:00:00Z

**6.3.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**6.3.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**6.3.3.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**6.4 - Service (granted): Qualified certificates issued by ANF High Assurance EV CA1**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [ en ] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[ es ] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [ en ] Qualified certificates issued by ANF High Assurance EV CA1

**Name** [ es ] Certificados cualificados emitidos por ANF High Assurance EV CA1

Service digital identities

Certificate fields details

Version: 3
Serial Number: 458635322224564480

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHRcCB...
-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer O: ANF Autoridad de Certificacion

Issuer OU: ANF Clase 1 CA

Issuer C: ES

Issuer CN: ANF Global Root CA

Issuer SERIAL NUMBER: G63287510

Subject O: ANF Autoridad de Certificacion

Subject OU: ANF Autoridad Intermedia Tecnicos

Subject C: ES

Subject CN: ANF High Assurance EV CA1

Subject SERIAL NUMBER: G63287510

Valid from: Fri May 20 16:48:24 CEST 2016

Valid to: Mon May 18 16:48:24 CEST 2026

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:77:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:45:34:9F:DE:00:07:5E:6F:80:DA:46:B4:FA:F8:69:79:D9:33:EB:BC:E5:F2:CD:23:FF:4F:53:C2:10:8F:7A:09:34:5:
B:FE:30:31:FA:0B:A4:81:1F:81:0B:DD:5D:CB:BA:FE:5E:F0:F3:3C:3A:9A:44:64:D9:7F:B0:78:9E:B3:1A:CC:F3:C8:BB:61:B7:39:6D:1D:30:04:DF:94:EF:B2:27:2F:D4:0B:F1:BE:74:68:B6:69:5A:20:D8:A7:16:E8:E7:72:
90:74:3E:38:25:B2:78:29:4E:AA:84:E7:F5:D1:A5:56:9E:20:76:3D:2F:3A:7C:DS:76:4F:3A:21:D9:45:14:FC:37:DC:43:EE:EA:EE:76:48:56:7E:B6:17:2B:4C:7B:21:C5:C0:13:25:40:1D:01:92:1F:F8:CD:2C:B2:61:B2:7C:41:B7:
88:EE:36:60:07:00:19:AC:74:28:45:0D:C5:77:1D:3F:53:6B:EE:01:61:2E:3E:61:3D:07:2E:61:95:6B:BE:3D:39:91:EA:9E:15:AE:CA:9C:60:E2:7E:9C:A6:D3:7E:8B:CF:3D:83:EF:31:DA:4B:89:88:71:8E:7D:06:A4:DC:60:E7:
BF:3A:09:F9:D9:20:15:FA:27:24:89:68:10:53:66:86:ED:94:2D:FE:D6:51:A9:10:21:7D:CE:DA:44:07:56:EB:F3:5F:A9:64:BS:15:BA:8B:AE:F4:3E:08:3D:F0:FE:89:CB:3C:A7:95:64:1B:7A:4B:07:33:0A:FE:74:CF:B2:FB:0B:5:
2:98:09:49:52:BE:E7:24:54:30:4E:CC:8C:C3:A0:40:7E:C0:E6:13:8D:AF:3F:08:5B:AD:1C:D1:33:BC:2C:3B:CF:D2:62:81:CI:A6:45:04:61:84:42:A1:B2:64:C5:93:E8:58:DA:A6:FD:B8:76:FA:02:B4:DB:6E:BB:80:3A:F8:8B:4:
7:71:40:F1:58:BE:EC:C9:DD:A6:3D:72:1E:36:D4:06:2D:A4:64:EB:4A:9C:2E:FE:22:DE:44:8B:8A:3F:CI:0K:95:E3:EC:BB:CE:64:D2:22:43:79:FE:C3:96:E2:42:AC:1D:72:80:CB:32:DE:3E:24:91:DE:93:14:11:9B:58:59:8C:35:
EC:0D:8D:80:0F:EC:FB:4A:59:9B:C9:04:BA:97:2F:8F:46:8B:73:9F:A4:37:66:88:29:FA:6E:E3:0F:12:E1:FB:AE:DD:A1:48:10:BB:4D:EC:9F:85:F9:05:B5:8D:11:65:DB:CB:15:E7:D5:7F:FB:73:17:42:90:55:85:3F:C3:
58:D9:CF:2F:FB:81:3F:F8:07:8D:2F:9C:8A:0D:6E:D3:3F:5B:61:BF:45:02:03:01:00:01

**Subject Key Identifier** 86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Basic Constraints** IsCA: true

**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]  
 CPS pointer: <http://www.anf.es/es/documentos>

**CRL Distribution Points** [http://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)  
[http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)

**Authority Info Access** <http://ocsp.anf.es/spain/AV>  
[http://anf.es/es/certificates\\_download/ANF\\_Global\\_Root\\_CA\\_SHA256\\_2036.cer](http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04

**X509SubjectName**

**Subject O:** ANF Autoridad de Certificacion

**Subject OU:** ANF Autoridad Intermedia Tecnicos

**Subject C:** ES

**Subject CN:** ANF High Assurance EV CA1

**Subject SERIAL NUMBER:** G63287510

**X509SKI**

**X509 SK I** hr7ji+7o/UsoRzErcpBe4gslzng=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2018-03-15T01:00:00Z

**Scheme Service Definition URI**





**Issuer OU:** ANF Clase 1 CA

**Issuer C:** ES

**Issuer CN:** ANF Global Root CA

**Issuer SERIAL NUMBER:** G63287510

**Subject O:** ANF Autoridad de Certificacion

**Subject OU:** ANF Autoridad Intermedia Tecnicos

**Subject C:** ES

**Subject CN:** ANF High Assurance EV CA1

**Subject SERIAL NUMBER:** G63287510

**Valid from:** Fri May 20 16:48:24 CEST 2016

**Valid to:** Mon May 18 16:48:24 CEST 2026

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201009145349FDE0075E6F80DA46B4FAF86979D933E8BCESF2CD23FF4E53C2108F7A09345  
BEE5031C1FA08A4811F810BDD3DCBBAFF5E40F33CA9A4464D97F80789EB31ACC43C8BB61B7396D1D3004DF94EFB2272FD408F1BE7468B6695A20D8A716E8E772  
90743E3825B2F8294EAA84E7F5D1A5569E20763D2F3A7CDS764F3A21D94514FC57DC43EEEA76748567EB6172B4C7B21C5C01325401D01921F8CD2CB261B27C41B7  
85E1366070019AC7428456DCS771D3F539B5E01612E86718D072E61956B8E5D3991EA9F15ABCA9C60E27F9CA6D37E9BCE3D83EF33DAB89B8718E7D06A4DC60E7  
BF3A09F9D92015F42724896810536686E9942DF6651A910213DCEDA440756EBF35FA964B515BABB4E743E083D30FF89CB3CA795641B7A4B07330A1F74CF82FB0B5  
29B604952BE72454304ECC8C3A0497E0E6138DAF3E085BADC1D133CB2C3BCFDE26281CIA64504618442A1B264C593E858D7A6FDB876FA02B4DB6E88803AF88B4  
7714FF158B0EC98DA65D721E26D462DA464EB4A9C2EFF22DE448B8A3FC10495E3ECBBCE64D224379FFC396E242AC1D12B0C032DE3E2491D29314119B58599C35  
EC0D0D8D800FECTB4A599BC904BA972F8F4680B739FA37668829FA6EE30F12E1FBAED0A14810BB4DEC9F85F905B58D1165D8CB15E7D57F7B73177F429055853FC3  
58D9CF2FB813FF8078D2F9CA0D6ED33FB361BF450203010001

**Subject Key Identifier** 86:BE:E3:8B:EE:E8:FD:4B:28:47:31:2B:72:90:5E:E2:0B:25:CE:78

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Basic Constraints** IsCA: true

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS text: [ANF AC emisor de certificados reconocidos conforme la legislacion espanola. Cualquier uso de este certificado implica la aceptacion de la CPS y de las limitaciones de responsabilidad en el establecidas.]  
CPS pointer: <http://www.anf.es/es/documentos>

**CRL Distribution Points**  
[http://www.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://www.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)  
[http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
[http://anf.es/es/certificates\\_download/ANF\\_Global\\_Root\\_CA\\_SHA256\\_2036.cer](http://anf.es/es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 1C:28:A8:C0:09:F2:58:50:B9:15:55:33:D4:A9:A1:4C:53:4B:24:DA:84:75:6E:82:D6:15:0B:50:62:D6:37:04

**X509SubjectName**

**Subject O:** ANF Autoridad de Certificacion

**Subject OU:** ANF Autoridad Intermedia Tecnicos

**Subject C:** ES

**Subject CN:** ANF High Assurance EV CA1

**Subject SERIAL NUMBER:** G63287510

**X509SKI**

**X509 SK I** hr7ji+7o/UsorZercpBe4gslzng=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time**

2022-01-11T02:00:00Z

**Scheme Service Definition URI**

**URI** [en] [https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\\_ANF.aspx](https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF.aspx)

**URI** [es] [https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\\_ANF.aspx](https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_ANF.aspx)

**6.5.1 - History instance n.1 - Status: granted****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

**Name** [en] Qualified timestamps issued by ANF High Assurance EV CA1

**Name** [es] Sellos de tiempo cualificados emitidos por ANF High Assurance EV CA1

**Service digital identities****X509SubjectName**

**Subject O:** ANF Autoridad de Certificacion

**Subject OU:** ANF Autoridad Intermedia Tecnicos

**Subject C:** ES

**Subject CN:** ANF High Assurance EV CA1

**Subject SERIAL NUMBER:** G63287510

**X509SKI**

**X509 SK I** *hr7ji+7o/UsoRzErcpBe4gslzng=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-03-15T01:00:00Z*

**6.6 - Service (withdrawn): Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q*

**Service type description** *[en] undefined.*  
*[es] undefined.*

**Service Name**

**Name** *[en] Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION*

**Name** *[es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION*

**Service digital identities**

**Certificate fields details**

**Version:** 3

**Serial Number:** 996613180148035949



**Subject SURNAME:** DIAZ VILCHES - 37271387W

**Subject O:** ANF AUTORIDAD DE CERTIFICACION ASOCIACION ANF AC

**Subject T:** PRESIDENTE

**Subject 2.5.4.13:** Cargo:PRESIDENTE .INSCRIPCIÓN: REG. ASOCIACIONES DEL MINISTERIO DEL INTERIOR. GRUPO 1º, SEC. 1ª, NUM. 171443. FECHA: 12.01.2004.

**Subject OU:** Certificado de Sello Electronico

**Subject SERIAL NUMBER:** TINESG63287510

**Valid from:** Mon Dec 24 11:03:11 CET 2018

**Valid to:** Wed Dec 23 11:03:11 CET 2020

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100A8AD80159E4BAC2027FDDAD72C3FD8A907D9B34BC230A63DFE4BF23351B1EC8AFE  
3C308CA81196D011E1F63D3525963A5007FC961F7C50B5A9C9484E79AD0CD6F9C24683730E6C98089B855A55E9CAF46EAD228D672D9B596DE7DB654A  
C88BA3E33813EEC1A5BD77A45476018B35A8138369BF156D9C82EC50E993E5C85D23797E15F5AC00AE009553B8D35FA8A7C851919A1DC7A48F13F15A6AF15B7C6F259AEC19BEB9  
R60E83915E269E20D6EC1263C75660E4184C947126F3B4AC74D6AE46BBFD53AC11A94E0E1E247C887B48E645C4EAC0601B69A21D27119E0A42C3CA1CF1772EF00EA1  
F67C0713FE9E6ED0F6B8B657AE7D6F45FCC09BA86692FES10DB4D650203010001

**Basic Constraints** IsCA: false

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
[http://www.anf.es/es/certificates\\_download/ANF\\_Assured\\_ID\\_CA1\\_SHA256.cer](http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer)

**CRL Distribution Points**  
[https://www.anf.es/crl/ANF\\_Assured\\_ID\\_CA1\\_SHA256.crl](https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl)

**Subject Directory Attributes**  
2.5.4.15 Private Organization  
1.3.6.1.4.1.311.60.2.1.1 Madrid  
1.3.6.1.4.1.311.60.2.1.2 Madrid  
1.3.6.1.4.1.18332.600 ARMD v.3.5.1.70  
1.3.6.1.4.1.18332.30.1 España  
1.3.6.1.4.1.18332.10.10.1 [https://tomcat2.anf.es/cliente\\_archivo\\_ws/poderes/119814498-89288764](https://tomcat2.anf.es/cliente_archivo_ws/poderes/119814498-89288764)  
2.5.4.9 PASEO DE LA CASTELLANA, 79  
1.3.6.1.4.1.18332.40.1 CERTIFICADO CUALIFICADO  
1.3.6.1.4.1.18332.41.1 1000  
2.5.4.17 28046  
1.3.6.1.4.1.18332.91.1 Asociación  
2.5.4.42 FLORENCIO  
2.5.4.4 DÍAZ VILCHES - 37271387W  
1.3.6.1.4.1.18332.42.1 000-0000  
2.5.4.9 PASEO DE LA CASTELLANA, 79

**QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15**id\_etsi\_qcs\_LimiteValue**Value: 1000**Currency: EUR***Subject Alternative Name***serviciotecnico@anf.es***Subject Key Identifier**

*30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:A0:80:15:9E:4B:AC:20:27:FD:AD:F7:2C:3F:D8:A9:07:D9:B3:4B:C2:30:A6:3D:FE:4B:F2:33:51:B1:EC:8A:FE:D3:C3:08:CA:81:19:6D:01:1E:F6:5D:35:25:96:3A:50:07:FC:96:1F:7C:50:B5:A9:C9:48:4E:79:AD:0C:D6:F9:C2:46:83:73:0E:6C:98:08:9B:85:5A:55:E9:CA:F4:6E:AD:22:8D:67:2D:9B:59:6D:E7:DB:65:4A:C8:8B:A3:E3:38:13:EE:C1:A5:BD:77:A4:54:76:61:8B:35:A8:13:83:69:BF:13:6D:9C:82:EC:50:E9:93:E5:C8:5D:23:79:7E:15:F5:AC:00:AE:A0:95:53:B8:D3:5F:A8:A7:C8:51:91:9A:DC:7A:48:F1:3F:F5:A6:AF:15:B7:C6:F2:99:AE:C1:9B:EB:9B:60:B3:91:5E:26:9B:20:D6:EC:12:63:C7:56:60:E4:18:4C:94:71:26:F5:B4:AC:F4:D6:AE:46:BB:FD:E5:AC:A1:A9:4E:0E:1E:24:7C:88:7B:48:E6:45:C4:EA:C6:61:B6:9A:21:D2:71:19:E0:A4:2C:3C:A1:CF:17:72:EF:00:EA:1F:67:C0:71:3F:E9:E6:ED:0F:6B:8B:65:7A:E7:D6:F4:5F:CC:09:BA:B6:69:2F:E5:10:DB:4D:65:02:03:01:00:01*

**Extended Key Usage***id\_kp\_codeSigning - id\_kp\_clientAuth - id\_kp\_serverAuth***Authority Key Identifier***35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D***Certificate Policies***Policy OID: 1.3.6.1.4.1.18332.25.1.1.1**CPS pointer: <http://www.anf.es/documentos>**CPS text: [Certificado conforme a la legislación de firma electrónica. Antes de aceptarlo compruebe integridad, limitaciones, vigencia y usos autorizados.]**Policy OID: 0.4.0.194112.1.1***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***B1:14:56:6D:66:73:7E:AC:6F:1C:A1:AA:16:C0:0F:51:89:69:A2:C4:4C:A6:D8:6D:8F:4F:97:EE:A2:41:C8:E9***X509SubjectName****X509SKI****X509 SK I**

*MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEaKCAFZ5LrCAn/a33LD/YqQfZs0vCMKY9/kvyM1Gx7Ir+08MIyoEZbQEe9I01JZY6UAf8lh98ULWpyUhOea0M1vnCRoNzDmyY CJuFWLXpyvRurSKNZy2bWW3n22VKyluj4zgT7sGlvXekVHZhizWoE4NpvxNtnLLsUOmT5chdl3l+FfWsAK6gIVO401+op8hRkZrcekjxP/WmrXW3xvKZrsGb65tgs5FeJpsgluwSY8dWYOQYTJR xJvW0rPTWrka7/eWsoalODh4kflh7SOZFxOrGYbaaldJxGeCkLDyhzxdy7wDqH2fAcT/p5u0Pa4tl eufW9F/MCbq2aS/IEntNZQIDAQAB*

**Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description***[en] undefined.**[es] undefined.***Status Starting Time***2021-01-26T01:00:00Z*

**6.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**6.6.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**6.6.3 - History instance n.1 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q">http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q</a>
-------------------------	---

**Service Name**

Name	[ en ]	Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AUTORIDAD DE CERTIFICACION
------	--------	---

Name	[ es ]	Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor ANF AUTORIDAD DE CERTIFICACION
------	--------	--

**Service digital identities****X509SubjectName****X509SKI**

X509 SKI	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEaKCAFZ5LrCAN/a33LD/YqQfZs0vCMKY9/kvyM1Gx7lr+08MIyoEZbQEe9l01JZY6UAf8lh98ULWpyUhOea0M1vnCRoNzDmyYCJuFWIXpyvRurSKNZy2bWW3n22VKyIuj4zgT7sGlvXekVHZhizWoE4NpvxNtnILsUOmT5chdI3l+FfWsAK6gIVO401+op8hRkZrcekjxP/WmrXW3xvKZrsGb65tgs5FeJpsgluwSY8dWYOQYTJR xJvW0rPTWrka7/eWsoalODh4kflh7SOZFxOrGYbaaIdJxGeCkLDyhzzxy7wDqH2fAcT/p5u0Pa4tl eufW9F/MCbq2aS/ENtNZQIDAQAB
----------	--

Service Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
----------------	---

Status Starting Time	2019-02-18T01:00:00Z
----------------------	----------------------

**6.6.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**6.6.3.2 - Extension (critical): additionalServiceInformation**





**Subject CN:** ANF High Assurance Server CA

**Subject OU:** ANF Autoridad intermedia tecnicos

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

**Subject SERIAL NUMBER:** G63287510

**Valid from:** Thu Sep 05 18:35:44 CEST 2019

**Valid to:** Sun Sep 02 18:35:44 CEST 2029

**Public Key:**  
3082 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 02 0F 00 30 82 02 0A 02 82 02 01 00 DD A8 CB E2 42 F5 FD 04 9F 26 7A 93 C5 2E 94 00 88 38 A6 35 96 FD D3 B5 CA 77 F6 C3 6E D1 D0 54 3F C8 4E 39 60 01 86 F6 B4 35 33 8F 4F CA 99 5A 95 FE AE 40 D6 96 C9 9B 74 C5 12 DA A0 00 B0 CB BF BC D5 0E 92 20 F4 CF F2 1C E6 3A 83 24 13 B2 8E 71 BC 12 9C 33 21 AD 05 CF 8B F1 00 C8 45 DE ED 89 99 4 F F0 35 0F 19 2B 6D 92 72 63 B2 9F 63 ED A7 31 88 CC E9 DB 1B 5B 18 BE A4 95 76 1D 06 D5 D9 44 6A AA 13 C4 FC F9 F8 4C 71 DD 90 89 1A F2 D5 19 52 6B 4E 8D 08 15 75 C7 30 D2 86 61 42 23 51 F3 6C 3D 0B 5F 5F D4 6A 88 A5 E5 43 62 F6 92 85 92 8E 0F 80 CA 0D 00 57 DA 69 42 2F 29 94 78 8D 38 A1 69 55 33 B5 5F 18 75 68 03 1A 50 F4 25 B0 10 08 E0 02 B9 23 6A D9 0E 94 FB D5 8B C1 36 C3 E0 47 B1 55 98 C7 A0 15 0A FD 3C 57 95 EE 7A 71 A0 1F 11 BA CF 99 2E 9C 4A 95 9E F0 0D 4B 3D B1 E7 AA 19 BC 8A C2 24 F5 C3 7B 13 E1 DD C8 B2 17 DE 33 CB BA 38 5D 25 6C 4B 0F 3B 1E 4F D4 E3 C6 CC BC 9E 6C B1 4 3 85 7E 07 20 21 FC 10 2E B3 78 09 3C 94 8C EF 2F 4B 67 67 EB 11 42 4E 06 ED EC 20 6F A0 D9 C2 35 96 84 0A 63 AC F6 E6 30 FS ED 28 AD 47 E8 9F 5B 7F 67 99 84 97 06 F7 D5 8E 8A E8 2D 8C 0E 65 A2 18 0 3 69 70 67 91 59 D9 67 14 A6 F5 D1 B9 C6 AD 94 89 47 AA 5C 86 BD 5F AB CA 59 89 8B 3A 5B 5C EC 06 AE 70 3C B0 DE 3F 1B ED 1C 33 3F 0F A5 EB E4 48 A7 29 23 D9 AB 20 CD EF 68 A2 3D E8 65 94 10 3E F3 36 F6 B4 8E 73 76 5E 20 2F C1 AE 0D B1 CC B1 27 49 60 7F 3E E0 AB 38 0A C8 6A F7 7B 99 4B D4 37 00 63 7B B3 88 9D 19 C6 64 3F 88 DA 61 B4 37 C9 69 E2 E1 3B 85 2B 81 E4 A2 3F 46 70 8D 0D CD BE 5E A0 9A 16 39 DC 98 20 A3 8D 72 8B 3F 9F 51 29 5F 6A 15 47 CD 02 03 01 00 01

**Authority Key Identifier** 9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37

**Subject Key Identifier** 94:BA:FA:EE:22:FA:32:1C:CB:05:77:B7:19:AF:12:F0:9A:6C:47:AB

**Extended Key Usage** id\_kp\_clientAuth - id\_kp\_serverAuth

**CRL Distribution Points**  
<http://crl.anf.es/crl/ANFSecureServerRootCA-ar1.crl>  
<http://www.anf.es/crl/ANFSecureServerRootCA-ar1.crl>

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.anf.es/es/documentos>

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
<http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer>

**Basic Constraints** IsCA: true

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:BA:05:3B:06:96:95:C1:74

**X509SubjectName**

**Subject CN:** ANF High Assurance Server CA

**Subject OU:** ANF Autoridad intermedia tecnicos

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

**Subject SERIAL NUMBER:** G63287510

## X509SKI

**X509 SK I** ILr67iL6MhzLBXe3Ga8S8JpsR6s=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

## Status Starting Time

2021-03-17T01:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 6.7.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

### 6.7.2 - History instance n.1 - Status: granted

## Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** [en] Qualified certificates issued by ANF High Assurance Server CA

**Name** [es] Certificados cualificados emitidos por ANF High Assurance Server CA

## Service digital identities

### X509SubjectName

**Subject CN:** ANF High Assurance Server CA

**Subject OU:** ANF Autoridad intermedia tecnicos

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

Subject SERIAL NUMBER: G63287510

X509SKI

X509 SK I ILr67iL6MhzLBXe3Ga8S8JpsR6s=

Service Status http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time 2019-11-25T01:00:00Z

6.7.2.1 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI [ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

6.8 - Service (withdrawn): Qualified timestamps issued by ANF High Assurance Server CA

Service Type Identifier http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens. [es] Un servicio de generacion de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [ en ] Qualified timestamps issued by ANF High Assurance Server CA

Name [ es ] Sellos de tiempo cualificados emitidos por ANF High Assurance Server CA

Service digital identities

Certificate fields details

Version: 3

Serial Number: 99659964253702882

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHhDCCBwYgAwIAGlIAWIONZ+rmlwDOYJKZlhcNAQELB0AwgYQeEjA0BgnVBAUTCUe2MzI4
NzUcMDELMARGAUUEBBMCRVMAJzIBGNVBAoTHKFORBBdXRvemkYwQzGlgQ2VydGlnaWNhbnV2Iv
bHJEMBRGAUUEcXMLEUcXGHEBIBFhaXoxijAgBgnVBAUTGUFORIBTZWNIcmUgl2VndmVjFh3Qg
QlEwIHRNTKxOTAJMTYzNTQWbheNMIwOTAJYTMZNTQWbheNMIwOTAJYTMZNTQWbheNMIwOTAJYTMZ
M0swCQYDVQOGEwJFJzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUz
KAYDVQQLEyFBRkYgQXQ0ODU3ZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUz
W4dEFTz3yYVWZSRBTZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUzZmUz
qMvOvX9B18mepPELpQAIimNZ6907AKdDhHqVDDTlJgAWb2DLz0KmVgVqSA1pblm3TF
EugALDlv7ZTDpI9MyHOYgyQIso5vBKMyFNBeLSDQRu7uzIBSDUUPGStkaJsp9/acx
MzpxdZLkANVdRZKp89Y8rBmcaZQh9y8m960Cv1z28mPCTHhZbDLX1Uuail
SUN9pKfK04PmONAFiaUlvKZR4jTlhaVUzV8YdWgDjD0BAOCCOACsNa2Q6U1--9WlwTbD4Ecx
VZjH0BUKTixXc56caAIEtrPm56cpWesAILPbHqpm8isik9cNTEHydLIX3PLuuhdWwLDese
TfEpy8omyoQVYByah8AuscgIPKSM9LZZTEUJ0Rb2S0Frgz2IloQK76z5D175dRrT
W39mYX8BvVjorolYwQZaIVa2hwZ5FZ2WJpXRUcaIIIHqlyGvVrylmJzpbXOwGmAs8N4/
G+0cMz8PwekSKp9mIMVakJ96GWUED7ZvnaIjN2XAvw84Vv8yJ0Igzf9glgKygCgc5LL
IDeAY3uz0IzcmQNPmIDeclh0MlEpeSPZqzQ3N0gm8Y53Iege0Ytze-tlSllhVl0QD
AQAB0IBT3CCAdkwHwYDVR0BBGwFoUnF0B6OjXSPk5gIyYHpsXcwTcwHOYDVR0BBYEFIS6
+u4+HcywV3tmvEvCabEerMAA4GAIUdDwEBwQEAWIbHAnBGNVBSIEDAeBggRgEgFBQcDAQYI
KwYBRQIHAwKCCsCAQIUFbMDMIRGAIUdHwAMHYCAAsdWGMZ0b0IAUy9pawwYVW3mlmVzL2Ny
bc9BTKZTZWNIcmVTZDZXJS290Q0EYXkLmNybDA5oDscNyzH8R0cDowl3d3dy5hmYuzXZMv
YJsl0FORINIY3VzVNIcmZklv83R0S1bcmuY38MEAGAUIUdIAQ5MDcwNOYEVROgADAiMKsG
C5GCAQIUFbWBBW0BwO8v8eEElmFuZ59cy9k9b2N1HWud09AMGIBggRgEgFBQcDAQYI
MhswJwYIKwYBBQUHMAAGG2b0dHA6Iy9hY3NwLmFuZiZl9cy9Gfph9BVBjOBggRgEgFBQcAnZE
aHR0kDowl3d3dy5hmYuzXZMvY2YVvGlnaWwNhaGVzLW8vZmZ5b2JkLlFORINIY3VzVNIcmZl
cD85RDQSSZKwDwYDVR0TAQHBAUwAwEFAAABgqkRgP9wIBAQcAOCAGeAFLS88thwvNPG
3vj7adP---ORgrvrlLb42pcw9aa60Gp9S7bHFDZKLraNIDe7FNwz2NEFBWystXO7IILCnlpUx
Fva89HNeuGsljggmavd3dHDE3XgNVdVBKmcHXARgXApaiRyGkXk0JwJSNevyG+WwP7sU/
k67b7hgHscw9R0F7teT55p9g8c8LgWg0dY5Vfzq87IbD8EPLKvSLKwYUW1yAKR8FV
sh3U/AcKch73ciaPSQ5vq0I2YCK89zFujWmSCIRPLVr9CpaZaSpkANfo404htat4YomQ
73T-2935wF4V1oopSslLpVl9HLymQpLbzwB66Wz7kmPEkbtGwmx10WAJZTCSdPUUAfz
NApPGI6fswYfE7K8v9Hsc8LgWg0dY5Vfzq87IbD8EPLKvSLKwYUW1yAKR8FV
Mol6bIOPBYYjPXBES09zQv4YTrkGxYwR79ocM6GTF+xxAcjdlJmVvXbXk78AmgOlpJ
VkfWx2lmaZn736DKL596v7maZyXh8U1BSPT1b6PUGbl+cczeIvPOAPnL6XgPRETPuUfB
U6WGD5I696ec3WLDKDbmImb5y3ygdVGBVzZaKkVYXomkVwydvw-thE=
-----END CERTIFICATE-----

**Signature algorithm:** *SHA256withRSA*

**Issuer CN:** *ANF Secure Server Root CA*

**Issuer OU:** *ANF CA Raiz*

**Issuer O:** *ANF Autoridad de Certificacion*

**Issuer C:** *ES*

**Issuer SERIAL NUMBER:** *G63287510*

**Subject CN:** *ANF High Assurance Server CA*

**Subject OU:** *ANF Autoridad intermedia tecnicos*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject C:** *ES*

**Subject SERIAL NUMBER:** *G63287510*

**Valid from:** *Thu Sep 05 18:35:44 CEST 2019*

**Valid to:** *Sun Sep 02 18:35:44 CEST 2029*

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0E:00:30:82:02:0A:02:82:02:01:00:DD:A8:CB:E2:42:F5:FD:04:9F:26:7A:93:C5:2E:94:00:88:38:A6:35:96:FD:D3:B5:CA:77:F6:C3:6E:D1:D0:54:3F:C8:4E:39:60:01:66:F6:B4:35:33:3F:4F:CA:99:5A:95:EA:40:D6:96:C9:9B:74:C5:12:DA:A0:00:B0:C8:BE:DC:D5:0E:92:20:F4:CF:F2:1C:E6:3A:83:24:15:B2:8E:71:BC:12:9C:33:21:AD:65:CF:80:F1:00:CN:45:DE:ED:89:99:41:F0:35:0F:19:2B:6D:92:72:63:B2:9F:63:ED:A7:31:88:CC:E9:DB:1B:5B:18:BE:A4:95:76:1D:06:D5:D9:44:6A:AA:13:C4:FC:F9:F8:4C:71:DD:90:89:1A:F2:D3:19:52:6B:4E:8D:08:15:75:C7:30:D2:86:61:42:23:51:F3:6C:3D:0B:5F:5F:D4:6A:88:A5:E5:43:62:F6:92:85:92:8E:0F:80:CA:0D:00:57:DA:69:42:2F:29:94:78:8D:38:A1:69:55:33:B5:5F:18:75:88:03:1A:30:F4:25:B0:10:08:E0:02:B9:23:6A:D9:0E:94:FB:DS:8B:CI:36:C3:E0:47:B1:55:98:C7:A0:15:0A:FD:3C:57:95:EE:7A:71:A0:1F:11:BA:CF:99:2E:9C:4A:95:9E:F0:0D:4B:3D:B1:E7:AA:19:BC:8A:C2:24:F5:C3:7B:13:E1:DD:C8:82:17:DE:33:CB:BA:38:5D:25:6C:4B:0F:3B:1E:4F:D4:E3:C6:CC:BC:9E:6C:B1:43:85:7E:07:20:21:FC:10:2E:B3:78:09:3C:94:8C:EF:2F:4B:67:67:EB:11:42:4E:06:ED:EC:20:6F:A0:D9:C2:35:96:84:0A:63:AC:F6:E6:30:F5:ED:28:AD:47:E8:9F:5B:7F:67:99:84:97:06:F7:DS:8E:8A:ES:2D:8C:0E:65:A2:18:03:69:70:67:91:59:D9:67:14:A6:F5:D1:B9:C6:AD:94:89:47:AA:5C:86:BD:5F:AB:CA:59:89:8B:3A:5B:5C:EC:06:AE:70:3C:B0:DE:3F:1B:ED:1C:33:3F:0F:A5:EB:E4:48:A7:29:23:D9:AB:20:CD:EF:68:A2:3D:E8:65:94:10:3E:F3:36:F6:B4:8E:73:76:5E:20:2F:C1:AE:0D:B1:CC:B1:27:49:60:7E:3E:E0:AB:88:0A:C8:6A:F7:7B:99:4B:D4:37:00:63:7B:B3:88:9D:19:C6:64:3F:88:DA:61:B4:37:C9:69:E2:E1:3B:85:2B:81:E4:A2:3F:46:70:8D:0D:CD:BE:5E:A0:9A:16:39:DC:98:20:A3:8D:72:8B:3F:9F:51:29:5F:6A:15:47:CD:02:03:01:00:01

**Authority Key Identifier** *9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37*

**Subject Key Identifier** *94:BA:FA:EE:22:FA:32:1C:CB:05:77:B7:19:AF:12:F0:9A:6C:47:AB*

**Extended Key Usage** *id\_kp\_clientAuth - id\_kp\_serverAuth*

**CRL Distribution Points**  
*http://crl.anf.es/crl/ANFSecureServerRootCA-ar1.crl*  
*http://www.anf.es/crl/ANFSecureServerRootCA-ar1.crl*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.anf.es/es/documentos*

**Authority Info Access**  
*http://ocsp.anf.es/spain/AV*  
*http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer*

**Basic Constraints** *IsCA: true*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** 8A:F5:5A:7E:98:53:66:24:CD:3E:4C:DC:EE:7F:7C:C5:91:46:0D:B7:81:BA:84:50:BA:05:3B:06:96:95:C1:74

## X509SubjectName

**Subject CN:** ANF High Assurance Server CA

**Subject OU:** ANF Autoridad intermedia tecnicos

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

**Subject SERIAL NUMBER:** G63287510

## X509SKI

**X509 SK I** ILr67iL6MhzLBXe3Ga8S8JpsR6s=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

## Status Starting Time

2022-01-11T02:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 6.8.1 - History instance n.1 - Status: granted

## Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

## Service Name

**Name** [en] Qualified timestamps issued by ANF High Assurance Server CA

**Name** [es] Sellos de tiempo cualificados emitidos por ANF High Assurance Server CA

## Service digital identities

### X509SubjectName

**Subject CN:** ANF High Assurance Server CA

**Subject OU:** ANF Autoridad intermedia tecnicos



**Signature algorithm:** *SHA256withRSA*

**Issuer CN:** *ANF Assured ID CA1*

**Issuer SERIAL NUMBER:** *G63287510*

**Issuer E:** *info@anf.es*

**Issuer OU:** *ANF Autoridad Intermedia de Identidad*

**Issuer O:** *ANF Autoridad de Certificacion*

**Issuer L:** *Barcelona (see current address at <http://www.anf.es/es/address-direccion.html> )*

**Issuer ST:** *Barcelona*

**Issuer C:** *ES*

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject CN:** *ANF AC Servicio de validación*

**Subject E:** *soporte@anf.es*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona*

**Subject ST:** *Cataluña*

**Subject C:** *ES*

**Valid from:** *Thu Dec 03 17:00:57 CET 2020*

**Valid to:** *Sat Dec 03 17:00:57 CET 2022*

**Public Key:** *30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:BD:08:D9:4E:A0:BB:8C:10:0C:09:11:9B:5F:D8:1F:A3:E3:64:6A:4A:03:64:CE:7F:76:B1:DE:7D:94:CD:F9:11:E5:46:F9:33:2C:10:78:87:CF:3B:89:E1:1D:C8:11:6C:C8:F7:49:17:3D:9C:B6:06:CF:6D:23:0C:A6:C3:CF:6D:52:A5:CE:EE:6D:50:AA:0D:24:86:72:AA:33:38:FF:78:66:6F:DA:09:04:5D:48:F6:ED:ED:AB:44:3E:19:AD:47:A3:1D:D:22:14:2F:D4:9D:1F:05:6D:79:8E:23:79:F8:80:05:0F:E3:42:74:11:31:4B:16:22:80:FB:82:68:2F:AB:82:68:12:4E:CA:65:F6:80:72:C5:B4:8F:07:0E:BD:31:3B:BE:D7:06:44:8B:4F:74:CC:99:8C:8A:9E:E6:3B:5E:A9:C4:61:0D:45:4C:C7:C3:07:A6:92:E8:5F:75:C1:25:CF:95:5B:0B:4C:B0:7F:2C:B4:4A:54:3F:B7:AD:F1:0B:90:E8:8C:CB:42:AA:FC:F9:FB:A0:86:88:B1:74:EA:8A:42:6E:36:74:12:DC:53:3E:02:01:06:E3:55:6E:E0:55:EC:51:FB:04:E7:3D:3C:13:CD:F1:63:A7:4C:E7:14:2B:99:84:5C:21:CA:FF:CE:93:ED:19:ED:B6:20:D2:AF:02:03:01:00:01*

**Authority Key Identifier** *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*

**Subject Key Identifier** *77:F8:48:FC:FA:22:DC:51:FD:89:73:E4:90:49:B5:B3:00:7F:26:0B*

**Subject Alternative Name** *soporte@anf.es*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *[https://www.anf.es/crl/ANF\\_Assured\\_ID\\_CA1\\_SHA256.crl](https://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl)*



**Certificate Policies***Policy OID: 1.3.6.1.4.1.18332.25.1.1.1**CPS pointer: <https://www.anf.es/documentos>**Policy OID: 0.4.0.194112.1.1***Authority Info Access***<http://ocsp.anf.es/spain/AV>**[http://www.anf.es/es/certificates\\_download/ANF\\_Assured\\_ID\\_CA1\\_SHA256.cer](http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer)***Basic Constraints***IsCA: false***QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***8D:25:C0:1A:24:CB:58:33:E4:97:46:90:D1:11:36:0A:B1:2A:F0:72:21:FD:8C:0C:7D:41:22:D9:12:54:65:C7***X509SubjectName****Subject 2.5.4.97:***VATES-G63287510***Subject CN:***ANF AC Servicio de validación***Subject E:***soporte@anf.es***Subject OU:***Certificado Cualificado de Sello Electronico***Subject O:***ANF Autoridad de Certificacion***Subject L:***Barcelona***Subject ST:***Cataluña***Subject C:***ES***X509SKI****X509 SK I***d/hI/Poi3FH9iXPkkEmIswB/Jgs=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2023-02-15T00:00:00Z***6.9.1 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

6.9.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

6.9.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

**Service Name**

**Name** [ en ] *Qualified validation service for qualified electronic signatures and qualified electronic seals by ANF AC Servicio de validación*

**Name** [ es ] *Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados por ANF AC Servicio de validación*

Service digital identities**X509SubjectName**

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject CN:** *ANF AC Servicio de validación*

**Subject E:** *soporte@anf.es*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona*

**Subject ST:** *Cataluña*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *d/hI/Poi3FH9iXPkkEm1swB/Jgs=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2021-01-26T01:00:00Z*





**Certificate Policies***Policy OID: 1.3.6.1.4.1.18332.25.1.1.1**CPS pointer: <https://www.anf.es/documentos>**Policy OID: 0.4.0.194112.1.1***Authority Info Access***<http://ocsp.anf.es/spain/AV>**[http://www.anf.es/es/certificates\\_download/ANF\\_Assured\\_ID\\_CA1\\_SHA256.cer](http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer)***Basic Constraints***IsCA: false***QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***20:94:FB:22:EC:CD:E5:50:9C:B8:87:D5:B8:34:2D:84:0C:75:D0:5E:46:1D:B7:82:00:14:0D:18:22:  
B8:3C:94***X509SubjectName****Subject 2.5.4.97:***VATES-G63287510***Subject CN:***Sign to Sign Delivery Services***Subject E:***soporte@anf.es***Subject OU:***Certificado Cualificado de Sello Electronico***Subject O:***ANF Autoridad de Certificacion***Subject L:***Barcelona***Subject ST:***Cataluña***Subject C:***ES***X509SKI****X509 SK I***ebLudB3q/eytq7utl/KmzdRLXfl=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2023-02-15T00:00:00Z***6.10.1 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

### Service Name

**Name** [en] *Qualified electronic registered delivery service ANF AC*

**Name** [es] *Servicio cualificado de entrega electrónica certificada de ANF AC*

### Service digital identities

#### X509SubjectName

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject CN:** *Sign to Sign Delivery Services*

**Subject E:** *soporte@anf.es*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona*

**Subject ST:** *Cataluña*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *ebLudB3q/eytq7utl/KmzdRLXfl=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2021-03-17T01:00:00Z*

### 6.11 - Service (withdrawn): Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

**Service type description** [en] *A preservation service for qualified electronic signatures.*

[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

### Service Name

**Name** [en] *Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC*



**Subject L:** *Barcelona*

**Subject ST:** *Cataluña*

**Subject C:** *ES*

**Valid from:** *Thu Dec 03 11:01:00 CET 2020*

**Valid to:** *Sat Dec 03 11:01:00 CET 2022*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100A53EED35E674201D4A1885DF3EB150DA79DA7819B16DE1ECDA7D E3E8B61AD490952B  
F6946BCF8FB1341DB0D3DA9D5A16AA8493CC2E30F7FEFF523D3C8C7A02EE72D94EA4D994D682D885401C51E1DDA9E961448C744F2D67D75D16B0AF1B20229  
F08BFB226E7D1C1EA779A5D9AD88140762C596B460B9182B3E537B9F39A3550A8A5674892E9A29257804C98F2B82B4C524218C3696F15AC A7DF593AFAEE66B8  
FFCD E2A038E0EB6E4E6A3CD8E75E DE78ECFA98E23FE3099E2D B27669B5CA B0B0E60E407E041A2BAD57374C3F9F3DCB30FD94F31A38724DC5BE9E DE5510CE C823  
8FB91089FDFAAF6D839B05C74BEB085615DD D1462165C1D4F763E55F0203010001

**Authority Key Identifier** *35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D*

**Subject Key Identifier** *11:5E:8B:8B:62:23:EB:73:D1:95:0B:C6:F8:05:EE:A3:FB:16:92:53*

**Subject Alternative Name** *soporte@anf.es*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *https://www.anf.es/crl/ANF\_Assured\_ID\_CA1\_SHA256.crl*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.18332.25.1.1.1*  
*CPS pointer: https://www.anf.es/documentos*  
*Policy OID: 0.4.0.194112.1.1*

**Authority Info Access**  
*http://ocsp.anf.es/spain/AV*  
*http://www.anf.es/es/certificates\_download/ANF\_Assured\_ID\_CA1\_SHA256.cer*

**Basic Constraints** *IsCA: false*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *54:AC:F8:77:4B:6F:AB:83:7B:AB:F5:47:3E:C7:8B:13:85:7E:5E:D1:D7:D5:9F:30:B3:5C:9C:EA:3  
E:9F:C8:62*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject CN:** *ANF AC Servicio de conservación*

**Subject E:** *soporte@anf.es*



**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject L:** *Barcelona*

**Subject ST:** *Cataluña*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *EV6Li2Ij63PRIQvG+AXuo/sWkIM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-02-15T00:00:00Z*

**6.11.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**6.11.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**6.11.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

**Service Name**

**Name** *[ en ]* *Qualified preservation service for qualified electronic signatures and qualified electronic seals by ANF AC*

**Name** *[ es ]* *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados de ANF AC*

**Service digital identities****X509SubjectName**

Subject 2.5.4.97: VATES-G63287510

Subject CN: ANF AC Servicio de conservación

Subject E: soporte@anf.es

Subject OU: Certificado Cualificado de Sello Electronico

Subject O: ANF Autoridad de Certificacion

Subject L: Barcelona

Subject ST: Cataluña

Subject C: ES

**X509SKI**

X509 SK I EV6Li2Ij63PRIQvG+AXuo/sWklM=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2021-03-17T01:00:00Z

**6.11.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**6.11.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**6.12 - Service (granted): Qualified Certificates issued by ANF Secure Server CA**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

Name [ en ] Qualified Certificates issued by ANF Secure Server CA



**Authority Key Identifier** *9C:5F:D0:6C:63:A3:5F:93:CA:93:98:08:AD:8C:87:A5:2C:5C:C1:37*

**Subject Key Identifier** *96:02:AD:E4:C9:F9:4F:B0:AD:38:0B:A4:FE:AE:6C:A6:6E:E4:7C:8A*

**Extended Key Usage** *id\_kp\_serverAuth*

**CRL Distribution Points** *http://crl.anf.es/crl/ANFSecureServerRootCA-ar1.crl*  
*http://www.anf.es/crl/ANFSecureServerRootCA-ar1.crl*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.anf.es/es/documentos*

**Authority Info Access** *http://ocsp.anf.es/spain/AV*  
*http://www.anf.es/es/certificates-download/ANFSecureServerRootCA.cer*

**Basic Constraints** *IsCA: true*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *30:6B:F8:09:96:36:A4:4F:FF:B5:EE:DC:E6:E3:0C:0F:36:C7:D4:3F:6C:CA:5A:2C:A3:AB:71:66:8F:35:33:20*

**X509SubjectName**

**Subject CN:** *ANF Secure Server CA*

**Subject OU:** *ANF Autoridad intermedia tecnicos*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject C:** *ES*

**Subject SERIAL NUMBER:** *G63287510*

**X509SKI**

**X509 SK I** *lgKt5Mn5T7CtOAuk/q5spm7kflO=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-03-17T01:00:00Z*

**6.12.1 - Extension (critical): additionalServiceInformation**



**Issuer SERIAL NUMBER:** G63287510

**Subject CN:** ANF AC Qualified Certificates for eSignature

**Subject OU:** Certificados Cualificados de Firma Electronica

**Subject 2.5.4.97:** VATES-G63287510

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

**Valid from:** Fri Nov 11 13:44:14 CET 2022

**Valid to:** Thu Nov 08 13:44:14 CET 2035

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C8DEFC2D4C9E4A6CFDE670E1658700CEA8876D446BFA99C4A4AD70C1B1F8ADB080C67  
F1C9DAE67E72C8C710A6C1A1C894A43BDF6387E439B67D873A52167313E34C37960249C8984B53233A737F78408AF62300430A43C62CD8F827CEE1B6E02E175E2609  
572B5ACFB058A06DC36A051747728B10836A18C9A1ABE973DBF25685DB692C16306A646DC2E07C4DDC6D5A5F2AB84B63BAC6D0AF2AE5FD90D597DF9E9E9E5F4  
7511E0612A48B535D2E2F2A3FC299AD87605280B92B742E540944CE67E33B89B581B717A5028F28953456165DD12E9C0CB94B0960ABDF981D95A5D06C33A4020  
AA63A81299E44D42E6F55F6A6A88AEB302ED3C359004B4AC79791E7392225A47E6F8E1BD008F08C7F5177422B457E7A55552575A722B3B9A2498207389E2E6923ED  
0E528D8B76041956E0CCFF182101E71BC9AA2B32778A6E58C8DC965A06ED5B2D79778BA68A173106DA34D707C7C487E6B6BF82C44A65E7CE7756C02DF34BAD32B2  
E0C2C8353BD2F2B152D22D9F92F1E1C26BA30196E48B1F88073E39023A99C8CC00976C21D98FEF078310E30179B3A6192F57324A9B6BE2593FF1430F8234FCA35  
0AEBAD95EE9259A83D154994AE6232A14B720AA3E6790406FC7C50F8736EA4D75F16C17DD8B06A86F7CC7B3A0DA82814BEF3C032245FE7A1019AF3219503302C0  
131D0D852DE4E8127D20CFA1D40A2EC9460FFAD.E90203010001

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Subject Key Identifier** 2A:2F:33:FC:BD:6C:7F:58:06:53:18:40:E2:7E:F6:B9:B0:13:8B:70

**CRL Distribution Points** [http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://anf.es/repositorio-legal/>  
CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC.]

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
[http://crl.anf.es/certificates\\_download/ANF\\_Global\\_Root\\_CA\\_SHA256\\_2036.cer](http://crl.anf.es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer)

**Basic Constraints** IsCA: true

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** B7:CD:F2:3A:73:A2:DA:1B:51:5A:64:40:3E:90:A3:B9:0C:45:DD:FB:B2:55:8B:C1:C1:2F:B9:BC:FA:2E:5A:23

**X509SubjectName**

**Subject CN:** ANF AC Qualified Certificates for eSignature

**Subject OU:** Certificados Cualificados de Firma Electronica

**Subject 2.5.4.97:** VATES-G63287510

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

## X509SKI

**X509 SK I** Ki8z/L1sf1gGUxhA4n72ubATi3A=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2023-01-31T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 6.13.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 6.13.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.18332.3.4.1.8.22

### 6.14 - Service (granted): Certificados electrónicos cualificados emitidos por «ANF AC Qualified Certificates for eSeal»

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.





**Valid to:** Thu Nov 08 14:01:36 CET 2035

**Public Key:**  
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:E8:BF:E5:ED:F3:12:DF:9B:1B:1C:6E:35:D1:F3:16:EA:7B:44:18:13:95:EF:77:94:6E:CC:F2:ED:B1:C6:31:A3:53:98:8  
8:20:62:45:9B:A6:AB:CD:CS:FB:96:D6:77:F8:5C:CF:EE:77:11:C7:18:9B:7B:91:8C:33:B0:99:56:36:A0:F9:17:0A:61:22:C4:B4:06:02:36:33:47:D3:A3:0F:41:5B:12:8D:57:4C:68:85:7C:2B:FA:97:0D:A1:9A:CB:8C:5B:A8:E1  
54:BF:61:4C:A5:FE:1C:73:DF:40:04:88:28:CD:8D:66:BD:D2:1D:54:49:FB:5E:B0:91:82:89:07:62:31:70:6E:8C:38:98:2D:56:2C:D2:82:0D:23:64:99:B7:71:3C:31:05:71:2D:3D:04:7E:E6:3D:E5:65:86:B0:F8:75:24:52:4D:AE  
88:15:E6:56:26:07:84:39:61:52:02:34:10:96:F6:3C:18:57:9A:16:DE:DA:99:FE:CE:51:D3:B7:B3:A4:2B:63:CD:B0:00:6F:F4:F9:37:3F:86:54:9E:FA:0F:5A:97:35:95:17:02:CB:46:A5:D5:35:62:42:FB:68:FF:48:96:9F:D8:4E:3F:  
65:BD:92:E9:D0:C5:0F:49:9C:80:48:2D:67:7C:33:50:3A:40:96:82:A6:EE:1D:5A:AD:1B:FC:0A:EF:D2:CE:1F:0B:A2:1A:97:C1:BB:E2:9A:1B:1A:56:28:98:69:A7:38:43:0A:4D:C4:1A:34:87:06:2C:74:D6:9E:43:6C:86:84:FF:  
8C:7E:B6:CB:19:22:3A:AE:1E:F7:4E:DE:D0:7D:FC:7D:69:59:00:E8:32:A7:54:8E:9C:92:F3:FA:16:8E:85:0A:F0:BF:31:A3:E3:02:2F:3E:EE:B0:B7:D7:B0:F4:DF:F9:63:82:69:58:38:13:B4:6F:3D:0F:45:77:A0:BE:1E:37:  
EC:DE:08:D9:EA:31:6B:92:EB:CB:EF:F9:41:65:6C:8B:50:63:F4:5C:58:43:C2:8F:1E:51:CS:75:E6:D6:C2:93:55:F0:3F:41:65:86:9B:47:6C:6E:82:E6:4A:97:55:77:49:12:90:A6:9F:30:DD:1D:4B:92:FB:C4:B6:D3:9E:A1:79:AE  
B3:FF:7A:D1:16:66:09:38:E4:63:02:48:C7:79:F3:39:D2:E2:1E:96:91:DF:CS:E2:3C:54:65:7A:1E:A9:42:E5:23:86:51:C4:69:0D:39:D2:15:AE:84:8B:3D:C1:5C:4F:2D:21:CF:7C:57:54:1D:1B:C0:CD:D5:36:88:9F:29:AE:CA:2  
701:CA:E3:A4:CA:03:DF:FC:B6:58:FA:6A:4B:2C:FF:6E:45:02:03:01:00:01

**Authority Key Identifier** 87:FA:9E:DF:52:76:75:EC:49:4A:20:6F:5B:70:96:8F:9D:EF:BB:17

**Subject Key Identifier** 7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C

**CRL Distribution Points** [http://crl.anf.es/crl/ANF\\_Global\\_Root\\_CA\\_2036\\_arl.crl](http://crl.anf.es/crl/ANF_Global_Root_CA_2036_arl.crl)

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://anf.es/repositorio-legal/>  
CPS text: [Certificado de Autoridad de Certificación Intermedia. Sujeto a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de ANF AC]

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
[http://crl.anf.es/certificates\\_download/ANF\\_Global\\_Root\\_CA\\_SHA256\\_2036.cer](http://crl.anf.es/certificates_download/ANF_Global_Root_CA_SHA256_2036.cer)

**Basic Constraints** IsCA: true

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 34:31:29:2A:66:FB:3E:A5:3F:8B:70:6E:A4:D9:80:38:1C:B8:65:DF:6C:99:F0:52:45:36:54:5B:58:C  
F:9F:FF

**X509SubjectName**

**Subject CN:** ANF AC Qualified Certificates for eSeal

**Subject OU:** Certificados Cualificados de Sello Electronico

**Subject 2.5.4.97:** VATES-G63287510

**Subject O:** ANF Autoridad de Certificacion

**Subject C:** ES

**X509SKI**

**X509 SK I** fNOsW6NNyfEwAnfdTrHVXWHkyow=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2023-01-31T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**6.14.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**6.14.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] <urn:oid:1.3.6.1.4.1.18332.25.1.1.9>

**Policy Identifier:**

**Identifier** [OIDAsURN] <urn:oid:1.3.6.1.4.1.18332.25.1.1.11>

**6.15 - Service (granted): Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de validación"**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

**Service type description** [en] undefined.  
[es] undefined.

**Service Name**

**Name** [en] *Qualified validation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de validación"*

**Name** [es] *Servicios de Validación de firma electrónicas cualificadas y sellos electrónicos cualificados "ANF AC Servicio de validación"*

**Service digital identities****Certificate fields details**

Version:

3

Serial Number:

995616158423738526593418293

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHpiCCBY6gAwIBAgI... ANF AC Qualified Certificates for eSeal

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

ANF AC Qualified Certificates for eSeal

Issuer OU:

Certificados Cualificados de Sello Electronico

Issuer 2.5.4.97:

VATES-G63287510

Issuer O:

ANF Autoridad de Certificacion

Issuer C:

ES

Subject L:

BARCELONA

Subject ST:

BARCELONA

Subject 2.5.4.97:

VATES-G63287510

Subject OU:

Certificado Cualificado de Sello Electronico

Subject O:

ANF Autoridad de Certificacion

Subject CN:

ANF AC Servicio de validación

Subject SERIAL NUMBER:

G63287510

Subject C:

ES

Valid from:

Wed Feb 01 17:06:59 CET 2023

Valid to:

Fri Jan 31 17:06:59 CET 2025

Public Key:

3082.01.22.30.0D.06.09.2A.86.48.8E.F7.0D.01.01.01.05.00.03.82.01.0F.00.30.82.01.0A.02.82.01.01.00.97.DA.77.03.7C.24.D7.04.30.A3.F7.AE.FA.59.BA.D7.41.EC.6D.96.96.C7.BC.B2.C8.06.07.18.CB.34.F3.C2.65.EB.97.6C.63.5B.32.FF.36.86.43.0F.EA.74.2F.12.04.C7.AC.7C.2E.43.7E.B6.74.7C.A5.46.19.A5.82.B1.ED.04.01.CD.5D.04.5C.66.59.D0.8E.B3.45.49.E3.63.2E.4D.0D.05.EE.B8.13.9B.B4.A6.A4.0E.47.EA.90.C4.99.E9.96.05.26.5A.81.FA.71.55.66.8E.A0.46.E5.F9.CA.7C.1C.CE.00.3E.02.CB.E9.09.88.46.FB.DD.E3.4F.9B.88.F1.01.E7.97.52.77.A1.EA.F7.2B.1B.3B.D7.15.2E.B2.C1.0D.CC.32.79.88.89.80.1D.57.89.23.22.47.34.F1.86.55.23.F3.33.C1.15.0A.78.64.1C.A8.F3.F4.C6.E8.CF.83.2A.41.2A.DF.4F.CB.86.13.45.17.24.5A.5A.31.B9.F2.36.04.9A.6E.C6.7B.FD.D1.32.1C.CB.66.BE.10.23.84.37.25.CD.D8.0D.01.73.77.CO.C1.32.15.1F.36.8E.E8.8E.A6.8A.50.25.DF.2F.A5.39.43.11.E1.D1.FF.11.2B.6A.EF.74.72.4B.27.AD.2A.C2.03.03.01.00.01

**Authority Key Identifier** *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*

**Subject Key Identifier** *52:D6:9F:52:83:94:E6:87:CA:9B:B9:46:42:E3:FB:69:1F:A3:80:1B*

**Subject Alternative Name**  
*soporte@anf.es*  
*OID.1.3.6.1.4.1.18332.10.4=G63287510*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *http://crl.anf.es/crl/ANF\_AC\_Qualified\_Certificates\_for\_eSeal.crl*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*  
*CPS pointer: http://www.anf.es/documentos*  
*Policy OID: 0.4.0.194112.1.3*

**Authority Info Access**  
*http://ocsp.anf.es/spain/AV*  
*http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer*

**Basic Constraints** *IsCA: false*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A3:E8:60:F2:D9:A5:E7:B4:B2:63:4B:87:BC:AC:1E:0D:3D:F7:56:54:F8:90:2D:83:DA:16:60:A3:F  
D:D6:FD:92*

**X509SubjectName**

**Subject L:** *BARCELONA*

**Subject ST:** *BARCELONA*

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject CN:** *ANF AC Servicio de validación*

**Subject SERIAL NUMBER:** *G63287510*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *UtafUoOU5ofKm7lGQuP7aR+jgBs=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2023-02-15T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**6.15.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**6.15.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**6.16 - Service (granted): Qualified electronic registered delivery service by "Sign to Sign Delivery Services"**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

**Service type description** *[en] An electronic delivery service providing qualified electronic deliveries.*  
*[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

**Service Name**

**Name** *[en] Qualified electronic registered delivery service by "Sign to Sign Delivery Services"*

**Name** *[es] Servicio cualificado de entrega electrónica certificada "Sign to Sign Delivery Services"*

**Service digital identities****Certificate fields details**

**Version:** 3



**Subject Key Identifier** *75:67:1B:D1:86:EB:46:D0:25:E3:97:A0:D4:63:03:3C:B0:F4:C5:CD*

**Subject Alternative Name** *soporte@anf.es*  
*OID.1.3.6.1.4.1.18332.10.4=G63287510*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *http://crl.anf.es/crl/ANF\_AC\_Qualified\_Certificates\_for\_eSeal.crl*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*  
*CPS pointer: http://www.anf.es/documentos*  
*Policy OID: 0.4.0.194112.1.3*

**Authority Info Access** *http://ocsp.anf.es/spain/AV*  
*http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer*

**Basic Constraints** *IsCA: false*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F6:91:23:12:D8:88:D3:BD:A4:E7:05:CE:BD:2A:E8:65:5B:15:05:E7:F3:AA:4B:23:F0:AA:20:7C:5D:0E:A1:A0*

**X509SubjectName**

**Subject L:** *BARCELONA*

**Subject ST:** *BARCELONA*

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject CN:** *Sign to Sign Delivery Services*

**Subject SERIAL NUMBER:** *G63287510*

**Subject C:** *ES*

**X509SKI**

X509 SK I

dWcb0YbrRtA145eg1GMDPLD0xc0=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Service status description

[en] undefined.
[es] undefined.

Status Starting Time

2023-02-15T00:00:00Z

Scheme Service Definition URI

URI [en]

https://avancedigital.mineco.gob.es/en-
us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

URI [es]

https://avancedigital.mineco.gob.es/es-
us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx

6.17 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de conservación"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

Service type description

[en] A preservation service for qualified electronic signatures.
[es] Un servicio de la preservación de las firmas electrónicas reconocidas.

Service Name

Name [en]

Qualified preservation service for qualified electronic signatures and qualified electronic seals "ANF AC Servicio de conservación"

Name [es]

Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados "ANF AC Servicio de conservación"

Service digital identities

Certificate fields details

Version:

3

Serial Number:

995304246984473328978043403

X509 Certificate

-----BEGIN CERTIFICATE-----
MIHhDCCBZCgAwIBAgI...
-----END CERTIFICATE-----



**Signature algorithm:** *SHA256withRSA*

**Issuer CN:** *ANF AC Qualified Certificates for eSeal*

**Issuer OU:** *Certificados Cualificados de Sello Electronico*

**Issuer 2.5.4.97:** *VATES-G63287510*

**Issuer O:** *ANF Autoridad de Certificacion*

**Issuer C:** *ES*

**Subject L:** *BARCELONA*

**Subject ST:** *BARCELONA*

**Subject 2.5.4.97:** *VATES-G63287510*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *ANF Autoridad de Certificacion*

**Subject CN:** *ANF AC Servicio de conservación*

**Subject SERIAL NUMBER:** *G63287510*

**Subject C:** *ES*

**Valid from:** *Wed Feb 01 17:06:59 CET 2023*

**Valid to:** *Fri Jan 31 17:06:59 CET 2025*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A028201010096EA9D037947EA812DF95362CE9D7F654E651995DE6D584EFD0884213D45C4492206344F6C4D7B8E07DE749400DCAC1594AA339FDE3B1681BA4D53AF1388309ADD853293D1376082353D66A0A9713198C91666B7E33DEEC4BF3F3D7DDF2718233138446FB48448FB7C331DF417DE6C6D711A40CB3A82EA58021BF93BE6753381FFC47B7AE5D695FB0F9FE182F3FA6814ADBA861C54F172380A250BB946FE8B7FA1EE173B6045E4969A265235151E227C9D8E9D8106978F984B3006BD E36F805DFBBA3C90DDBB C8E07671D643F3B95223E366B77B3CF6DE3DE0F21EBE29602E0526AACE E6C1DD3BAEC5488606E05E95DB5BD1ABFE69C01AB92A6D915D6C9B04A10203010001

**Authority Key Identifier** *7C:D3:AC:5B:A3:4D:C9:F1:30:02:77:DD:4E:B1:D5:5D:61:E4:CA:8C*

**Subject Key Identifier** *31:A0:3E:00:2E:C7:E3:95:6A:7D:CF:0E:3C:D0:34:FE:6B:B3:AC:39*

**Subject Alternative Name**  
*soporte@anf.es*  
*OID.1.3.6.1.4.1.18332.10.4=G63287510*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points** *http://crl.anf.es/crl/ANF\_AC\_Qualified\_Certificates\_for\_eSeal.crl*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.18332.25.1.1.9*  
*CPS pointer: http://www.anf.es/documentos*  
*Policy OID: 0.4.0.194112.1.3*

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
<http://crl.anf.es/certificates-download/ANFACQualifiedCertificatesforeSeal.cer>

**Basic Constraints**  
*IsCA: false*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Key Usage:**  
*digitalSignature - nonRepudiation*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*A9:F1:05:6A:B9:B3:F9:3C:0F:35:4A:C1:F4:00:6D:9E:ED:41:F8:95:95:29:4B:ED:2E:2E:4D:16:9E:F5:1F:D9*

**X509SubjectName**

**Subject L:**  
*BARCELONA*

**Subject ST:**  
*BARCELONA*

**Subject 2.5.4.97:**  
*VATES-G63287510*

**Subject OU:**  
*Certificado Cualificado de Sello Electronico*

**Subject O:**  
*ANF Autoridad de Certificacion*

**Subject CN:**  
*ANF AC Servicio de conservación*

**Subject SERIAL NUMBER:**  
*G63287510*

**Subject C:**  
*ES*

**X509SKI**

**X509 SK I**  
*MaA+AC7H45Vqfc8OPNA0/muzrDk=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**  
*2023-02-15T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**6.17.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]*<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**6.17.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]*<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

## 7 - TSP: Consejo General de la Abogacía Española

### TSP Name

**Name** [ en ] *Consejo General de la Abogacía Española*

**Name** [ es ] *Consejo General de la Abogacía Española*

### TSP Trade Name

**Name** [ en ] *VATES-Q2863006I*

**Name** [ en ] *AC ABOGACÍA*

**Name** [ es ] *AC ABOGACÍA*

**Name** [ en ] *Consejo General de la Abogacia NIF:Q-2863006I*

**Name** [ en ] *Consejo General de la Abogacia NIF Q2863006I*

**Name** [ en ] *Consejo General de la Abogacia*

**Name** [ en ] *CONSEJO GENERAL DE LA ABOGACIA*

### PostalAddress

**Street Address** [ en ] *Paseo de Recoletos, 13*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28004*

**Country Name** [ en ] *ES*

### PostalAddress

**Street Address** [ es ] *Paseo de Recoletos, 13*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28004*

**Country Name** [ es ] *ES*

### ElectronicAddress



**Subject CN:** *ACA - Certificados Corporativos*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Subject E:** *ac@acabogacia.org*

**Subject L:** *Madrid*

**Subject C:** *ES*

**Valid from:** *Wed Jun 15 09:28:04 CEST 2005*

**Valid to:** *Wed Jun 14 00:00:00 CEST 2017*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100CD46D0140C87AC8AD1766635577311BD76AA09A9A58334AA2A13368A5BC836958395CAF41C3F74F839508EFDA544F8C63158641F5D558A786CE2D7B242753753DDB028D8CAB7C0C1B4E886469DEAE088271AC71CC6B47B0D2ED24C11CA665C91E142BA46737321A2F4469252B43A29629E402B61E044D3CFEADB31BC8A78204ECCD9E64C20AD99ABDAD7D2E8DF55C01614798FD5482A4970B08A43A0275FC9A49DB2DC6749E7AF6CA9BEDCAFCD3DB2C6106056283F880D191A8FC6D40E428970833D2B775CC4E658745215A873B8A15E3AA6D1C679F2801C2BDDB6C099C8D7FCA11839C23063BCF928F6E45433FC63BCC9E5A4973022AE59F66AB97DB575DAB0203010001

**Issuer Alternative Name** *ac@acabogacia.org*

**Subject Alternative Name** *ac@acabogacia.org*  
*http://www.acabogacia.org*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *5A:79:4C:A1:0C:FC:08:16:2C:C2:85:45:4F:32:AB:E7:2B:45:C0:11*

**Authority Key Identifier** *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.16533.10.1.1*  
*CPS pointer: uri:http://www.acabogacia.org/doc*  
*CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]*

**CRL Distribution Points** *http://www.acabogacia.org/crl/acabogacia.crl*  
*http://crl.acabogacia.org/crl/acabogacia.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *C3:2F:2C:6D:70:6F:AC:23:94:7D:2B:09:21:A4:B5:A6:98:0B:E7:96:BB:2D:D6:F2:11:8E:BA:6D:82:54:A8:FC*

**X509SubjectName**

**Subject CN:** *ACA - Certificados Corporativos*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Subject E:** *ac@acabogacia.org*

**Subject L:** *Madrid*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2017-12-04T01:00:00Z*

#### 7.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1*

#### 7.1.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 7.1.3 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified certificate provided by AC Certificados Corporativos*

**Name** *[es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos*

#### Service digital identities

**X509SubjectName**

**Subject CN:** *ACA - Certificados Corporativos*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Subject E:** *ac@acabogacia.org*

**Subject L:** *Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *WnIMoQz8CBYswoVFTzKr5ytFwBE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**7.1.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	<i>[OIDAsURN]</i>	<i>urn:oid:1.3.6.1.4.1.16533.10.5.1</i>
-------------------	-------------------	---

**7.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	-------------	--

**7.1.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

<b>Name</b>	<i>[en]</i>	<i>Qualified certificate provided by AC Certificados Corporativos</i>
-------------	-------------	---

<b>Name</b>	<i>[es]</i>	<i>Certificados Reconocidos emitidos por CA AC Certificados Corporativos</i>
-------------	-------------	--

**Service digital identities**



**X509SubjectName**

**Subject CN:** ACA - Certificados Corporativos

**Subject OU:** Autoridad de Certificación de la Abogacia

**Subject O:** Consejo General de la Abogacia NIF:Q-2863006I

**Subject E:** ac@acabogacia.org

**Subject L:** Madrid

**Subject C:** ES

**X509SKI**

**X509 SK I** WnlMoQz8CBYswoVFTzKr5ytFwBE=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time**

2007-05-22T00:00:00Z

**7.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

**7.2 - Service (withdrawn): Qualified Digital certificate provided by Autoridad de Certificación de la Abogacia****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

**Service Name**

**Name** [en] Qualified Digital certificate provided by Autoridad de Certificación de la Abogacia



**Subject Alternative Name** *http://www.acabogacia.org*

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *22:BA:59:71:AC:73:A4:13:6D:3C:18:AF:F5:D0:82:E3:56:BD:93:B0*

**Authority Key Identifier** *33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.13177.10.10.1*  
*CPS pointer: http://www.firmaprofesional.com/cps/cps.htm*

**CRL Distribution Points** *http://crl.firmaprofesional.com/firmaprofesional.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *BC:85:94:4D:A4:E3:04:E9:B7:05:8A:19:B6:73:AF:95:F5:40:D0:0D:CD:A0:10:90:3A:00:9D:A2:F  
B:AC:AB:6E*

**X509SubjectName**

**Subject CN:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF Q28630061*

**Subject OU:** *Consulte http://www.acabogacia.org*

**Subject L:** *Paseo de Recoletos 13 Madrid*

**Subject E:** *ac@acabogacia.org*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

**7.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**7.2.2 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

### Service Name

**Name** *[ en ]* *Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía*

### Service digital identities

#### X509SubjectName

**Subject CN:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF Q2863006I*

**Subject OU:** *Consulte <http://www.acabogacia.org>*

**Subject L:** *Paseo de Recoletos 13 Madrid*

**Subject E:** *ac@acabogacia.org*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *IrpZcaxzpBNtPBiv9dCC41a9k7A=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

**Status Starting Time** *2007-05-21T22:00:00Z*

### 7.2.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

### Service Name

**Name** *[ en ]* *Qualified Digital certificate provided by Autoridad de Certificación de la Abogacía*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA Autoridad de Certificación de la Abogacía*

### Service digital identities

#### X509SubjectName

**Subject CN:** *Autoridad de Certificación de la Abogacia*

**Subject O:** *Consejo General de la Abogacia NIF Q2863006I*



**Issuer CN:** *Autoridad de Certificacion de la Abogacia*

**Issuer O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Issuer C:** *ES*

**Subject CN:** *ACA - Trusted Certificates*

**Subject O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject E:** *ca@acabogacia.org*

**Subject C:** *ES*

**Valid from:** *Tue Jun 02 12:42:10 CEST 2009*

**Valid to:** *Sat Jun 02 00:00:00 CEST 2029*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B3799F43E5D001B065D6455BA620D36AC30FBAE1904E11210340BCA211DBD863B1B0C04AE4731A047A77A621822769B387C8D444776C1D4C3986DDA0CE54739713783FA28B75E78C32AA6723D69EE338B79E3F35573829F9A01EA4B09047E1E9D7E78A742892465A5F612E91B1A7534SEFC9BEBD16C0DB658C3A65AEBB4113F8067CF42DCBA814DEC8D8127C300D8C84C012043A6BFBA84192AC6838889432661C0DB47B75822D6FF57E669A1F7009666EA89D4E66BF27657E936C1823C437DEB39C0C4833F55034ADE71C232A499993462134A70D7E94B10131764D54F2694181299EB0437B5B08BB5A868D2B12FF1979CA5B91EF3DED84ACEAD0242F1C93FB0203010001

**Issuer Alternative Name** *ca@acabogacia.org*

**Subject Alternative Name** *http://www.acabogacia.org*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *5A:F6:34:CE:96:76:56:B7:7C:E9:DC:DC:1D:13:6C:79:DE:0F:30:76*

**Authority Key Identifier** *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.16533.10.1.1*  
*CPS pointer: uri:http://www.acabogacia.org/doc*  
*CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]*

**CRL Distribution Points**  
*http://www.acabogacia.org/crl/acabogacia.crl*  
*http://crl.acabogacia.org/crl/acabogacia.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *68:07:A3:F3:7B:3C:6C:18:07:48:52:65:73:0B:BE:3F:6A:37:86:6F:34:8F:5E:F2:12:3C:E8:63:77:38:E0:FC*

**X509SubjectName**

**Subject CN:** *ACA - Trusted Certificates*

**Subject O:** *Consejo General de la Abogacia NIF:Q-2863006I*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject E:** *ca@acabogacia.org*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2017-12-04T01:00:00Z*

### 7.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.16533.20.2.1*

### 7.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 7.3.3 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified Certificates issued by ACA Trusted*

**Name** *[es] Certificados Reconocidos emitidos por CA ACA Trusted*

### Service digital identities

**X509SubjectName**

**Subject CN:** *ACA - Trusted Certificates*

**Subject O:** Consejo General de la Abogacia NIF:Q-2863006I

**Subject OU:** Autoridad de Certificacion de la Abogacia

**Subject E:** ca@acabogacia.org

**Subject C:** ES

**X509SKI**

**X509 SK I** WvY0zpZ2Vrd86dzcHRNsed4PMHY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

#### 7.3.3.1 - Extension (critical): Qualifiers [NotQualified]

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.16533.20.2.1
-------------------	------------	----------------------------------

#### 7.3.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

#### 7.3.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by ACA Trusted
-------------	------	--

<b>Name</b>	[es]	Certificados Reconocidos emitidos por CA ACA Trusted
-------------	------	--

#### Service digital identities

**X509SubjectName**



**Subject CN:** ACA - Trusted Certificates

**Subject O:** Consejo General de la Abogacia NIF:Q-2863006I

**Subject OU:** Autoridad de Certificacion de la Abogacia

**Subject E:** ca@acabogacia.org

**Subject C:** ES

**X509SKI**

**X509 SK I** WvY0zpZ2Vrd86dzcHRNsed4PMHY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2012-09-27T22:00:00Z

#### 7.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.20.2.1

#### 7.4 - Service (withdrawn): Qualified certificate provided by AC Certificados Corporativos 2014

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

**Service Name**

**Name** [en] Qualified certificate provided by AC Certificados Corporativos 2014

**Name** [es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014

**Service digital identities**





**Public Key:**

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B0:FA:18:04:60:97:FB:EB:1B:44:39:56:05:30:F3:8A:F1:4D:F1:BF:29:27:6C:B2:EB:B5:ES:8E:56:5A:E0:C8:EE:C8:E  
 6:1E:89:BF:A9:87:49:2C:0B:B3:C7:D1:F3:54:CD:AA:A6:74:99:0C:4C:D1:E5:89:A2:80:12:86:2F:7C:30:7D:A2:CF:94:E6:D2:D7:EE:97:AE:D7:48:72:33:03:94:9C:B6:CA:51:58:F6:98:7C:74:92:AA:95:C8:ES:1C:EB:26:8D:1  
 4:27:8D:B4:84:88:76:CD:9D:FD:57:4E:89:40:15:EC:70:2:A9:4E:EF:47:D1:42:12:47:30:00:30:15:FE:B3:CF:A7:03:EF:D6:5A:EF:7B:BE:02:AC:F4:4F:21:E7:BA:EF:3C:6D:72:A9:77:7D:B8:2A:B9:A2:70:DA:75:B7:FD:8C:  
 3B:EF:4F:14:2E:91:B3:C8:7E:83:04:CD:9B:1B:75:A7:5B:EC:BC:BC:77:FA:EA:E4:CO:98:35:68:47:50:B9:70:4A:EE:6E:6A:66:69:F5:1B:3E:36:07:5C:83:E1:92:A7:B4:12:F9:18:D5:C6:B6:47:A0:1F:DE:2F:AE:A3:2A:D9:F5:  
 EF:B9:19:C2:55:EC:F0:E4:CE:71:5A:9E:FC:38:3E:BB:9F:D0:AF:88:FD:15:EA:A0:CF:2A:39:02:03:01:00:01

**Basic Constraints**

IsCA: true

**Subject Key Identifier**

33:6D:D0:E9:CD:18:D7:B4:EB:4E:FC:F3:E3:CD:FB:3D:5B:C0:A3:9E

**Authority Key Identifier**

FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.16533.10.1.1

CPS pointer: uri:http://www.acabogacia.org/doc

CPS text: [Consulte la declaracion de practicas de certificacion en http://www.acabogacia.org]

**CRL Distribution Points**

http://www.acabogacia.org/crl/acabogacia.crl

http://crl.acabogacia.org/crl/acabogacia.crl

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

5C:DF:25:EE:A9:A1:49:42:F3:4B:38:B8:EA:17:24:2D:DC:53:F8:78:1D:25:A7:8A:98:18:9E:94:E1:  
 69:72:91

**X509SubjectName****Subject CN:**

ACA - Certificados Corporativos - 2014

**Subject SERIAL NUMBER:**

Q2863006I

**Subject OU:**

Autoridad de Certificacion de la Abogacia

**Subject O:**

Consejo General de la Abogacia

**Subject C:**

ES

**Service Status**

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2017-12-04T01:00:00Z

**7.4.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description**

[en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

#### 7.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 7.4.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

**Name** [en] *Qualified certificate provided by AC Certificados Corporativos 2014*

**Name** [es] *Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014*

##### Service digital identities

##### X509SubjectName

**Subject CN:** *ACA - Certificados Corporativos - 2014*

**Subject SERIAL NUMBER:** *Q2863006I*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *M23Q6c0Y17TrTvzz4837PVvAo54=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 7.4.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.16533.10.5.1

**7.4.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

**7.4.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** http://uri.etsi.org/TrstSvc/Svctype/CA/QC

**Service Name**

**Name** [en] Qualified certificate provided by AC Certificados Corporativos 2014

**Name** [es] Certificados Reconocidos emitidos por CA AC Certificados Corporativos 2014

**Service digital identities****X509SubjectName**

**Subject CN:** ACA - Certificados Corporativos - 2014

**Subject SERIAL NUMBER:** Q2863006I

**Subject OU:** Autoridad de Certificacion de la Abogacia

**Subject O:** Consejo General de la Abogacia

**Subject C:** ES

**X509SKI**

**X509 SK I** M23Q6c0Y17TrTvzz4837PVvAo54=

**Service Status** http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision

**Status Starting Time** 2014-06-04T22:00:00Z

**7.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [en] it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.



**Subject CN:** *ACA - Trusted Certificates - 2014*

**Subject SERIAL NUMBER:** *Q28630061*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia*

**Subject C:** *ES*

**Valid from:** *Wed Oct 07 15:35:07 CEST 2015*

**Valid to:** *Tue Oct 07 15:35:07 CEST 2025*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B85F6FEA56D16F00209D1D832F72208516AEBD350206BEA21584FDA11816F65646F20  
B90630440D2DBE44E8D12E83177F014B47527BC3B5105E481523A2779138FA26A0B1037FC43B99B CD E5A016077BD4872190590C99BD510B0D67941E4FE9809E513D79  
1EAD177B8EC3CD497836440E08D9E455479ACA02B95C6A8E79A9110FC1DE1713A0D6A5E39A80B1E933162CEC3FA5D5B048FB9556EB2DD0858955F74406E2D9F669  
4EDE0022D9DCE1CA79407CACB4DD EFB556157126A04D19078F69BE04FF E339D146BF2E61B5C9CE85D12F6FE00D9409EA3E47724E51ABAA BDAA0F F58871BE3258C  
C7A7521FE EFB6D4CF2BD819A31D B5C66F08BC656F7CB49700470203010001

**Issuer Alternative Name** *ac@acabogacia.org*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *81:8F:D1:63:00:4A:CA:4D:20:97:A6:52:00:60:2E:D2:CC:36:8B:6D*

**Authority Key Identifier** *FC:88:4C:8E:6D:04:A1:20:90:D3:F8:1C:9A:B3:67:04:5F:79:80:C6*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.16533.10.1.1*  
*CPS pointer: <http://www.acabogacia.org/doc>*  
*CPS text: [Consulte la declaracion de practicas de certificacion en <http://www.acabogacia.org>]*

**CRL Distribution Points**  
*<http://www.acabogacia.org/crl/acabogacia.crl>*  
*<http://crl.acabogacia.org/crl/acabogacia.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *2C:26:DA:29:72:06:1F:AF:E7:15:13:CD:CD:C3:EB:72:0E:BD:A8:6E:93:AB:04:A1:97:05:99:0C:B  
A:48:A2:94*

**Certificate fields details**

**Version:** *3*

**Serial Number:** *103184541973990179423004459516921083112*





**Thumbprint:** *BE:F7:3E:BA:EE:78:9B:5B:7A:FC:E3:87:04:2E:1D:E9:3F:B4:57:BD:3B:A7:DC:CE:5C:BB:9F:A9:9F:15:24:DD*

## X509SubjectName

**Subject CN:** *ACA - Trusted Certificates - 2014*

**Subject SERIAL NUMBER:** *Q2863006I*

**Subject OU:** *Autoridad de Certificacion de la Abogacia*

**Subject O:** *Consejo General de la Abogacia*

**Subject C:** *ES*

## Service Status

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2017-12-04T01:00:00Z*

### 7.5.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

#### Criteria list assert=*atLeastOne*

##### Policy Identifier:

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.16533.20.2.1*

### 7.5.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 7.5.3 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

## Service Name

**Name** *[ en ] Qualified Certificates issued by ACA Trusted 2014*

**Name** *[ es ] Certificados Reconocidos emitidos por CA ACA Trusted 2014*

**Service digital identities****X509SubjectName**

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q2863006I*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

**X509SKI**

X509 SK I *gY/RYwBKyk0gl6ZSAGAu0sw2i20=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**7.5.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.16533.20.2.1*

**7.5.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**7.5.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified Certificates issued by ACA Trusted 2014*

Name [es] *Certificados Reconocidos emitidos por CA ACA Trusted 2014*

### Service digital identities

#### X509SubjectName

Subject CN: *ACA - Trusted Certificates - 2014*

Subject SERIAL NUMBER: *Q28630061*

Subject OU: *Autoridad de Certificacion de la Abogacia*

Subject O: *Consejo General de la Abogacia*

Subject C: *ES*

#### X509SKI

X509 SK I *gY/RYwBKyk0gl6ZSAGAu0sw2i20=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

Status Starting Time *2014-06-04T22:00:00Z*

#### 7.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA/ CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

#### Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.16533.20.2.1*

#### 7.6 - Service (granted): Qualified certificate issued by ACA CA1

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

#### Service Name



**Basic Constraints** *IsCA: true*

**Extended Key Usage** *id\_kp\_clientAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.acabogacia.org/doc*

**Subject Key Identifier** *72:A9:E7:D6:8E:02:67:A0:4A:4C:1A:67:31:BC:B7:FE:CB:84:B4:9B*

**Authority Info Access** *http://ocsp.redabogacia.org*  
*http://www.acabogacia.org/certificados/aca\_root.crt*

**Authority Key Identifier** *1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD*

**CRL Distribution Points** *http://www.acabogacia.org/crl/aca\_arl.crl*  
*http://crl.acabogacia.org/crl/aca\_arl.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *70:5E:B3:A0:B1:F0:9D:ED:A3:ED:45:76:6B:BB:C0:21:97:70:0A:BB:1E:2D:1D:9E:28:62:AC:58:9D:C9:FD:77*

**X509SubjectName**

**Subject CN:** *ACA CA1*

**Subject O:** *CONSEJO GENERAL DE LA ABOGACIA*

**Subject OU:** *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

**Subject 2.5.4.97:** *VATES-Q2863006I*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *cqnn1o4CZ6BKTbMby3/suEtJs=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2016-11-02T00:00:00Z*

**7.6.1 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>7.7 - Service (granted): Qualified certificates issued by ACA CA2**Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[ en ]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[ es ]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name****Name**

[ en ]

Qualified certificates issued by ACA CA2

**Name**

[ es ]

Certificados cualificados emitidos por ACA CA2

Service digital identities**Certificate fields details****Version:**

3

**Serial Number:**

97911743187377240900748830157217551837

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIHHTCCBO2gAwIBAgIQSakdpc0NgMNx9EeAJTJV7IANBgkqhkiG9w0BAQsFAADBMQswCQYDVQQG
EwVFR1ZEMSA6AUAUEBRMjUFRhNjUwMDZlMzkwYjY0OQkDSDT0STRlbnRlZlRlYSQwRkRETEg
QUIPR0FDSUUESETAPBgnVBAAMCEFFDOSBSt09UMB4XDTE2MDYyMzEyMDE0FoXDTMwMDYyMzEy
MDE0FowgZysCzAIBgNVBAYTAKVTRMRgZjYyDVORhDA9W9RFLYjIRMGz2MzAwNkxkMjAwBgNV
BAsMKUUVVENSNUBRBCERSBDRVJUSUZQOFESLW0HERIEBHFCT04BO0BMSwCQYDVQODBSDT0STRl
jpbIEAFTRVSQWwREUgTEEEQUUPR0FDSUUEEAD0BgnVBAAMMB0FDOSBDO1WgggIAOCCSgS3b3DQEB
AQLAA4ICDwAwggKAAoIQAQDqjF9jgSYMaxpOx4EWQpNOMFic0PAbc43CA3AZkCremMqmPsoQncp
pcXZ7pyWzG6N9j9e4u+Qc8rDKSW3oaUQmMhg85Y7MYHUccpmxgswTosN0uDMEMWYU5Ej
dVHhNglpwWNOBSYmz0pT7V19dhF1uHT7FgRjD6sJvc7EnpM1Bxj0c51UwNT104k8F8EBO
IEgOqLHgrMnA0hLqN1kCkZuoGaba0YRUxet8gzDulInX16uE4weloQKz5ShgyVhQh-VF
XkKwTADwZgm1880tp0A0f0SSZ3Nw0hVclsaQcMA1X4kcp0NkicCV0YKGgAUFW4F
taDla05FHECE3YkA2necrcic8G9grYg8BypL0orSxmjDtrqpxZy0CVMhzD152M5cB6AYi
QemMPKjWkGk0rWdz50hVLTKTJc8eRcHl4QNEWwkd0KSSFTUJNpYImuRYaXwJfOG+N
YLTU4E50w165F1ZGR7fhe0iR2DDmusalnegHhSopH19BUUWw41SP4T5MxZjtheBj
xoAhaBho0cB4SFDYyWWOL7uq4HRQW-KulsoMRKauXwFxC07Cun12b0PLUpoNyraakTQT28IPRa1
bnV1OhmSNx23lZz9jEwIDAQABo4BpTCCAaAwwDwYDVROTAAQHBALwAwEBAQoBgnVHQBAB8E
BAMCAQYwH0YDROBBYwFAyBkwYBBQJIAwGCCcGAQUFBwMDMGMGA1UgIQAQMDUwMwEYVR0gADAr
MCKGCcGAQUFBwIBFBHodHRwO8vd3d3LmFjYyWVZ2ZjAWEab3Jl2RyYzAdBgNVHQ4EFgQUbU1
r5VhwEHcyqKkEJh0MAweAYKwYBBQJIAQEEhDBGMcGCGCAGAUFBzABh0dHRwO8vb2Nz
cC5zW8Ym9hYWNpYSScncwPwYKwYBBQJIAKAGGZmB0HAd1y3d3cay1WwNy9hYWNpYSScncw
Y2VydGlnaWwNbzG9Zl2FjYV9y9h290LmNy4DAIBgNVHSMEGDAWgBQ0VcVMclxmxHUHfAD1wKAW/
z7BIBgNVHREXjBcMfgeWKBWh0dHRwO8vd3d3LmFjYyWVZ2ZjAWEab3Jl2NybC9hY2FjYXk6
LmNy9hYWNpYSScncwY2VydGlnaWwNbzG9Zl2FjYV9y9h290LmNy4DAIBgNVHSMEGDAWgBQ0Vc
VMclxmxHUHfAD1wKAW/AGELBOADggIBALP7topBAMAX0j9vbjZ13WvYdN-ECdJWp2UkRbeAowwdeMauVnmF1W40
dsYh5tMZRAc06PZWWY0Q2y4IjggMGA0b47EXH1IG+ImqzZEWwuz3Psw1GhJKpms1gh
MCAfM0M0w4NcnyZgKk0z0r1W0v8ZlZQfbc70yR44Wmm3EXL8D1kA+S85e9+FeRd3t
PIASc3bIA5jGep1SBXq29yB5b03E2ImMXMFEatx5Fhwkysye1blWQLHP7FwrvPm2DD
AGwFvXxiVj+BE/xUbyGjK9vXy745N0h0zic49lzmMNe0R0v5MkoWQWwZjQ0wZRUljGM
qnamF+KXV152z0X0B5j0h4fQD0B5JC8mE4ZBhmP6MxY10p0j0z0mZx0p0H1pLk
ag80A6nDZlmoxtD5u4wrg3gFgM7CZwXchry80MVDH1FD6Gz3bRPlggh8Z08jPvco4r3Dnjb
emf0zZUaZdYFRIDLruWwgnXoyO+-MKexKm8blU469Zg029h6amXmPWZawH0Q09hwkZuy
SpAA8v+Z2E7P8CXAkm55S3uG60Eua8VWLQ28MdzK6Cz7p08W1mp91CYs6QZU5e97CqCM
nfx+MIKBJY

```

-----END CERTIFICATE-----

**Signature algorithm:**

SHA256withRSA

**Issuer CN:**

ACA ROOT

**Issuer O:**

CONSEJO GENERAL DE LA ABOGACIA

**Issuer SERIAL NUMBER:**

Q28630061

**Issuer C:**

ES

**Subject CN:**

ACA CA2

**Subject O:** CONSEJO GENERAL DE LA ABOGACIA

**Subject OU:** AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

**Subject 2.5.4.97:** VATES-Q2863006I

**Subject C:** ES

**Valid from:** Thu Jun 23 14:07:58 CEST 2016

**Valid to:** Sun Jun 23 14:07:58 CEST 2030

**Public Key:**  
3082022230D06092A864886F70D01010105000382020F003082020A0282020100EA146F48A9260C6B1A4E C44590A8F34E3057DCD0F01B738DC2D80B77033282AD E98C  
AA63E84277A9A5C75767BA725B31BA348F48F5EE2E990C62F3F0CA496D E2BA4510B0C6DD801E584C60751E723A67C460C314E8C5237D9C3375A061412C8FF7551E  
126D808B65C16350052626CFD294FF575E5D845D6E1D3AFB1694618C3EAC26FC7B127A4CD41B718F47B9214CF1F353D382A4F050441B4B441203ADF CB1E0B4C9C0E  
A12EA375902931673B B41AE6DAE98454C5EB7CCE0C3B94B6E5E B2FA B84FB8C1E96E40ACF94A182FCY585087E5455E42B04C00F05338219E5F3C7FB6909B39D94E  
8D24990CD5B1F61155784B1441CDD013C47C99A5F4898A473E09541828612A8C0B855ACE05B5ADDF6B4E451C4084E189230369DEAD E19CF06F74828620F01F12A5  
4A2B490C66A837EB AEAA B1664C8E095321C730F5E7633FE5C081E8062241E98C3CA8C55A48862A87D6773E74C7454B4D729309CF1E45C7E522BE103445BF FF091D B8  
E2AC4854C950DA587CC62458697C2245386F8D60B4D4C44B3CC3573A545D6364647B15F85E6E21D1D830E6BACB949DC8111E1E5EAA DB C74FD16152D596AF87F9  
3ED1538B2317CE37ED6D E065C680216816E739E0784830D8C9058E2FBBAAE07AD05BE2AE22CA0C44A6AE5F017108EE C2BA74C8D9B40F2D4A68372ADA C644D04F6  
F253D16B856E7F5342199235E5F697796E66FF63130203010001

**Basic Constraints** IsCA: true

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.acabogacia.org/doc>

**Subject Key Identifier** 8A:15:1F:AF:74:EF:1F:01:07:73:2A:90:2A:41:09:7E:1B:48:D0:C0

**Authority Info Access** <http://ocsp.redabogacia.org>  
[http://www.acabogacia.org/certificados/aca\\_root.crt](http://www.acabogacia.org/certificados/aca_root.crt)

**Authority Key Identifier** 1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD

**CRL Distribution Points** [http://www.acabogacia.org/crl/aca\\_arl.crl](http://www.acabogacia.org/crl/aca_arl.crl)  
[http://crl.acabogacia.org/crl/aca\\_arl.crl](http://crl.acabogacia.org/crl/aca_arl.crl)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 7E:93:16:A5:CE:CF:B9:0A:53:AD:C3:C7:76:94:50:F4:2C:DC:3A:9B:85:DF:4C:75:77:B0:53:DC:B  
B:25:58:12

**X509SubjectName**

**Subject CN:** ACA CA2

**Subject O:** CONSEJO GENERAL DE LA ABOGACIA

**Subject OU:** AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

**Subject 2.5.4.97:** VATES-Q2863006I



**Subject C:** ES

## X509SKI

**X509 SK I** ihUfr3TvHwEHcyqQKkJfhtI0MA=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2017-12-04T01:00:00Z

### 7.7.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 7.7.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 7.7.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** [en] Qualified certificates issued by ACA CA2

**Name** [es] Certificados cualificados emitidos por ACA CA2

## Service digital identities

### X509SubjectName

**Subject CN:** ACA CA2

**Subject O:** CONSEJO GENERAL DE LA ABOGACIA

**Subject OU:** AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

**Subject 2.5.4.97:** VATES-Q2863006I



**Signature algorithm:** *SHA256withRSA*

**Issuer CN:** *ACA ROOT*

**Issuer O:** *CONSEJO GENERAL DE LA ABOGACIA*

**Issuer SERIAL NUMBER:** *Q2863006I*

**Issuer C:** *ES*

**Subject CN:** *ACA CA3*

**Subject O:** *CONSEJO GENERAL DE LA ABOGACIA*

**Subject OU:** *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

**Subject 2.5.4.97:** *VATES-Q2863006I*

**Subject C:** *ES*

**Valid from:** *Thu Jun 23 14:02:49 CEST 2016*

**Valid to:** *Sun Jun 23 14:02:49 CEST 2030*

**Public Key:**  
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C2:88:A3:05:7C:AE:AC:36:C6:DD:B7:D3:69:62:66:22:57:1B:1A:8C:04:88:F9:0F:BC:06:F7:AA:F7:05:26:AF:FB:11:FB:D1:CF:83:D5:E2:7D:28:42:BA:DC:24:81:20:62:95:C5:7E:01:4A:05:6D:B0:D8:99:87:3B:C4:85:D3:84:1A:AE:D3:F3:9F:D9:D1:24:3D:C2:56:23:48:7A:2E:38:7D:F5:46:B0:F7:46:8A:19:04:9E:0A:BD:ED:07:04:03:CA:00:19:93:B8:09:31:1C:82:73:B0:D0:D2:AB:F2:F1:CO:72:78:F0:EE:CE:47:E2:75:48:4C:AC:50:21:AF:F6:BD:74:FD:1D:AF:FF:C6:CB:8F:E3:09:64:3E:30:CE:D3:43:70:D9:21:57:60:C8:B3:BA:90:FC:C9:5A:F6:A3:8F:32:09:07:3B:BF:92:3E:A9:F8:35:3C:F4:41:9F:6B:CC:4D:93:7B:FC:D9:D5:5C:E7:77:31:F1:8B:0C:CB:CA:EA:E5:6C:E4:3B:F5:C7:63:4A:6C:74:B3:82:6E:FA:7C:6A:92:F6:E5:F8:4A:B7:F2:78:CF:D6:03:D8:46:C1:27:D3:F4:C7:22:B9:FB:65:0A:12:E1:17:08:3B:49:80:27:CC:71:19:DC:74:FA:AD:03:FB:9D:80:CD:41:94:17:C7:A6:89:5B:50:E5:56:95:C7:39:67:BB:63:82:B5:62:E9:EF:1B:80:0E:51:6C:11:F4:76:B1:40:0D:E5:CE:7F:28:34:6D:36:6D:D3:43:0E:3E:00:38:D8:B7:9F:AD:06:20:97:D0:FF:97:59:1B:4A:C4:B7:EB:AA:1B:13:2A:48:87:45:3C:94:61:DE:EA:03:0A:E7:3D:93:C5:C0:FB:D6:D4:8D:B5:19:31:00:77:B7:BB:A1:21:49:E7:54:55:FD:6B:BF:7C:B5:89:76:99:22:50:8C:C7:65:F7:BC:A0:6A:95:55:B6:06:07:EE:16:46:F9:52:58:95:95:B7:09:EB:D3:83:D7:70:9A:0E:83:E6:B3:86:4D:80:A4:38:52:0F:6C:4E:6D:E7:34:6C:F9:86:F6:AB:EB:13:01:EE:1E:3B:33:EB:4B:03:67:4B:49:61:42:A2:C2:58:E7:2C:50:A5:F4:C8:00:6D:3C:34:2D:64:E0:DF:81:6D:70:18:79:9F:71:26:61:6F:03:13:C0:AF:8B:6F:6A:D6:FA:14:70:35:8E:75:07:65:0F:8E:E0:7D:5D:0D:4D:B5:58:77:5A:55:12:C3:94:33:D2:AE:8A:C7:58:00:17:43:52:F5:D5:37:D0:6A:AD:C7:5E:E6:13:09:39:C5:65:48:29:69:E9:07:63:02:03:01:00:01

**Basic Constraints** *IsCA: true*

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://www.acabogacia.org/doc>*

**Subject Key Identifier** *3D:D8:DD:01:BA:C6:28:C5:4C:B5:39:C2:F0:AD:E6:D7:35:95:4F:2F*

**Authority Info Access**  
*<http://ocsp.redabogacia.org>*  
*[http://www.acabogacia.org/certificados/aca\\_root.crt](http://www.acabogacia.org/certificados/aca_root.crt)*

**Authority Key Identifier** *1A:55:E4:15:31:E2:31:9B:11:D4:88:71:7A:00:3D:70:28:05:BF:CD*

**CRL Distribution Points**  
*[http://www.acabogacia.org/crl/aca\\_arl.crl](http://www.acabogacia.org/crl/aca_arl.crl)*  
*[http://crl.acabogacia.org/crl/aca\\_arl.crl](http://crl.acabogacia.org/crl/aca_arl.crl)*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *AF:57:FD:80:5A:0E:F9:0E:97:57:65:C0:D5:D5:5E:3F:D2:4C:FC:49:B7:3A:A1:A4:9E:19:79:01:8D:54:FC:26*

**X509SubjectName**

**Subject CN:** *ACA CA3*

**Subject O:** *CONSEJO GENERAL DE LA ABOGACIA*

**Subject OU:** *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

**Subject 2.5.4.97:** *VATES-Q2863006I*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *PdjdAbrGKMVMtTnC8K3m1zWVTy8=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-09-14T00:00:00Z*

**7.8.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**7.8.2 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified certificates issued by ACA CA3*

**Name** *[es] Certificados cualificados emitidos por ACA CA3*

**Service digital identities****X509SubjectName**

**Subject CN:** *ACA CA3*

**Subject O:** *CONSEJO GENERAL DE LA ABOGACIA*

**Subject OU:** *AUTORIDAD DE CERTIFICACION DE LA ABOGACIA*

**Subject 2.5.4.97:** *VATES-Q2863006I*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *PdjAbrGKMVMfTnC8K3m1zWVTy8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2017-12-04T01:00:00Z*

**7.8.2.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

## 8 - TSP: Colegio de Ingenieros de Caminos, Canales y Puertos

### TSP Name

**Name** [ en ] *Colegio de Ingenieros de Caminos, Canales y Puertos*

**Name** [ es ] *Colegio de Ingenieros de Caminos, Canales y Puertos*

### TSP Trade Name

**Name** [ en ] *CICCP*

**Name** [ es ] *CICCP*

**Name** [ en ] *VATES-Q2867009I*

**Name** [ en ] *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

### PostalAddress

**Street Address** [ es ] *Almagro, 42*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28010*

**Country Name** [ es ] *ES*

### PostalAddress

**Street Address** [ en ] *Almagro, 42*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28010*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *mailto:informatica@ciccp.es*

**URI** [ en ] *http://www.ciccp.es*

### TSP Information URI

URI [en] <http://www.ciccp.es>

URI [es] <http://www.ciccp.es>

## 8.1 - Service (withdrawn): Qualified Certificate

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

**Name** [en] Qualified Certificate

**Name** [es] Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 458165872953085692739587

#### X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIGITCCBQmgAwIBAgIKYQU4AAAAAAsANBgkqhkiG9w0BAQUFAADCBzELMAkGA1UEBhMCRVVx
DzANBgNVBAMTbG9zZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEpZDEp
aW9kZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZl
SUNDUCBDLkkuR4glUS0yODY3MDA5LkxkEjAFBgNVBAMTCEBIBIENJQ0NMRswGOYJKozIhvcNAQoB
Fgw2IAy2fY3AuzXMwHhenMDkMDkMTUxNjM0MwheNMDYwMTLMTUyNjM0MwCzZzZzZzZzZzZzZz
SjBzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
VQOHZwZNYWRYaWQzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
bWlub3MgQ2FuYWxlc3R5bG9zZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
STEZMBAGAUUEAAAMQ0gQ00Q01AgQ2zhe2l/gMxCSAStwDQYKozIhvcNAQoBIBOAgEgEPADCCAQoC
ggEBAL96x16kiLv1Ihmbhmi40mCEV3JkLesDlq3CtdaCdBogPevVikI1QV7nL5C0SgCDi
WLpe4BEm7AqWvcAWkpzmZB7mhwbipdY0mN12oH0ubsUWgenQ0T66f7C7hEQE7kAsI8tkJoH
Yhuk3mGosk9pbeecmQg5zCjgibhA6fih0h0ppYh5e3XCPHvysCAuIAPhHCsMGGA
SPAgzYR2xFnacCtTJ5S5COZOseW4FqjRR0BscHZB0128Zs5S0KHylXReVZJS9QQuNuB5F9
T0lq3agelZdPINSNSGvB95ALXysdGMLy2TgusCAwEAAtOCAGMwggHMBAAGCStGAAQOBgcY
AQODAgEAMBRGA1Ugd9wBBTubN0FfP8S0BPkxERyTb0kZzALBgNVK0EBAwMCACwDwYDVRO0
AQHBAUwAwEBzCB0gYDVR0BBHkMHhHhBS3erHVUS0RwFzmc7BiaZ0wqGqBqaSbjCBozEL
MAkGA1UEBhMCRVVxZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
VQOKExBIEtMglZVnaXZpZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
DKIQIyBTRVJWURPUKVTMR4wHAYJKozIhvcNAQoBEG9peCFNAwFpbCSpchMuzXOCawCQgjBjBzNV
HREXDbaMcmg6AhiNodHRwO8vcgplmNpY2NwLmVzL3BraS9YWNpY2NwLmNybDAtocCugKYYn
aHR0cDovLjBraWJlZy5na2J3ZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
BgrBgfEBQcwoAoYjHR0cDovLjBraS9YWNpY2NwLmVzL3BraS9YWNpY2NwLmNybDAtocCugKYYn
MAKGL2h0dHA6Ly9wa2JlZy5na2J3ZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZzZz
AOKCAgEAAaRkPMLLlIjYgRqg9Kclz85j08wzZ-HlgandSNTns-vRec46hmiwaf9I
zpaBRI9wK9AEqnDHsgSWNFSPdyD7J2SM+Y+ZaY3TVpUNYDLZASFoWFEM4s7kMj3b9FTY
ZPAOPyO6RkgXACDxNOw6HtZHUExp08CQ73+4srtwbl7ccGYxp2Jm+4RdUKRU9tTpIbcAOY
swRUw9pce1pKRMZz0BJz6B+wkZVMY4V6VdEL5q6gMdosW8EesYDV-0nSvVaJHh0OP9WduJl
IAHxCSQ+4psUoa+GIR91ZaDreU.DlnXZOY1YqZocclTmOQ==

```

-----END CERTIFICATE-----

**Signature algorithm:** SHA1withRSA

**Issuer E:** pki@ciccp.es

**Issuer CN:** CA CICCP

**Issuer OU:** CICCP C.I.F. Q-2867009-I

**Issuer O:** CICCP - Colegio de Ingenieros de Caminos Canales y Puertos

**Issuer L:** Madrid

**Issuer ST:** Madrid

**Issuer C:** ES

**Subject CN:** CA CICCIP Clase 3

**Subject OU:** CICCIP C.I.F. Q-2867009-I

**Subject O:** CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos

**Subject L:** Madrid

**Subject ST:** Madrid

**Subject C:** ES

**Subject E:** pki@ciccp.es

**Valid from:** Wed Oct 23 17:16:34 CEST 2002

**Valid to:** Mon Jan 23 16:26:34 CET 2006

**Public Key:**

30820122300D06092A864886F70D01010105000382010F003082010A0282010100B93DEB1D7A92218BBEFD4899B8A19A2E34982115DC990B7AC943C49AA7DC24DD682741A203DEB95864D65415EE72F908E4AA0A90F858BA427B80449B802A5A7F005A4A7F99907B9A1C394DFA5D634B67388D481F4B9B145A0900393BB47E2FC2EEF110104EE403997C22D909A07BE585A2B7B301A8B3CAB86DE7389908399F114988687296403A3F58652343E98E9609C128B75EB18F407CB2B02AC0B82200E0CFE80709C18C180E4F020CD8476C4535A09C4532724B9CC23993A8796E050AA95104E07170766B074FC8D8C8F19B394B4287C8B5D1795F198D2F5042B36E07917D4D096A9376A078565D3C836C352B46BC1F7900B5F2B1D1BF30BCBF093C6382EB0203010001

**Subject Key Identifier**

EE:8E:43:4E:DC:53:F7:6D:24:01:3D:1C:44:46:36:1F:07:A2:BB:FB

**Basic Constraints**

IsCA: true

**Authority Key Identifier**

BA:DD:EB:7F:1D:55:12:D1:1F:B0:17:39:82:7C:1B:5A:66:B3:B0:8A

**CRL Distribution Points**

<http://pki.ciccp.es/pki/caciccp.crl>  
<http://pkiback.ciccp.es/pki/caciccp.crl>

**Authority Info Access**

<http://pki.ciccp.es/pki/caciccp.crt>  
<http://pkiback.ciccp.es/pki/caciccp.crt>

**Key Usage:**

digitalSignature - nonRepudiation - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

DD:5A:AB:55:AB:2D:22:CC:CB:DB:C3:71:33:CC:FB:B3:E5:1A:D4:B9:C3:3C:EC:15:3F:AF:3B:48:B6:8C:58:C2

**X509SubjectName**

**Subject CN:** CA CICCIP Clase 3

**Subject OU:** CICCIP C.I.F. Q-2867009-I

**Subject O:** CICCIP - Colegio de Ingenieros de Caminos Canales y Puertos



**Subject L:** *Madrid*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Subject E:** *pki@ciccp.es*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

### 8.1.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 8.1.2 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### Service Name

**Name** *[en] Qualified Certificate*

**Name** *[es] Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *CA CICCP Clase 3*

**Subject OU:** *CICCP C.I.F. Q-2867009-I*

**Subject O:** *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

**Subject L:** *Madrid*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Subject E:** *pki@ciccp.es*

**X509SKI**

**X509 SK I** *7o5DTtxT920kAT0cREY2Hweiu/s=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

**Status Starting Time** *2010-01-25T00:00:00Z*

**8.1.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificate*

**Name** *[ es ]* *Certificados Reconocidos emitidos por la CA CICCP Clase 3 PKI anterior*

**Service digital identities****X509SubjectName**

**Subject CN:** *CA CICCP Clase 3*

**Subject OU:** *CICCP C.I.F. Q-2867009-I*

**Subject O:** *CICCP - Colegio de Ingenieros de Caminos Canales y Puertos*

**Subject L:** *Madrid*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Subject E:** *pki@ciccp.es*

**X509SKI**

**X509 SK I** *7o5DTtxT920kAT0cREY2Hweiu/s=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2005-03-03T00:00:00Z*

**8.2 - Service (withdrawn): Qualified Certificate**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*



**Subject L:** Madrid

**Subject ST:** Madrid

**Subject C:** ES

**Subject E:** pki@ciccp.es

**Valid from:** Mon Aug 17 12:25:28 CEST 2009

**Valid to:** Sat Aug 17 12:35:26 CEST 2019

**Public Key:**

```
30820222300D06092A864886F70D010105000382020F003082020A0282020100D072CEFB30214A27144E1C78D1EC9C756807F74082DB85E181B291DF9E1D46843EAA8B
83E36026D814D481C9D9B1BE411058716C78B7BB6091A5916509A7A5DEFB061F6886A548B9243057F99E1D0602F04E25AB571D9D93C962D271EF278165034E12A1BF
9034E1CB0C1E2B0C1E275D1E65454B811075027D5E87ADDEB6B23DC73B802CFD0BB151365EE1F3DCE97D505622DE93B040BA0EE40FBD0FBD880CAED7D20D0D3F3
08661F35BA01CEC3F82882CA906B74A43D7FB79D11189C4E6344FB04E9AB561532E6B90995CC44364FC1E47B01B1782055F68492517678F67B1E78AD7CEC82982119
A52B33EB111F33557742859898D7439F30FECBF19104FC7E7B8ED782339915D4E5E599EE35A1D0929D8B4174E152035E368045B27FC92711E15A2D7B730CB83B21
21BFB78BCDE98FB78E8DA775702114B45447BAC092BFA4B274B0748AB8237CS92205D3F5AB60150933208EF728766D9C863DA95EAAB74525893B8CD7372732D139
0B34B70FE01C99C83A9FCCE3BD97344ADFE2CD3D6805852334107C2AA0CDC7F7D9DA2E2E1869FD85E3E176773FE26B7C9B3E2ECCDB956EDA8AFF09277C6F17F1
CF6017B11486AC4FC7DA9EBBE063F43D3943610E8311F0ECCFE3762F30ACE8C6A2B1329180A4B83AEDB00B6640F97637A889E19537F219C2EFAA4D3369082AB
BF0938B9C1DA05EDFD55FBC49460258DA83E687BFE0203010001
```

**Basic Constraints**

IsCA: true

**Subject Key Identifier**

CF:8D:6A:94:4F:AB:4A:E4:3D:40:37:4D:D0:06:C7:A9:3B:59:60:D2

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**AE:6B:A1:14:86:B5:17:CD:68:88:7F:55:86:68:49:67:DD:C9:EB:46:F6:7A:9D:BF:59:3E:31:D2:D2  
:4E:95:37**X509SubjectName****Subject CN:**

CA CICCP Clase 3

**Subject OU:**

CICCP C.I.F. Q-2867009-I

**Subject O:**

CICCP - Colegio de Ingenieros de Caminos Canales y Puertos

**Subject L:**

Madrid

**Subject ST:**

Madrid

**Subject C:**

ES

**Subject E:**

pki@ciccp.es

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2016-06-30T22:00:00Z

**8.2.1 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne**

<b>Key Usage</b>	[ digitalSignature ]	true
<b>Key Usage</b>	[ nonRepudiation ]	true
<b>Key Usage</b>	[ keyEncipherment ]	true
<b>Key Usage</b>	[ dataEncipherment ]	true
<b>Key Usage</b>	[ keyAgreement ]	false
<b>Key Usage</b>	[ keyCertSign ]	false
<b>Key Usage</b>	[ crlSign ]	false
<b>Key Usage</b>	[ encipherOnly ]	false
<b>Key Usage</b>	[ decipherOnly ]	false

**8.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	--------	---

**8.2.3 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificate*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3*

**Service digital identities**

**X509SubjectName**

**Subject CN:** CA CICCPClase 3  
**Subject OU:** CICCPC.I.F. Q-2867009-1  
**Subject O:** CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos  
**Subject L:** Madrid  
**Subject ST:** Madrid  
**Subject C:** ES  
**Subject E:** pki@ciccp.es

**X509SKI**

**X509 SK I** z41qlE+rSuQ9QDdN0AbHqTtZYNI=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** 2015-03-19T23:00:00Z

**8.2.3.1 - Extension (critical): Qualifiers [QCStatement]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne**

<b>Key Usage</b>	[ digitalSignature ]	true
<b>Key Usage</b>	[ nonRepudiation ]	true
<b>Key Usage</b>	[ keyEncipherment ]	true
<b>Key Usage</b>	[ dataEncipherment ]	true
<b>Key Usage</b>	[ keyAgreement ]	false
<b>Key Usage</b>	[ keyCertSign ]	false
<b>Key Usage</b>	[ crlSign ]	false

**Key Usage** [ *encipherOnly* ] *false*

**Key Usage** [ *decipherOnly* ] *false*

#### 8.2.4 - History instance n.2 - Status: supervisionincessation

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** [ *en* ] *Qualified Certificate*

**Name** [ *es* ] *Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3*

#### Service digital identities

#### **X509SubjectName**

**Subject CN:** *CA CICCPC Clase 3*

**Subject OU:** *CICCPC C.I.F. Q-2867009-I*

**Subject O:** *CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos*

**Subject L:** *Madrid*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Subject E:** *pki@ciccp.es*

#### **X509SKI**

**X509 SK I** *z41qlE+rSuQ9QDdN0AbHqTtZYNI=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation*

**Status Starting Time** *2013-07-07T00:00:00Z*

#### 8.2.4.2 - Extension (critical): Qualifiers [QCStatement]

**Qualifier type description** [ *en* ] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[ *es* ] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne**

<b>Key Usage</b>	[ digitalSignature ]	true
<b>Key Usage</b>	[ nonRepudiation ]	true
<b>Key Usage</b>	[ keyEncipherment ]	true
<b>Key Usage</b>	[ dataEncipherment ]	true
<b>Key Usage</b>	[ keyAgreement ]	false
<b>Key Usage</b>	[ keyCertSign ]	false
<b>Key Usage</b>	[ crlSign ]	false
<b>Key Usage</b>	[ encipherOnly ]	false
<b>Key Usage</b>	[ decipherOnly ]	false

**8.2.5 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** [ en ] *Qualified Certificate*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA CA CICCPC Clase 3*

**Service digital identities****X509SubjectName**

**Subject CN:** *CA CICCPC Clase 3*

**Subject OU:** *CICCPC C.I.F. Q-2867009-I*

**Subject O:** *CICCPC - Colegio de Ingenieros de Caminos Canales y Puertos*

**Subject L:** *Madrid*

**Subject ST:** *Madrid*

**Subject C:** *ES*

**Subject E:** *pki@ciccp.es*

**X509SKI**



**X509 SK I**

*z41qlE+rSuQ9QDdN0AbHqTtZYNI=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time**

*2010-01-25T00:00:00Z*

**9 - TSP: HEALTHSIGN, S.L.****TSP Name**

**Name** [ en ] *HEALTHSIGN, S.L.*

**Name** [ es ] *HEALTHSIGN, S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B17944554*

**Name** [ en ] *HEALTHSIGN, S.L.*

**Name** [ es ] *HEALTHSIGN, S.L.*

**Name** [ en ] *Col·legi Oficial de Infermeria de Lleida*

**Name** [ es ] *Col·legi Oficial de Infermeria de Lleida*

**Name** [ en ] *Col·legi Oficial de Infermeria de Girona*

**Name** [ es ] *Col·legi Oficial de Infermeria de Girona*

**Name** [ en ] *Col·legi Oficial de Infermeria de Tarragona*

**Name** [ es ] *Col·legi Oficial de Infermeria de Tarragona*

**Name** [ en ] *Col·legi Oficial de Metges de Lleida*

**Name** [ es ] *Col·legi Oficial de Metges de Lleida*

**Name** [ en ] *Col·legi Oficial de Metges de Girona*

**Name** [ es ] *Col·legi Oficial de Metges de Girona*

**Name** [ en ] *Col·legi Oficial de Metges de Tarragona*

**Name** [ es ] *Col·legi Oficial de Metges de Tarragona*

**Name** [ en ] *Col·legi Oficial de Infermeria de Lleida – CIF Q-2566003-F*

**Name** [ en ] *Col·legi Oficial de Infermeria de Tarragona – CIF Q4366005I*

**Name** [ en ] *Col·legi Oficial de Metges de Lleida – CIF Q2566001J*

**Name** [ en ] *Col·legi Oficial de Infermeria de Girona – CIF Q1766003F*

**Name** [ en ] *Col-legi Oficial de Metges de Girona – CIF Q1766001J*

**Name** [ en ] *Col-legi Oficial de Metges de Tarragona – CIF Q4366001H*

#### PostalAddress

**Street Address** [ en ] *C/Albereda, 3-5, ático*

**Locality** [ en ] *Girona*

**State Or Province** [ en ] *Gerona*

**Postal Code** [ en ] *17004*

**Country Name** [ en ] *ES*

#### PostalAddress

**Street Address** [ es ] *C/Albereda, 3-5, ático*

**Locality** [ es ] *Girona*

**State Or Province** [ es ] *Gerona*

**Postal Code** [ es ] *17004*

**Country Name** [ es ] *ES*

#### ElectronicAddress

**URI** [ en ] *mailto:healthsign@healthsign.org*

**URI** [ en ] *http://www.healthsign.org*

#### TSP Information URI

**URI** [ en ] *http://www.healthsign.org/pub/eng*

**URI** [ es ] *http://www.healthsign.org*

### 9.1 - Service (withdrawn): Certificado de Colegiado Reconocido emitido por CA CODILL CA

#### Service Type Identifier

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name



**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.28537.1.1  
 CPS pointer: <http://www.healthsign.org/repository/>  
 Policy OID: 2.5.29.32.0

**Authority Key Identifier**  
 0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

**CRL Distribution Points**  
<http://www.healthsign.org/repository/hesica.crl>

**Authority Info Access**  
<http://www.healthsign.org/repository/hesica.crt>

**Key Usage:**  
 digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 C7:F6:82:27:03:47:4B:47:1C:14:4F:B8:B8:13:B3:9C:D9:69:53:7F:AD:59:5B:56:C8:06:B4:C5:3C:  
 D1:A0:43

**X509SubjectName**

**Subject CN:**  
 CODILL CA

**Subject OU:**  
 Paer Casanovas 37 - altell 25008 - LLEIDA

**Subject O:**  
 Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F

**Subject C:**  
 ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**  
 2016-06-30T22:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**9.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**9.1.2 - History instance n.1 - Status: supervisionceased**

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
<b>Service Name</b>		
<b>Name</b>	[ es ]	<i>Certificado de Colegiado Reconocido emitido por CA CODILL CA</i>
<b>Name</b>	[ en ]	<i>Qualified Member Certificate issued by CA CODILL CA</i>

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>CODILL CA</i>
<b>Subject OU:</b>	<i>Paer Casanovas 37 - altell 25008 - LLEIDA</i>
<b>Subject O:</b>	<i>Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F</i>
<b>Subject C:</b>	<i>ES</i>

**X509SKI**

<b>X509 SK I</b>	<i>sFjnBNUGXoTWSEsabdEZc71S72w=</i>
------------------	-------------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased</a>
-----------------------	---

<b>Status Starting Time</b>	<i>2015-11-30T23:00:00Z</i>
-----------------------------	-----------------------------

**9.1.3 - History instance n.2 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ es ]	<i>Certificado de Colegiado Reconocido emitido por CA CODILL CA</i>
<b>Name</b>	[ en ]	<i>Qualified Member Certificate issued by CA CODILL CA</i>

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>CODILL CA</i>
<b>Subject OU:</b>	<i>Paer Casanovas 37 - altell 25008 - LLEIDA</i>
<b>Subject O:</b>	<i>Col-legi Oficial de Infermeria de Lleida – CIF Q-2566003-F</i>
<b>Subject C:</b>	<i>ES</i>



**Subject OU:** Avda. Pau Casals. 13-5e. 43003 - TARRAGONA

**Subject O:** Col-legi Oficial de Infermeria de Tarragona – CIF Q43660051

**Subject C:** ES

**Valid from:** Thu Apr 26 13:07:08 CEST 2007

**Valid to:** Tue Apr 26 13:17:08 CEST 2022

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100BC6F2E58FBF7626B73F27B89DCBB22AD22E76F44445A8D57F4772407CD132569FD9B  
C446DBA1C2C7DE39A9106A9E91AE83EF87D7FF250E0408289C8C6F4D9D3E01271EACCA3C98F823E00415CE594437FA56BB8A543A78C1B6715CA2E20303A1B42A2F  
D483C387394B1CSB6CCE052C645407027F035E1010F1E798937E7F2057D2C54EC91A199D64BC09254318F20BD8F87E89126084907819BDB2F33F53AC8E92D8604CE8E  
C2CSB63BCB894440B6ED1466C01B82744FA39F3A7AC8AFEC0C64AF0CB414CA6966AFE976445D14E0F6570C2DBB536A4AF4B4C459AA1BCEB2677200B6B3AFEE11DE  
552E09DBB0FF2864C0D748AC8CEFF7AE43C585F62CB017AA8AE3B50203010001

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 4B:7F:CC:2F:1E:1D:60:2A:E7:1D:49:2E:C2:74:7B:41:12:32:B1:44

**Certificate Policies** Policy OID: 1.3.6.1.4.1.28537.1.1  
CPS pointer: <http://www.healthsign.org/repository/>  
Policy OID: 2.5.29.32.0

**Authority Key Identifier** 0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

**CRL Distribution Points** <http://www.healthsign.org/repository/hesica.crl>

**Authority Info Access** <http://www.healthsign.org/repository/hesica.crt>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** F8:07:01:AE:DC:23:5D:23:71:03:C1:08:61:7D:94:46:5D:41:3C:40:37:17:0B:59:9E:AB:DD:64:8D:33:56:5E

**X509SubjectName**

**Subject CN:** CODITA CA

**Subject OU:** Avda. Pau Casals. 13-5e. 43003 - TARRAGONA

**Subject O:** Col-legi Oficial de Infermeria de Tarragona – CIF Q43660051

**Subject C:** ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2016-06-30T22:00:00Z



**Scheme Service Definition URI**

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**9.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**9.2.2 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Member Certificate issued by CA CODITA CA*

**Name** [ es ] *Certificado de Colegiado Reconocido emitido por CA CODITA CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *CODITA CA*

**Subject OU:** *Avda. Pau Casals. 13-5e. 43003 - TARRAGONA*

**Subject O:** *Col-legi Oficial de Infermeria de Tarragona – CIF Q43660051*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *S3/MLx4dYCrnHUkuwnR7QRlysUQ=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2015-11-30T23:00:00Z*

**9.2.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[ en ]	Qualified Member Certificate issued by CA CODITA CA
<b>Name</b>	[ es ]	Certificado de Colegiado Reconocido emitido por CA CODITA CA

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	CODITA CA
<b>Subject OU:</b>	Avda. Pau Casals. 13-5e. 43003 - TARRAGONA
<b>Subject O:</b>	Col-legi Oficial de Infermeria de Tarragona – CIF Q43660051
<b>Subject C:</b>	ES

**X509SKI**

<b>X509 SK I</b>	S3/MLx4dYCrnHUkuwnR7QRIysUQ=
------------------	------------------------------

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time**

2009-09-09T00:00:00Z

**9.3 - Service (withdrawn): Qualified Member Certificate issued by CA COMLL CA****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[ en ]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[ es ]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

<b>Name</b>	[ en ]	Qualified Member Certificate issued by CA COMLL CA
<b>Name</b>	[ es ]	Certificado de Colegiado Reconocido emitido por CA COMLL CA

**Service digital identities****Certificate fields details**

<b>Version:</b>	3
<b>Serial Number:</b>	86355775820241070718986



**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *80:D0:B3:C8:B8:C3:1C:D3:3E:36:0E:1A:DA:20:8A:37:12:EF:FE:09:1B:B2:84:40:52:A7:35:F7:B4:5C:CC:42*

### X509SubjectName

**Subject CN:** *COMLL CA*

**Subject OU:** *Rambla Arago 14. pral. 25002 - LLEIDA*

**Subject O:** *Col-legi Oficial de Metges de Lleida – CIF Q2566001J*

**Subject C:** *ES*

### Service Status

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

### Status Starting Time

*2016-06-30T22:00:00Z*

### Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

### 9.3.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 9.3.2 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

### Service Name

**Name** *[en] Qualified Member Certificate issued by CA COMLL CA*

**Name** *[es] Certificado de Colegiado Reconocido emitido por CA COMLL CA*

### Service digital identities

### X509SubjectName

**Subject CN:** *COMLL CA*

**Subject OU:** *Rambla Arago 14. pral. 25002 - LLEIDA*

**Subject O:** *Col-legi Oficial de Metges de Lleida – CIF Q2566001J*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *VNY3KgJCiR2H21XB3HXoW/8AmuE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased*

**Status Starting Time** *2015-11-30T23:00:00Z*

**9.3.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Member Certificate issued by CA COMLL CA*

**Name** *[ es ]* *Certificado de Colegiado Reconocido emitido por CA COMLL CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *COMLL CA*

**Subject OU:** *Rambla Arago 14. pral. 25002 - LLEIDA*

**Subject O:** *Col-legi Oficial de Metges de Lleida – CIF Q2566001J*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *VNY3KgJCiR2H21XB3HXoW/8AmuE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2009-09-09T00:00:00Z*

**9.4 - Service (withdrawn): Qualified Member Certificate issued by CA CODIGI CA**



**Public Key:**

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:CB:55:DC:5B:D9:19:FA:BS:5C:7E:06:7A:BF:64:FC:EF:24:B7:7D:3D:AB:88:4C:78:51:AC:69:03:75:B8:39:A8:6  
E:4B:0A:29:27:3A:DA:AD:47:FD:66:C5:B9:C3:B3:E7:CC:97:6F:00:E7:07:DB:C3:85:FC:CD:DE:6C:70:DC:09:BD:5B:12:27:E7:99:89:45:29:14:BD:27:88:23:CB:94:D9:6B:EA:A1:05:13:88:E6:5C:94:49:42:2B:3D:16:C5  
48:4E:8B:9F:49:04:81:F3:5E:02:06:DA:06:5D:70:7E:A5:43:2F:02:D9:0E:2A:C1:3E:D5:59:54:5E:CB:5E:2F:70:BE:0E:73:A7:5C:6B:C5:F9:79:D4:71:50:9E:37:15:3F:AE:89:63:11:9A:44:16:88:04:56:94:5B:19:98:59:3D:A7C  
A:E4:E2:0A:79:0C:63:D0:2E:B5:F6:56:B8:4F:C8:32:19:82:A3:4C:CD:0C:CB:6A:4F:11:EE:3C:20:74:F4:2F:55:51:67:E7:29:CE:0A:AC:6D:B8:35:FB:3F:8D:62:F3:04:84:CE:73:C7:EF:34:20:8F:40:A5:9B:47:05:94:BE:DF:92  
E0:36:E5:15:4B:D8:79:D1:C2:D7:B5:37:EC:52:65:E6:EE:29:7C:ADD7:1E:37:A4:07:47:02:03:01:0001

**Basic Constraints**

IsCA: true - Path length: 0

**Subject Key Identifier**

E6:81:F5:66:F5:F5:D7:9D:DB:BF:94:6B:99:6E:49:37:20:22:F1:54

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.28537.1.1

CPS pointer: <http://www.healthsign.org/repository/>

Policy OID: 2.5.29.32.0

**Authority Key Identifier**

0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79

**CRL Distribution Points**

<http://www.healthsign.org/repository/hesica.crl>

**Authority Info Access**

<http://www.healthsign.org/repository/hesica.crt>

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

E2:2F:28:CC:4C:F2:3F:D3:2B:9B:C1:93:04:A9:91:82:00:8A:BF:69:65:4D:CA:42:BA:65:CC:9B:FA:10:D9:D4

**X509SubjectName****Subject CN:**

CODIGI CA

**Subject OU:**

Albereda. 3-5. 3a. 17004 - GIRONA

**Subject O:**

Col·legi Oficial de Infermeria de Girona – CIF Q1766003F

**Subject C:**

ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2016-06-30T22:00:00Z

**Scheme Service Definition URI****URI**

[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI**

[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**9.4.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**9.4.2 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Member Certificate issued by CA CODIGI CA*

**Name** [ es ] *Certificado de Colegiado Reconocido emitido por CA CODIGI CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *CODIGI CA*

**Subject OU:** *Albereda. 3-5. 3a. 17004 - GIRONA*

**Subject O:** *Col-legi Oficial de Infermeria de Girona – CIF Q1766003F*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *5oH1ZvX1153bv5RrmW5JNyAi8VQ=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2015-11-30T23:00:00Z*

**9.4.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Member Certificate issued by CA CODIGI CA*

**Name** [ es ] *Certificado de Colegiado Reconocido emitido por CA CODIGI CA*

**Service digital identities****X509SubjectName**





**Issuer OU:** Albereda num. 3-5. Atic. 17004 - GIRONA

**Issuer O:** HEALTHSIGN SL – CIF B17944554

**Issuer C:** ES

**Subject CN:** COMG CA

**Subject OU:** Albereda 3-5. Atic. 17004 - GIRONA

**Subject O:** Col-legi Oficial de Metges de Girona – CIF Q1766001J

**Subject C:** ES

**Valid from:** Fri Apr 27 09:34:17 CEST 2007

**Valid to:** Wed Apr 27 09:44:17 CEST 2022

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:AC:30:C0:25:FD:19:27:CA:BB:D4:BC:4A:84:48:BA:FC:E9:07:C2:24:A1:B8:09:49:A3:26:73:47:C2:10:17:5D:36:4F:FC:59:4E:0B:A8:E6:7E:91:8D:54:BB:D1:C0:6D:DE:26:6A:71:1E:32:50:13:DE:BE:33:27:C4:1E:02:C5:95:EA:98:6D:9C:EE:6D:F3:9A:61:BD:55:11:72:7D:33:98:EA:41:8B:33:AD:8D:9E:03:8F:6C:70:0D:E8:77:4B:C0:37:03:73:6B:D0:5D:C8:07:C3:43:2D:57:2E:7E:6A:56:70:7E:7B:D9:C2:D2:4F:13:33:01:20:B7:CA:B9:31:A2:3C:F9:8F:D4:82:F9:84:31:53:45:51:D5:35:47:8E:2C:7D:D5:58:54:C2:9B:42:ED:1C:72:4B:B4:FC:45:0D:6F:30:5A:C0:BF:C0:F4:3B:48:7B:65:93:49:AB:2A:65:D2:A2:2A:8A:3E:95:6E:D8:57:19:5D:F5:9F:2D:BE:94:E9:65:87:CA:C9:BE:90:6F:DF:53:97:02:50:35:74:FD:C2:0F:80:8C:67:53:74:F5:C8:E6:5D:F1:45:E5:6B:3F:32:C0:28:ED:D5:41:AB:B2:ED:7C:29:DE:5D:CD:01:8D:5D:C5:C2:45:62:F0:26:B2:A5:61:9A:7C:B1:37:B8:E7:02:03:01:00:01

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *19:51:0E:6F:D0:EB:96:D8:1D:04:76:76:59:89:CE:39:F4:CB:D7:EA*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.28537.1.1*  
*CPS pointer: <http://www.healthsign.org/repository/>*  
*Policy OID: 2.5.29.32.0*

**Authority Key Identifier** *0B:6E:93:62:5D:C8:6A:60:C0:28:1F:BA:B3:AF:7B:E1:D3:72:B1:79*

**CRL Distribution Points** *<http://www.healthsign.org/repository/hesica.crl>*

**Authority Info Access** *<http://www.healthsign.org/repository/hesica.crt>*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *98:1F:E6:9D:F6:31:4B:83:0B:F9:94:91:FF:81:29:AC:D7:C0:AA:30:53:59:4E:1C:31:07:56:15:3B:C8:E0:60*

**X509SubjectName**

**Subject CN:** COMG CA

**Subject OU:** Albereda 3-5. Atic. 17004 - GIRONA

**Subject O:** Col-legi Oficial de Metges de Girona – CIF Q1766001J

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

#### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 9.5.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 9.5.2 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Member Certificate issued by CA COMG CA

**Name** [es] Certificado de Colegiado Reconocido emitido por CA COMG CA

#### Service digital identities

##### X509SubjectName

**Subject CN:** COMG CA

**Subject OU:** Albereda 3-5. Atic. 17004 - GIRONA

**Subject O:** Col-legi Oficial de Metges de Girona – CIF Q1766001J

**Subject C:** ES

##### X509SKI

**X509 SK I** GVEOb9DrltgdBHZ2WYnOOofTL1+o=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2015-11-30T23:00:00Z*

### 9.5.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### Service Name

**Name** *[en]* *Qualified Member Certificate issued by CA COMG CA*

**Name** *[es]* *Certificado de Colegiado Reconocido emitido por CA COMG CA*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *COMG CA*

**Subject OU:** *Albereda 3-5. Atic. 17004 - GIRONA*

**Subject O:** *Col-legi Oficial de Metges de Girona – CIF Q1766001J*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *GVEOb9DrltgdBHZ2WYnOOofTL1+o=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2009-09-09T00:00:00Z*

### 9.6 - Service (withdrawn): Qualified Member Certificate issued by CA COMT CA

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** *[en]* *Qualified Member Certificate issued by CA COMT CA*

**Name** *[es]* *Certificado de Colegiado Reconocido emitido por CA COMT CA*

#### Service digital identities



**Authority Info Access** <http://www.healthsign.org/repository/hesica.crt>

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *FC:6F:34:24:8C:BB:7D:A5:73:06:E6:0C:4A:4F:92:4A:39:2D:7F:F6:FC:23:E6:04:27:08:3D:E7:72:7C:9E:A9*

## X509SubjectName

**Subject CN:** *COMT CA*

**Subject OU:** *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

**Subject O:** *Col·legi Oficial de Metges de Tarragona – CIF Q4366001H*

**Subject C:** *ES*

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*

*[es] undefined.*

## Status Starting Time

*2016-06-30T22:00:00Z*

## Scheme Service Definition URI

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 9.6.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[en]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 9.6.2 - History instance n.1 - Status: supervisionceased

## Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** *[en]* *Qualified Member Certificate issued by CA COMT CA*

**Name** *[es]* *Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities**X509SubjectName**

**Subject CN:** *COMT CA*

**Subject OU:** *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

**Subject O:** *Col·legi Oficial de Metges de Tarragona – CIF Q4366001H*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *p2b1KSwPwwOQpZhyKZYFsEUMW5M=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>*

**Status Starting Time** *2015-11-30T23:00:00Z*

9.6.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service Name**

**Name** *[ en ]* *Qualified Member Certificate issued by CA COMT CA*

**Name** *[ es ]* *Certificado de Colegiado Reconocido emitido por CA COMT CA*

Service digital identities**X509SubjectName**

**Subject CN:** *COMT CA*

**Subject OU:** *Via Imperi Roma n. 11 bis. 43003 - TARRAGONA*

**Subject O:** *Col·legi Oficial de Metges de Tarragona – CIF Q4366001H*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *p2b1KSwPwwOQpZhyKZYFsEUMW5M=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2009-09-09T00:00:00Z*

## 10 - TSP: Infraestructuras y Servicios de Telecomunicaciones y Certificación SA

### TSP Name

<b>Name</b>	[ en ]	<i>Infraestructuras y Servicios de Telecomunicaciones y Certificación SA</i>
<b>Name</b>	[ es ]	<i>Infraestructuras y Servicios de Telecomunicaciones y Certificación SA</i>
<b>Name</b>	[ ca ]	<i>Infraestructures i Serveis de Telecomunicacions i Certificació</i>
<b>Name</b>	[ en ]	<i>Instituto Valenciano de Finanzas</i>

### TSP Trade Name

<b>Name</b>	[ en ]	<i>Agencia de Tecnología y Certificación Electrónica - ACCV</i>
<b>Name</b>	[ es ]	<i>Agencia de Tecnología y Certificación Electrónica - ACCV</i>
<b>Name</b>	[ en ]	<i>ACCV</i>
<b>Name</b>	[ es ]	<i>ACCV</i>
<b>Name</b>	[ en ]	<i>Generalitat Valenciana</i>
<b>Name</b>	[ es ]	<i>Generalitat Valenciana</i>
<b>Name</b>	[ en ]	<i>Institut Valencià de Finances - IVF</i>
<b>Name</b>	[ es ]	<i>Institut Valencià de Finances - IVF</i>
<b>Name</b>	[ en ]	<i>ISTEC</i>
<b>Name</b>	[ es ]	<i>ISTEC</i>
<b>Name</b>	[ en ]	<i>Instituto Valenciano de Finanzas</i>
<b>Name</b>	[ en ]	<i>VATES-A40573396</i>

### PostalAddress

<b>Street Address</b>	[ en ]	<i>Pista de Ademuz S/N</i>
<b>Locality</b>	[ en ]	<i>Burjassot</i>
<b>State Or Province</b>	[ en ]	<i>Valencia</i>
<b>Postal Code</b>	[ en ]	<i>46100</i>
<b>Country Name</b>	[ en ]	<i>ES</i>



**PostalAddress**

<b>Street Address</b>	[ es ]	<i>Pista de Ademuz S/N</i>
<b>Locality</b>	[ es ]	<i>Burjassot</i>
<b>State Or Province</b>	[ es ]	<i>Valencia</i>
<b>Postal Code</b>	[ es ]	<i>46100</i>
<b>Country Name</b>	[ es ]	<i>ES</i>

**ElectronicAddress**

<b>URI</b>	[ en ]	<i>mailto:accv@accv.es</i>
<b>URI</b>	[ en ]	<i>http://www.accv.es</i>

**TSP Information URI**

<b>URI</b>	[ en ]	<i>http://www.accv.es/quienes-somos/who-are-we</i>
<b>URI</b>	[ es ]	<i>http://www.accv.es</i>

**10.1 - Service (withdrawn): Certificados Reconocidos emitidos por CA ACCV-CA2****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

<b>Service type description</b>	[ en ]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[ es ]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

**Service Name**

<b>Name</b>	[ es ]	<i>Certificados Reconocidos emitidos por CA ACCV-CA2</i>
<b>Name</b>	[ en ]	<i>Qualified Certificates issued by ACCV-CA2</i>

**Service digital identities****Certificate fields details**

<b>Version:</b>	<i>3</i>
<b>Serial Number:</b>	<i>1146754895</i>



**Thumbprint:** AF:2A:96:31:00:E0:AB:38:18:E0:AD:5A:D4:38:22:1D:0C:B1:E8:6C:65:5E:5E:5A:9D:D3:1C:87:57:56:43:2C

## X509SubjectName

**Subject C:** ES

**Subject O:** Generalitat Valenciana

**Subject OU:** PKIGVA

**Subject CN:** ACCV-CA2

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

## Status Starting Time

2016-06-30T22:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 10.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

### 10.1.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

**10.1.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**10.1.4 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Reconocidos emitidos por CA ACCV-CA2*

**Name** [ en ] *Qualified Certificates issued by ACCV-CA2*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject O:** Generalitat Valenciana

**Subject OU:** PKIGVA

**Subject CN:** ACCV-CA2

**X509SKI**

X509 SK I

s3jtBaV5QTrC9MBSKP9jQz+/44E=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time

2016-05-01T00:00:00Z

**10.1.4.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

**10.1.4.2 - Extension (critical): Qualifiers [QCStatement]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

### 10.1.5 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ es ] *Certificados Reconocidos emitidos por CA ACCV-CA2*

**Name** [ en ] *Qualified Certificates issued by ACCV-CA2*

#### Service digital identities

##### X509SubjectName

**Subject C:** ES

**Subject O:** *Generalitat Valenciana*

**Subject OU:** PKIGVA

**Subject CN:** ACCV-CA2

##### X509SKI

**X509 SK I** s3jtBaV5QTrC9MBSKP9jQz+/44E=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2007-03-16T00:00:00Z

### 10.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

**Qualifier type description** [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[ es ] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.16.2.0

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.17.2.0

#### 10.1.5.4 - Extension (critical): Qualifiers [QCStatement]

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.1.0

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.4.0

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.5.0

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.4.0

#### 10.2 - Service (withdrawn): Qualified Certificates issued by CA GVA

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** [en] *Qualified Certificates issued by CA GVA*

**Name** [es] *Certificados Reconocidos emitidos por CA GVA*

#### Service digital identities

#### Certificate fields details

**Version:** 3





**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *9D:AE:71:05:BD:9A:45:07:D2:78:21:01:FD:23:19:10:88:3E:22:27:26:47:0E:2D:98:33:3B:68:7F:9A:4F:63*

**X509SubjectName**

**Subject CN:** *CAGVA*

**Subject OU:** *PKIGVA*

**Subject O:** *Generalitat Valenciana*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2016-06-30T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**10.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**10.2.2 - History instance n.1 - Status: supervisionceased****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en]* *Qualified Certificates issued by CA GVA*

**Name** *[es]* *Certificados Reconocidos emitidos por CA GVA*

**Service digital identities**

**X509SubjectName**

**Subject CN:** CAGVA

**Subject OU:** PKIGVA

**Subject O:** Generalitat Valenciana

**Subject C:** ES

**X509SKI**

**X509 SK I** cUwDVPJya1yNHnHUWIIN1x9Xt90=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** 2012-04-15T22:00:00Z

**10.2.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [*en*] Qualified Certificates issued by CA GVA

**Name** [*es*] Certificados Reconocidos emitidos por CA GVA

**Service digital identities****X509SubjectName**

**Subject CN:** CAGVA

**Subject OU:** PKIGVA

**Subject O:** Generalitat Valenciana

**Subject C:** ES

**X509SKI**

**X509 SK I** cUwDVPJya1yNHnHUWIIN1x9Xt90=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2005-11-03T00:00:00Z



**Valid from:** Thu May 04 14:26:56 CEST 2006

**Valid to:** Sun May 01 14:26:56 CEST 2016

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:B9:07:0A:03:EF:D6:3D:0E:DC:02:87:AF:02:EC:CC:5F:F4:C1:7A:71:F5:65:8B:D9:3B:69:B2:E8:80:6C:E2:4D:37:06:  
 B4:99:5E:08:2B:3C:8D:86:6D:A2:85:6E:9D:5F:E2:9E:F3:07:CF:0C:E1:94:88:AD:DA:79:9F:AD:41:24:1E:87:6A:9D:AB:B1:2D:FF:26:E9:24:6E:CD:77:A3E:B2:A1:16:B2:BA:98:FF:C8:09:26:37:88:CF:8E:88:D5:34:6C:44:  
 EF:C9:72:AB:D2:52:23:DC:AD:D8:7B:9B:C3:60:36:47:5D:74:21:82:99:2C:79:48:37:BA:53:75:CA:22:D7:34:B5:F6:AA:5A:A2:8F:2E:BF:05:D7:0D:78:46:65:57:9A:67:1D:A8:A2:B5:8D:16:A4:F9:BB:43:4C:17:DC:88:DF:  
 F:D0:F0:11:45:31:75:5D:15:51:27:BB:2B:02:FE:C9:EE:C8:F3:FB:69:D6:BF:EE:ES:90:30:98:E1:FC:89:B4:3E:D6:3C:D1:1E:E6:D6:B8:AB:18:E7:32:E9:8C:A9:28:FE:C0:E2:1D:4D:20:02:63:BA:04:01:99:0F:CC:C5:91:E1:4  
 E:19:4F:D7:64:BB:43:DD:6E:87:BD:9F:2D:ES:7E:44:18:2C:91:14:59:E8:90:DF:85:CC:BA:71:02:03:01:00:01

**Basic Constraints** IsCA: true - Path length: 0

**Certificate Policies** Policy OID: 1.3.6.1.4.1.8149.2.1.0  
 CPS text: [Autoridad de Certificación Raíz de la Generalitat Valenciana.  
 La Declaración de Prácticas de Certificación que rige el funcionamiento de la presente Autoridad de  
 Certificación se encuentra en la dirección web <http://www.pki.gva.es/cps>]

CPS pointer: <http://www.pki.gva.es/cps>

**Authority Key Identifier** 7B:35:D3:40:D2:1C:78:19:66:EF:74:10:28:DC:3E:4F:B2:78:04:FC

**Subject Key Identifier** 1B:90:85:EB:CC:C2:5D:36:64:9B:EA:C6:24:74:41:30:C9:CA:24:52

**Thumbprint algorithm:** SHA-256

**Thumbprint:** C7:D8:33:48:A3:0A:A6:7A:79:C7:20:38:D1:EF:E5:33:18:89:E6:4D:A1:47:E2:7A:1D:8F:FE:47:AE  
 :8C:BE:29

## X509SubjectName

**Subject C:** ES

**Subject O:** Generalitat Valenciana

**Subject OU:** PKIGVA

**Subject CN:** ACCV-CA1

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 10.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.8149.3.10.1.0
-------------------	------------	-----------------------------------

**10.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
------------	------	---

**10.3.3 - History instance n.1 - Status: supervisionceased**

<b>Service Type Identifier</b>	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
--------------------------------	---

**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by ACCV-CA1
-------------	------	---

<b>Name</b>	[es]	Certificados Reconocidos emitidos por ACCV-CA1
-------------	------	--

**Service digital identities****X509SubjectName**

<b>Subject C:</b>	ES
-------------------	----

<b>Subject O:</b>	Generalitat Valenciana
-------------------	------------------------

<b>Subject OU:</b>	PKIGVA
--------------------	--------

<b>Subject CN:</b>	ACCV-CA1
--------------------	----------

**X509SKI**

<b>X509 SK I</b>	G5CF68zCXTZkm+rGJHRBMMnKJFI=
------------------	------------------------------

<b>Service Status</b>	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased
-----------------------	---

<b>Status Starting Time</b>	2016-05-01T00:00:00Z
-----------------------------	----------------------

**10.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
-----------------------------------	------	--

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

### Criteria list assert=atLeastOne

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

### 10.3.3.2 - Extension (critical): Qualifiers [QCStatement]

Qualifier type description [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

### Criteria list assert=atLeastOne

#### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

### 10.3.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] *Qualified Certificates issued by ACCV-CA1*

Name [es] *Certificados Reconocidos emitidos por ACCV-CA1*

### Service digital identities

#### X509SubjectName

Subject C: ES

Subject O: Generalitat Valenciana

Subject OU: PKIGVA

Subject CN: ACCV-CA1

#### X509SKI

X509 SK I

G5CF68zCXTZkm+rGJHRBMMnKJFI=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2007-03-16T00:00:00Z

**10.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

**10.3.4.4 - Extension (critical): Qualifiers [QCStatement]**

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.10.1.0

**10.4 - Service (granted): Qualified Certificates issued by ACCVCA-110**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [ en ] Qualified Certificates issued by ACCVCA-110







**Subject OU:** *PKIACCV*

**Subject CN:** *ACCVCA-110*

**Valid from:** *Thu May 07 14:25:39 CEST 2015*

**Valid to:** *Fri Jan 01 00:59:00 CET 2027*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A0754BCE2FA6882DBDFFB1065F8D02CB92BDE0107235700EC4BF498990E8F1E63929  
93B69ECD4D13B3FC4339559C59562FA6A3CSAD9297C433AED9885D035A27421A238CC2F1F1E1BA22C7498B343D330A7206371B62D799CFE078AA67B93DBBE624C  
A32E9317E5535B5A5FD380C8F1507CDAA39160A3DB48C46501049DD5BECE5343CD6BBA7E5A81765E6D4CC751D2AC34DEDB3206FB015E04C59082A28F31C30397  
1E9837F175934FEDE8B3B1B427128322A82F3051FCF05A9D78977CB98556A41A68848959D06B7BAF72BD6FA8CDCE540B56964978701CB0D67E7098CA0C4FC57  
E81B5BA5552BBE298B81DCC373F1BE0806A17320D8D7FCFF6712825D778690827EB6B884A2667C3D4C2743AC6190CA4A163283AA2942A39790AF8F428040EB45  
B0221828C64C02D48622E55D2E7220056A6B3C6098B7534FD936DB51E20F895253E39FB55BA22F0E5B960ACC817A7B50FA40D137A80241CF0ECAA0C7C349D30667C  
ADF0C1736FFE0E973B0EDEF8D297C40493D174405F7EDEF2726173E9D04B61082C6430F22B6F039096C8BF0B437AF0744B642B69B337B31C8A048986E8B34C9BB672C69  
BD7E4F3D7CF578831849FE94C264C05EDBFCA01512E3A071098644890A2A2808596E51C72D6253EAD4FBA0C15788CE965939566FC0F57448A02557E4DD76F6555B4  
8C5EF38BC128549A56F73E3C1883DC6BA6C5949C90203010001

**Authority Info Access** *http://ocsp.accv.es*

**Subject Key Identifier** *92:52:AE:46:6D:5B:BD:BE:85:C1:B3:61:47:A8:FF:B7:D9:93:C0:0E*

**Basic Constraints** *IsCA: true*

**Authority Key Identifier** *D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en http://www.accv.es]*  
*CPS pointer: http://www.accv.es/legislacion\_c.htm*

**CRL Distribution Points** *http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1\_der.crl*

**Subject Alternative Name** *accv@accv.es*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *E9:32:7A:34:7C:BE:1C:B9:4C:DC:9A:A5:4C:B3:1B:6E:43:D6:89:68:D1:7D:09:CE:32:6A:09:1B:F  
C:2F:0B:11*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *ACCV*

**Subject OU:** *PKIACCV*

**Subject CN:** *ACCVCA-110*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2018-01-16T01:00:00Z*

### Scheme Service Definition URI

**URI** *[ en ]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[ es ]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 10.4.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

##### Policy Identifier:

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

#### 10.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 10.4.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

### Service Name

**Name** *[ en ]* *Qualified Certificates issued by ACCVCA-110*

**Name** *[ es ]* *Certificados Reconocidos emitidos por ACCVCA-110*

### Service digital identities

#### X509SubjectName

**Subject C:** *ES*

**Subject O:** *ACCV*

Subject OU: PKIACCV

Subject CN: ACCVCA-110

X509SKI

X509 SK I kIKuRm1bvb6FwbNhR6j/t9mTWA4=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

#### 10.4.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description	[en]	undefined.
	[es]	undefined.

#### Criteria list assert=atLeastOne

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.8149.3.10.2.0
------------	------------	-----------------------------------

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.8149.3.22.1.0
------------	------------	-----------------------------------

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.8149.3.10.3.0
------------	------------	-----------------------------------

Policy Identifier:

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.8149.3.22.2.0
------------	------------	-----------------------------------

#### 10.4.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	------	---

#### 10.4.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

**Name** [en] *Qualified Certificates issued by ACCVCA-110*

**Name** [es] *Certificados Reconocidos emitidos por ACCVCA-110*

### Service digital identities

#### X509SubjectName

**Subject C:** ES

**Subject O:** ACCV

**Subject OU:** PKIACCV

**Subject CN:** ACCVCA-110

#### X509SKI

**X509 SK I** *klKuRm1bvb6FwbNhR6j/t9mTWA4=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time** *2012-04-15T22:00:00Z*

#### 10.4.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA/ CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.10.2.0*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.22.1.0*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.10.3.0*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.8149.3.22.2.0*

**10.4.4.4 - Extension (critical): Qualifiers [QCStatement]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi» identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.10.2.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.22.1.0

**10.5 - Service (granted): Qualified Certificates issued by ACCVCA-120**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [ en ] Qualified Certificates issued by ACCVCA-120

**Name** [ es ] Certificados Reconocidos emitidos por ACCVCA-120

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 7242567391183044774







**Public Key:**

30820222300D06092A864886F70D010105000382020F003082020A02820201009B0623171ED26666AB2E3D3E3E3A9D267EAA B791303E9817C67133CC57CE490AD29B  
 ACAS825013D54C4CE797D6B99BF09D340C6081518A340FA134C1426AD152E4FEA727C5D9E1245B20B459E9E814A170D5F5E232D08816EECC24B3CE877D47D8EB5E  
 BF14A2C0613C8A98C9055833FEA9830512979D00B443D87CC5D1756B992F387D63B32BBCA1DBE7780AA3C27D7D56D1A19E04ADB38240015C45DE460643AF55399  
 262D1640A06E4D641E973DC55DB9D06F95EDF33B69C53E561E0CCB1148ED45C10A742FBB5C119D5D436BFBFA1A B751F2467AC3ADB219FFFB100C2F0AED35FD C  
 21951930E90C7957C4D3389C503496B10509EC341C38D53057E2C25C33179D307C0D979F43D2ED6833D26B3FA37AA221D593FB78129CE39B0C34966DC1E18D1D5027  
 8AF966D9443A8AEFC1AFF4A7DE68C5103991F4AC9BE630C780657CA91762BA9E60D226A7312836894E51C46CE3BDD1942C38009AF27F7C1B8232FD79ACB33F1  
 C E336313436CD1D17C44FA4E5C4466D2CAD7018BDE5AD781700D5CB156490CD3C39120070B9ED963190C896F8B8C75E A8797E46ED072B2A8412F0309D5A11A58433  
 1524E7019242C9B654632A2B666224C8A11885691B784B8FB4D38AC795C6E6F4473BE876D298162C9AE21FAE4F2748F0C69EFD0B3A8AC85A5D727E9CE51669  
 1F4D3C96E9F379C292DE12442ECC8C04C84C56E8F0203010001

**Authority Info Access**

<http://ocsp.accv.es>

**Subject Key Identifier**

E8:40:9B:8E:FB:66:3F:C1:44:D8:A1:DF:D4:4A:81:42:08:17:CB:E5

**Basic Constraints**

IsCA: true

**Authority Key Identifier**

D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en <http://www.accv.es>]

CPS pointer: [http://www.accv.es/legislacion\\_c.htm](http://www.accv.es/legislacion_c.htm)

**CRL Distribution Points**

[http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1\\_der.crl](http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl)

**Subject Alternative Name**

[accv@accv.es](mailto:accv@accv.es)

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

2D:E6:20:F2:D1:20:0A:A9:0B:16:C3:CC:F6:70:FD:7E:D1:43:79:AB:06:FA:8B:03:1C:FE:F8:DA:05:1E:A5:A2

**X509SubjectName****Subject C:**

ES

**Subject O:**

ACCV

**Subject OU:**

PKIACCV

**Subject CN:**

ACCVCA-120

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2018-01-16T01:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI**

[es]

<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**10.5.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.16.3.0

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.14.3.0

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.15.3.0

**10.5.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

Qualifier type description	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.7.5.0

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.6.6.0

**10.5.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**10.5.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**10.5.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
-----	--------	---

**10.5.6 - History instance n.1 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
-------------------------	---

**Service Name**

Name	[ en ]	Qualified Certificates issued by ACCVCA-120
------	--------	---

Name	[ es ]	Certificados Reconocidos emitidos por ACCVCA-120
------	--------	--

**Service digital identities****X509SubjectName**

Subject C:	ES
------------	----

Subject O:	ACCV
------------	------

Subject OU:	PKIACCV
-------------	---------

Subject CN:	ACCVCA-120
-------------	------------

**X509SKI**

X509 SK I	6ECbjvtmP8FE2KHf1EqBQggXy+U=
-----------	------------------------------

Service Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
----------------	---

Status Starting Time	2016-06-30T22:00:00Z
----------------------	----------------------

**10.5.6.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[ en ]	undefined.
----------------------------	--------	------------

	[ es ]	undefined.
--	--------	------------

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.16.3.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

**10.5.6.2 - Extension (critical): Qualifiers [QCStatement, QCForESig]**

<b>Qualifier type description</b>	[en]	it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.
	[es]	está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.7.5.0

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.8149.3.6.6.0

**10.5.6.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**10.5.7 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] Qualified Certificates issued by ACCVCA-120

**Name** [ es ] Certificados Reconocidos emitidos por ACCVCA-120

**Service digital identities**

**X509SubjectName**

**Subject C:** ES

**Subject O:** ACCV

**Subject OU:** PKIACCV

**Subject CN:** ACCVCA-120

**X509SKI**

**X509 SK I** 6ECbjvtmP8FE2KHf1EqBQggXy+U=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time**

2012-04-15T22:00:00Z

**10.5.7.4 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.16.3.0

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.8149.3.17.3.0

**10.5.7.5 - Extension (critical): Qualifiers [QCStatement]**

**Qualifier type description** [en] *it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that all certificates issued under the service (CA/QC) identified in 'Service digital identity' and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates is issued as a Qualified Certificate.*

[es] *está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o de acreditación) que todos los certificados expedidos en el marco del servicio (CA / CC) identificado en «Service digital identity» y precisado por la información anterior (filtros) utilizada para identificar aún más bajo el servicio de confianza "Sdi" identificado ese conjunto concreto de certificados para el que se exige esta información adicional con respecto a la expedición de dichos certificados se expide como certificado reconocido.*

**Criteria list assert=atLeastOne****Policy Identifier:**



**Subject C:** ES

**Subject O:** ACCV

**Subject OU:** PKIACCV

**Subject CN:** ACCVCA-130

**Valid from:** Thu Jan 15 11:23:24 CET 2015

**Valid to:** Fri Jan 01 00:59:00 CET 2027

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A39289AE8E7B24F101C69742F0F7F7A8DF2F7CF47DF1D0966729DB8CB057BF3A138F0  
0227A14EA.D57F0E.CC440DA6A5A4A4DA72328E8F60D81F05320616842B0F483BC49A0E54985C419CB8C704931220FED50A53154BD2A2755BBE9C3F0FA599E8F217  
9CB1F178C89CCBA7F303FE5C08B23921E59A7D7BA715049B1291124363881695359160E0FF47BS6804A6BBEDBE60ACB6651A4E3E8EA4E1E1A522C146CFDC88CD58A  
2D216AC0DFE372EFD7D179D79B4D1971486263672E330595F7CB2AE025F3B8DB946A919F9CA1306B8936C3F4E601F90FF1796242EA83A03CDCA9B282C22C818CCDE  
F661688560DC1E9ACCS10073CF465F73EE4A428A5F216953160BD271D61FB07749E80E66FA698593D18C8C956E148E4B4E3B6CA14F137A58B65D62263AD5181  
9397266472906EA070E59A2848424D6E6BEDEC854C551054C3460FBC6AF95E69914DBE5E618A5490E1CE0896F4A7BB0031F849FE90FA6F003EEC11BD05E95075  
CA0CB9E747CAF137946A98C6E876E5AD EEEFF2BD EE3A33FAAABSD21647E5E36B1318D6576D03945EA419A8E82F6A74CE6E5E4DF6DA675EA8559AE9993786F7  
975A6B0CE01C37573FA0787A5EBB1B6EF98D03689365AEE704FDA0A00CEB1A26369EB3B2B2E608F64401A8C3FC0533E5881F7CAF083DC66407E12B3FAF5CD92B7  
C6DFA6632A41A35391E55BCA104AACD5B9D57F72E330203010001

**Authority Info Access** <http://ocsp.accv.es>

**Subject Key Identifier** E5:27:FD:0C:58:B7:60:C1:53:57:86:2D:FB:56:03:8B:FE:9F:C5:B2

**Basic Constraints** IsCA: true

**Authority Key Identifier** D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS text: [Autoridad de Certificación Intermedia de la ACCV (Agencia de Tecnología y Certificación Electrónica, CIF Q4601156E). CPS en <http://www.accv.es>]  
CPS pointer: [http://www.accv.es/legislacion\\_c.htm](http://www.accv.es/legislacion_c.htm)

**CRL Distribution Points** [http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1\\_der.crl](http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl)

**Subject Alternative Name** [accv@accv.es](mailto:accv@accv.es)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 57:2B:F8:99:FD:77:43:62:DC:19:21:96:25:EC:C1:57:BB:55:43:4E:A5:16:6D:57:58:DC:4B:4F:89:0D:66:53

**X509SubjectName**

**Subject C:** ES

**Subject O:** ACCV

**Subject OU:** PKIACCV

**Subject CN:** ACCVCA-130

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

### Scheme Service Definition URI

**URI** [es] <https://avancedigital.mineco.gob.es/es-Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 10.6.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 10.6.2 - History instance n.1 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

### Service Name

**Name** [en] Qualified Certificate issued by ACCVCA-130

**Name** [es] ACCVCA-130

### Service digital identities

#### X509SubjectName

**Subject C:** ES

**Subject O:** ACCV

**Subject OU:** PKIACCV

**Subject CN:** ACCVCA-130

#### X509SKI

**X509 SK I** 5Sf9DFi3YMFTV4Yt+1YDi/6fxbl=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2016-06-23T22:00:00Z





**Subject O:** *Agencia de Tecnología y Certificación Electrónica - ACCV*

**Subject OU:** *PKIACCV*

**Subject CN:** *TSA1 ACCV 2016*

**Valid from:** *Mon Feb 29 17:37:50 CET 2016*

**Valid to:** *Sun Feb 25 17:37:50 CET 2029*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100B913C4B3B8C9E36CADC3C0C3021109A75B8CDF326D3240432985FD2A0B0E7561744E  
E3AEBC7BF017E0F9CB3191284C602032801465F75ECS78119D03B11C9B7D1E48F3F3C27503FE9098E8D63C00C73D2E972C50CA964310F39BDE4641E7AEBC28F1  
2D6D29830E55B437A7B976E0F299384186264BDE87DS95DSFD66268171EE2B4404D28FC48F254E398E9A57AB317D7DA11A1C1E41A95386F99DAE1C0F87BDBC75BDB  
294186CA06947280652B3221F5A1D8FA1D1739B0F57E1671FC201C59F569D6392A8AB7A0896CEEE57D93BD41F0D3120C4E9086310D4A80ACEFC4B330EAC0F6300FB8  
A1E74D04D6CC46856934F9978686C5A95E10E3EED0A79C5BF34D760F03CC08D4565F7C910D3539A4E4B606A90DBB0CFDE01FAD0565E08B44C7A439867A4929  
A139C33768501188625A753A7517F4B8F37C488FE1E90AA14B281DA41709D5152BF6166396AFB8BA20BBC7758521D0090A87C0B4120EC5B66FE6CA411ABA  
90E0C4259E69DCCFE3A89C4FFDF952D0B3954102EC8D9D3842D0703D21EC47E50D4C3E7955E738BEA4C6B13EA6BADBDEFBCDC7D19207B22B4A42DD77D6  
087C4EAK6236698AE01B2B973091F46B1685520D4998A6E68B2D129827313A132BD7A18E84BD9B7F7A8D191728FA0F6F5198FC4A01F6C8A4DC7F392F4BC29C62924EC  
C0F77A6ED4D83F6AE2900D6D2AD764AAD44282BD090203010001

**Authority Info Access**  
<http://www.accv.es/gestcert/ACCVRAIZ1.crt>  
<http://ocsp.accv.es>

**Subject Key Identifier**  
*C6:C4:D8:40:C8:48:94:9D:9D:4B:51:C3:FA:4E:D5:0E:54:62:95:94*

**Authority Key Identifier**  
*D2:87:B4:E3:DF:37:27:93:55:F6:56:EA:81:E5:36:CC:8C:1E:3F:BD*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.8149.3.100.2.0*  
*CPS text: [Servidor de Sellado de Tiempo de la Agencia de Tecnología y Certificación Electrónica IVF (Pl. de Napoles y Sicilia 6, CP 46003 CIF Q9650010C). CPS y CP en http://www.accv.es]*  
*CPS pointer: http://www.accv.es/legislacion\_c.htm*

**CRL Distribution Points**  
[http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1\\_der.crl](http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl)

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Key Usage:**  
*digitalSignature - nonRepudiation*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*2C:8D:42:33:F9:BC:80:93:4E:46:6F:0C:9F:76:41:1F:65:A5:C1:78:98:30:16:0B:66:68:59:EF:93:DE  
:25:66*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Valencia*

**Subject L:** *Valencia*

**Subject O:** *Agencia de Tecnología y Certificación Electrónica - ACCV*

**Subject OU:** *PKIACCV*

**Subject CN:** *TSA1 ACCV 2016*

**X509SKI**

**X509 SK I** *xsTYQMhIIJ2dS1HD+k7VDIRiLZQ=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2019-12-23T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**10.8 - Service (granted): Certificados electrónicos cualificados emitidos por ACCV RSA1 CLIENTE**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[es] Certificados electrónicos cualificados emitidos por ACCV RSA1 CLIENTE*

**Name** *[en] Qualified Certificates issued by ACCV RSA1 CLIENTE*

**Service digital identities****Certificate fields details**

**Version:** *3*

**Serial Number:** *92566109452946322105178398124690431893696298808*



**Authority Info Access**[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crt](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt)<http://ocsp.accv.es>**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <https://www.accv.es>]**Extended Key Usage**

id\_kp\_clientAuth

**CRL Distribution Points**[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crl](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl)

CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES

**Subject Key Identifier**

0D:F8:F0:62:B7:5F:36:D3:39:85:FC:67:E0:D3:C1:9E:19:98:B3:53

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

A6:6B:48:56:45:A5:D6:6A:57:14:A3:60:E0:2D:DF:3A:B7:18:75:E7:7D:B1:98:BA:32:1A:8F:62:FF:01:D7:E1

**X509SubjectName****Subject CN:**

ACCV RSA1 CLIENTE

**Subject 2.5.4.97:**

VATES-A40573396

**Subject O:**

ISTEC

**Subject L:**

BURJASSOT

**Subject ST:**

VALENCIA

**Subject C:**

ES

**X509SKI****X509 SK I**

DfjwYrdfNtM5hfxn4NPBnhmYs1M=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-12-21T00:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>



**Issuer ST:** VALENCIA

**Issuer C:** ES

**Subject CN:** ACCV RSA1 PROFESIONALES

**Subject 2.5.4.97:** VATES-A40573396

**Subject O:** ISTECE

**Subject L:** BURJASSOT

**Subject ST:** VALENCIA

**Subject C:** ES

**Valid from:** Tue Jul 25 14:17:19 CEST 2023

**Valid to:** Fri Jul 19 14:17:18 CEST 2024

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D06D48712448BF6014F6A410F6E2622051F3778EECB76FF04773FB8412580ABD39478E79B82288E60CD315BAAE12D6CE35788E8D9FEA535CCA423DF4A3E87E78E4B4ED029D82B0D7140C0F4D1102FF3F77D7FB6A37200977A2396196FF143B4D8632D0106824B7D2BF5D15DBA08FE398E282CBE6CE30E1E1504688B6835212E81E9683B36FCBE625CBFDA3FD99504082112CC9651864E564894CEB54069C3197E6D0C33C655E218CCD2F47B501E85D0D1C7198023F3CB0D3B6C6A820754A36C72F9530D85AF0CD1DBF3F3A9FAB82542542B1005BBCED04A912C6E83238C2D633700191A803757D442B43F583E6CE06FF44C9E75E6240DD178F2CBA6A1000F7B4C4BDAD909FAFD36D3C6CB94E620A9A54F36B458E9AB2493FFAA5373AC4B5754F356BC140AA84B1462DB99C190D8DE535814EFFFDA3F240763075959A32DE5F6BD5A1A1F2FC83563661C121A4F645FC9CB7F8B5F28F3A36EAD983A78E94889D7BAE2F2B69133DC33C654FB43B5A4B7D17373BDB0C130CC6AC303FFE6CB65DD230A22B573F9DB36036994FA84DA3C09AE3E7DC670C09E9925062FC8764BAFF36AE4649C7CE296EDE1B1D1B9D489E4B658039836084F43EBCE9448B46644D73F089723F4AB7462DACA35F5E90C16D731CB98C8B0EAE0F9CF7E0A21769BD8D44F027F39F511F8C8332AC7B16659CB715B3D7355E9D500CD57C6A5BA0DD4EECD2F0203010001

**Basic Constraints** IsCA: true

**Authority Key Identifier** 19:5A:13:3A:A1:9D:27:F7:A6:38:49:7B:54:59:5A:6E:A6:6A:A4:BB

**Authority Info Access**  
[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crt](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt)  
<http://ocsp.accv.es>

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <https://www.accv.es>]

**Extended Key Usage** id\_kp\_clientAuth

**CRL Distribution Points**  
[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crl](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl)  
CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES

**Subject Key Identifier** C0:3E:7C:2D:92:B6:55:A8:56:7D:76:CE:E8:AC:34:64:B1:77:02:96

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 60:AD:C7:42:48:A4:5F:7D:F9:68:58:7F:38:11:9F:50:E9:9B:4E:06:D1:A6:24:1D:C6:B8:F6:D1:9C:D2:A3:8A

X509SubjectName

**Subject CN:** ACCV RSA1 PROFESIONALES

**Subject 2.5.4.97:** VATES-A40573396

**Subject O:** ISTECS

**Subject L:** BURJASSOT

**Subject ST:** VALENCIA

**Subject C:** ES

## X509SKI

**X509 SK I** wD58LZK2VahWfXbO6Kw0ZLF3ApY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2023-12-21T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 10.9.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 10.10 - Service (granted): Certificados cualificados emitidos por ACCV RSA1 COMPONENTES

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

## Service Name

**Name** [es] Certificados cualificados emitidos por ACCV RSA1 COMPONENTES

**Name** [en] Qualified Certificates issued by ACCV RSA1 COMPONENTES

## Service digital identities





**Public Key:**

3082022230D06092A864886F70D010105000382020E003082020A0282020100EC A57A9224D551F9A1B28408816CA1B6D2478F13AB6391B6B7C49763692B6329DBC3E  
 DE06B2CA236E564B360AF08E9A833F62D4EA9579BE3DD79693D12AB6D8852E0CFF685FAFC510784731740D57439129B84D1E8140BB45022E7AF15583AEBBAA C61E  
 3236C74E6A30137949AAFAF00DCB99EC2BA9AE29097B12F179AD9C0C571B A5D9EB7C22075811EA52841EB9185FB9A192369D80CD93087C0991933238B37E423  
 D230E0AEA C7B53E7AF2D0D24F9DBC2DE2BC220619414F5F83F2E202F1C04C58355F059D5A7557509FB210F9A87661843F188B E46F520C869929FA B54293D8B89F019  
 1BB7A804E6C E8736F501A7317DDFA38EF979F86DC0E1CDD8835E5D0A5C64F069E6A EEF8C87F3E9CD4A5053C32DF8BA4D50E593BE3B3CE7474E38422278FA D774DF  
 2C864F6A120F7185A8AA9F2F643D07CE5F3F5A6A7E7B96ED6A7A1F13304AF5BD C3CDC CBA76ADDAECF298B51B4E4F8158CC72A8A59005775D E5F121C72A5242  
 01E282DF86227013D FE1A4ED86663DA88D6FD9FA01190C51E87E4FC2A72F54823D0F7F62C351BBA5A816E56D3D1F77BF1B D61688E3CDCEB6D6747B6185CB1763A8  
 9F712374EBB3A188715D121A9C782A66DD556B0C EB3D63408EE1494597A190849421401E6B0926EEC6CC3A877F6484E29763C8524F587424AE B90F6552F6903C611E2  
 526987020F973DC47B062E2DA903366C8E453410203010001

**Basic Constraints**

IsCA: true

**Authority Key Identifier**

19:5A:13:3A:A1:9D:27:F7:A6:38:49:7B:54:59:5A:6E:A6:6A:A4:BB

**Authority Info Access**

[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crt](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crt)

<http://ocsp.accv.es>

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <https://www.accv.es>]

**Extended Key Usage**

id\_kp\_clientAuth

**CRL Distribution Points**

[http://www.accv.es/gestcert/accv\\_root\\_rsa\\_eidas\\_2023.crl](http://www.accv.es/gestcert/accv_root_rsa_eidas_2023.crl)

CRL issuer: 4: CN=ACCV ROOT RSA EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES

**Subject Key Identifier**

A9:48:0F:4C:E0:8C:43:E6:7E:D5:82:94:18:49:B2:45:26:D7:01:D5

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

50:D5:74:8D:83:1C:28:64:45:9B:23:D8:B9:9D:F5:3D:BA:43:BB:BB:2B:C4:BF:CD:DB:57:31:B5:2B:56:B6:9E

**X509SubjectName****Subject CN:**

ACCV RSA1 COMPONENTES

**Subject 2.5.4.97:**

VATES-A40573396

**Subject O:**

ISTEC

**Subject L:**

BURJASSOT

**Subject ST:**

VALENCIA

**Subject C:**

ES

**X509SKI****X509 SKI**

qUgPTOCMQ+Z+1YKUGEmyRSbXAdU=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en] undefined.

[es] undefined.



**Issuer O:** *ISTEC*

**Issuer L:** *BURJASSOT*

**Issuer ST:** *VALENCIA*

**Issuer C:** *ES*

**Subject CN:** *ACCV ECC1 CLIENTE*

**Subject 2.5.4.97:** *VATES-A40573396*

**Subject O:** *ISTEC*

**Subject L:** *BURJASSOT*

**Subject ST:** *VALENCIA*

**Subject C:** *ES*

**Valid from:** *Tue Jul 25 14:15:02 CEST 2023*

**Valid to:** *Fri Jul 19 14:15:01 CEST 2047*

**Public Key:**  
30:81:9B:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:23:03:81:86:00:04:00:24:ED:8E:71:D8:76:75:01:54:13:19:74:BB:A1:FC:6E:B8:A6:D0:64:0E:E8:0C:B1:47:86:25:D3:9B:C5:95:F2:57:AE:4B:48:5D:58:43:46:24:3F:44:E2:C1:F0:2D:B1:A5:29:6E:BF:9C:8B:37:60:07:9C:88:1B:8E:F8:11:0A:FB:00:9E:8F:07:33:15:5B:F0:EB:97:0D:2F:5A:B0:98:0B:CC:36:5F:7A:5E:85:5C:96:54:9C:48:51:82:CF:BC:BA:F1:C9:25:BB:DD:9C:65:FA:BEDA:F3:F5:E9:F1:A4:55:43:42:57:81:39:47:E2:CO:AD:ED:69:5B:CD:4B:3A:22:1E:6F

**Basic Constraints** *IsCA: true*

**Authority Key Identifier** *9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15*

**Authority Info Access**  
[http://www.accv.es/gestcert/accv\\_root\\_ecc\\_eidas\\_2023.crt](http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crt)  
<http://ocsp.accv.es>

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points**  
[http://www.accv.es/gestcert/accv\\_root\\_ecc\\_eidas\\_2023.crl](http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crl)  
*CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES*

**Subject Key Identifier** *37:C4:94:3D:38:EB:EB:86:F5:8E:31:CC:5C:DB:8C:78:C3:D1:96:C1*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** 5C:AF:44:B2:92:3B:14:6C:B5:75:AB:2A:B9:A0:A2:93:A1:34:60:23:35:D9:7E:57:9C:44:49:35:32:F4:84:96

## X509SubjectName

**Subject CN:** ACCV ECC1 CLIENTE

**Subject 2.5.4.97:** VATES-A40573396

**Subject O:** ISTECE

**Subject L:** BURJASSOT

**Subject ST:** VALENCIA

**Subject C:** ES

## X509SKI

**X509 SK I** N8SUPTjr64b1jjHMXNuMeMPRIsE=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2023-12-21T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 10.11.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 10.12 - Service (granted): Certificados cualificados emitidos por ACCV ECC1 PROFESIONALES

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

## Service Name

**Name** [es] Certificados cualificados emitidos por ACCV ECC1 PROFESIONALES



**Basic Constraints** *IsCA: true*

**Authority Key Identifier** *9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15*

**Authority Info Access**  
*http://www.accv.es/gestcert/accv\_root\_ecc\_eidas\_2023.crt*  
*http://ocsp.accv.es*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en https://www.accv.es]*

**Extended Key Usage** *id\_kp\_clientAuth*

**CRL Distribution Points**  
*http://www.accv.es/gestcert/accv\_root\_ecc\_eidas\_2023.crl*  
*CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES*

**Subject Key Identifier** *31:DE:C0:D5:C6:B8:47:F5:94:0B:31:A3:A4:87:FF:C6:9F:98:88:1C*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *34:FD:B6:F3:D2:D1:07:0D:D8:42:8B:CE:11:D6:22:94:E1:FF:2C:49:E8:B1:28:B6:11:60:D7:48:C7:A5:37:AA*

**X509SubjectName**

**Subject CN:** *ACCV ECC1 PROFESIONALES*

**Subject 2.5.4.97:** *VATES-A40573396*

**Subject O:** *ISTEC*

**Subject L:** *BURJASSOT*

**Subject ST:** *VALENCIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Md7A1ca4R/WUCzGjpIf/xp+YiBw=*

**Service Status**

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2023-12-21T00:00:00Z*

**Scheme Service Definition URI**

URI [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**10.12.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**10.13 - Service (granted): Certificados cualificados emitidos por ACCV ECC1 COMPONENTES**

**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [ en ] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
 [ es ] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

Name [ es ] Certificados cualificados emitidos por ACCV ECC1 COMPONENTES

Name [ en ] Qualified Certificates issued by ACCV ECC1 COMPONENTES

**Service digital identities**

**Certificate fields details**

Version: 3

Serial Number: 288384503797355422930025878200965719802385314764

**X509 Certificate**

```
-----BEGIN CERTIFICATE-----
MIIE6TCCBggAwIBAgIU06v76ljYFjgoNcolf0wCsSwCgYIKoZlZ0EAWQwYExCzAIBgNV
BAYTAKVIMREDeYDVOQIDABWQIaFENJQTESMBAGAIUEBwswQVSSSEFTU09IMQ9uDAYDVQQKDAVJ
U1RlZmYyYmYGAUUEYQwPwRFRVYVMDQwNzZzMAZEMSEHsYDVOQDDBBBQWJWEPFTHQUNDEVEJ
REFITDwMjMwHbcNMjMwNzJIM1yMDM5WbcNNDcwnZE5MTlyMDMwWJwB-MQswCOYDVOQGEwJFuzER
MARGAIUECAwIVAFMRUSDSUExEiAOBGNVBAeMCUVJkRUBINP/DEOMAwGAUUECwFSVNRUMxGDAW
BGNVIGEMDZBVEVTLLEMDU/3M2MSNjeEMBwGAIUEAwVQUdVYBFO0MAEPT/VPBTKVOVEVETMGB
MBAGBqGSM49AgEGBSuBBAIAAGGAAQAKIQA1HhkaT5dvaG-P0cCcs3B7LbcYaCnVcB8E6AE
im8Yb98V9XifsdEHWwZa8SEp-wJK9N7GLaGYB80wogDzX6KytInLvs20H4QerSizpSL-
Fzj1B86g7B0FTwCjDWEENEJTFWJAZGIVs4898Aw9pUisggdAMHCWTAPEgVHRRMB
AREBTADAQHMB8GAIUdhwOYMBaAFyIAEjIXUyZHSyCNPkBBULoVMHUGCCsGAOUFBwEBB8Gk
ZBE8ggBgEFR0wAoY4aHR0DovL3d3shY2N2ImVzL2dlc3RlZ0JlZjY3Zkcm9udF90Y2Nl
ZWVhYmYyYmYGAUUEYQwPwRFRVYVMDQwNzZzMAZEMSEHsYDVOQDDBBBQWJWEPFTHQUNDEVEJ
MHwccgYEVROgADBYMHAGCCsGAOUFBwICMGOMYkNclmRzmlYWRvIGRHEEIdG9wWRhZCBZSBD
ZXJ0aWZpY2Fic0Zm4gQ29uc3VsdGUpbGZlZGNvbnRyY2VhbnVzIGRlIHVzbyBliBodHRwczov
L3d3shY2N2ImVzL2dlc3RlZ0JlZjY3Zkcm9udF90Y2NlZmVhYmYyYmYGAUUEYQwPwRFRVYVMDQw
NzZzMAZEMSEHsYDVOQDDBBBQWJWEPFTHQUNDEVEJREFTDwMjMwHbcNMjMwNzJIM1yMDM5WbcNNDcwnZE5
MTlyMDMwWJwB-MQswCOYDVOQGEwJFuzER MARGAIUECAwIVAFMRUSDSUExEiAOBGNVBAeMCUVJkRUBINP
/DEOMAwGAUUECwFSVNRUMxGDAW BGNVIGEMDZBVEVTLLEMDU/3M2MSNjeEMBwGAIUEAwVQUdVYBFO0MAEPT
/VPBTKVOVEVETMGB MBAGBqGSM49AgEGBSuBBAIAAGGAAQAKIQA1HhkaT5dvaG-P0cCcs3B7LbcYaCnVcB8E6AE
q5wFGP-wPQ=
-----END CERTIFICATE-----
```

Signature algorithm: SHA512withECDSA

Issuer CN: ACCV ROOT ECC EIDAS 2023

Issuer 2.5.4.97: VATES-A40573396

Issuer O: ISTECE



**Issuer L:** BURJASSOT  
**Issuer ST:** VALENCIA  
**Issuer C:** ES  
**Subject CN:** ACCV ECC1 COMPONENTES  
**Subject 2.5.4.97:** VATES-A40573396  
**Subject O:** ISTECE  
**Subject L:** BURJASSOT  
**Subject ST:** VALENCIA  
**Subject C:** ES  
**Valid from:** Tue Jul 25 14:20:39 CEST 2023  
**Valid to:** Fri Jul 19 14:20:38 CEST 2047  
**Public Key:** 30819B301006072A8648CE3D020106052B810400230381860004009254350078C7B5A913E5DBEE1BE3CEA027397B707B2E179868236BBC287C13A0048AD9FC61BF7C57D5ED16C744F07B705B86AF3391229FEC9908AF4D5C818B6886601F34C24A2A0F35FA2B26D39CBBECD8E97841EAD2939A792FE162CC9D416DB83B07F3A54C5C140AB8C35A1D8D123353885389BF6189B55FE0E21F6CC40C39F6952C6  
**Basic Constraints** IsCA: true  
**Authority Key Identifier** 9C:9F:00:48:A3:95:75:32:66:D1:D2:C8:23:69:54:A0:67:50:BA:15  
**Authority Info Access** [http://www.accv.es/gestcert/accv\\_root\\_ecc\\_eidas\\_2023.crt](http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crt)  
<http://ocsp.accv.es>  
**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <https://www.accv.es>]  
**Extended Key Usage** id\_kp\_clientAuth  
**CRL Distribution Points** [http://www.accv.es/gestcert/accv\\_root\\_ecc\\_eidas\\_2023.crl](http://www.accv.es/gestcert/accv_root_ecc_eidas_2023.crl)  
CRL issuer: 4: CN=ACCV ROOT ECC EIDAS 2023,2.5.4.97=VATES-A40573396,O=ISTEC,L=BURJASSOT,ST=VALENCIA,C=ES  
**Subject Key Identifier** EC:57:F3:2F:01:10:3A:FB:61:47:D2:3B:68:96:33:F5:15:68:53:7E  
**Key Usage:** digitalSignature - keyCertSign - cRLSign  
**Thumbprint algorithm:** SHA-256  
**Thumbprint:** D2:6E:70:2D:03:9A:57:13:DD:AB:F7:10:E4:71:93:73:4E:55:50:71:17:63:78:50:51:78:8D:0F:D2:D7:F4:EA

**X509SubjectName**

**Subject CN:** *ACCV ECC1 COMPONENTES*

**Subject 2.5.4.97:** *VATES-A40573396*

**Subject O:** *ISTEC*

**Subject L:** *BURJASSOT*

**Subject ST:** *VALENCIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *7FfzLwEQOvthR9I7aJYz9RVoU34=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2023-12-21T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**10.13.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**11 - TSP: AC Camerfirma, S.A.****TSP Name**

**Name** [ en ] AC Camerfirma, S.A.

**Name** [ es ] AC Camerfirma, S.A.

**TSP Trade Name**

**Name** [ en ] VATES-A82743287

**Name** [ en ] Camerfirma

**Name** [ es ] Camerfirma

**Name** [ en ] AC Camerfirma S.A.

**Name** [ en ] AC Camerfirma SA

**Name** [ en ] AC CAMERFIRMA S.A.

**PostalAddress**

**Street Address** [ en ] C/Ribera del Loira n°12

**Locality** [ en ] Madrid

**State Or Province** [ en ] Madrid

**Postal Code** [ en ] 28042

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] C/Ribera del Loira n°12

**Locality** [ es ] Madrid

**State Or Province** [ es ] Madrid

**Postal Code** [ es ] 28042

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ en ] <mailto:info@camerfirma.com>



**Issuer O:** AC Camerfirma S.A.

**Issuer C:** ES

**Subject CN:** RACER - 2009

**Subject L:** Madrid (see current address at <https://www.camerfirma.com/address>)

**Subject SERIAL NUMBER:** A82743287

**Subject O:** AC Camerfirma S.A.

**Subject C:** ES

**Valid from:** Wed Mar 25 11:47:09 CET 2009

**Valid to:** Sat Mar 23 11:47:09 CET 2019

**Public Key:**

```
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D8E4548862772F8925727FB0CE5EB93831A3E532E8BCBES230CF3177932587F511A03
F23F39565D3CF1E076C62ED0C4AAB9320CFFA1BE185E2FF6C800ED8E189D6331889442E27F721285FC29B9A9A16F411E01FCDC074280E2E22BE3F46F678C533C6
A05B804D0A0E03BA33C9E729056F86AAD07AEAB5F66A80011CD073599099406EF1F2B7F4375B79100B32C838F1EC9D66499F47829D2BA6E6DDDB55924654952A897
A96AEFFCFCD7AB47DD5F00480F4B1F6E0FA1695AE72B78DEFF7A13A311DA0A0EE72F99400C7D97820B2DB2681C4EB1D0CFED9A9EA10E130D9A57194CF8E61308
7D34C1F567CCB36732A4F8060F387C257925EC879A25A911455FE0CB63E3FF53E3447B6726EBE32906924F2AA5C56A573F9ACFCCA98016F2E98D7108EFAEF77
C5FB26E86CA472DAD22204700E38DAS9252633C92BB49030DC53702869160DA55599F851BAE09E794C7D7E763EC063F9D103E0BAC271E67FB4A2E067D6FACDE560
24A7C5ABFBE2041DA90D5610DE9F94B5C81FE3ADF3BAB64AC131CF940AE2CA0295CE98240D7ED02C5FF5FB231CA9B58402FF4133696ACB9C2D001BD1C4B4975
7367F5D74003EBD1713AK1910B79E8253B83A63BAAS2448BAE328E48016855EC36EBA4D530D9C19BA1CB4F73DA553727BC944FCAB850C2AF18E7BDBFF1A096C
53EB805093B85DB92E221594460D91EA7BA484CCF750203010001
```

**Basic Constraints**

IsCA: true - Path length: 1

**Subject Key Identifier**

AC:16:D7:10:D1:6F:75:F6:84:88:68:E6:44:25:11:72:CA:B3:1B:80

**Authority Key Identifier**

C8:00:0F:FC:C6:52:FC:9F:DB:3B:64:2E:32:B9:6E:2E:71:F3:65:79

**Authority Info Access**

[http://www.camerfirma.com/certs/ac\\_camerfirma-2009.crt](http://www.camerfirma.com/certs/ac_camerfirma-2009.crt)  
<http://ocsp.camerfirma.com>

**Certificate Policies**

Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**

[http://crl.camerfirma.com/ac\\_camerfirma-2009.crl](http://crl.camerfirma.com/ac_camerfirma-2009.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma-2009.crl](http://crl1.camerfirma.com/ac_camerfirma-2009.crl)

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

47:CF:DE:E3:76:09:72:5C:FF:03:7B:56:A0:71:C4:3A:A0:58:69:A8:44:28:A5:D8:61:FF:92:B9:45:0  
 2:92:AA

**X509SubjectName****Subject CN:**

RACER - 2009

**Subject L:**

Madrid (see current address at <https://www.camerfirma.com/address>)

**Subject SERIAL NUMBER:** A82743287

**Subject O:** AC Camerfirma S.A.

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2017-07-21T00:00:00Z

#### 11.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

#### 11.1.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 11.1.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by CA AC Racer-2009*

**Name** [es] *Certificados Reconocidos emitidos por la CA Racer - 2009*

### Service digital identities

#### X509SubjectName

**Subject CN:** *RACER - 2009*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *rBbXENFvdfaEiGjmRCURcsqzG4A=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 11.1.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

**11.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.1.4 - History instance n.2 - Status: undersupervision**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ en ] *Qualified Certificates issued by CA AC Racer-2009*

Name [ es ] *Certificados Reconocidos emitidos por la CA Racer - 2009*

**Service digital identities****X509SubjectName**

Subject CN: *RACER - 2009*

Subject L: *Madrid (see current address at <https://www.camerfirma.com/address>)*

Subject SERIAL NUMBER: *A82743287*

Subject O: *AC Camerfirma S.A.*

Subject C: *ES*

**X509SKI**

X509 SK I *rBbXENFvdfäEiGjmRCURcsqzG4A=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2010-07-02T00:00:00Z*

**11.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[ es ] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

Criteria list assert=atLeastOne





**Signature algorithm:** *SHA1withRSA*

**Issuer CN:** *Chambers of Commerce Root - 2008*

**Issuer O:** *AC Camerfirma S.A.*

**Issuer SERIAL NUMBER:** *A82743287*

**Issuer L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Issuer C:** *EU*

**Subject CN:** *Camerfirma Certificados Camerales - 2009*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject C:** *ES*

**Valid from:** *Mon Mar 16 18:40:20 CET 2009*

**Valid to:** *Thu Mar 14 18:40:20 CET 2019*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100F8F10279F318A749B5B224D1A2B2FFAF3FEF51C2B441B0E.DA68921726EA.D2F38D228  
C097A5FC64D1282FA45E30F9CED71293E5B4E1A2C709E681C77C5696C91982DC.CA36C4278F435E7E1C77FAA0683F939894A7122CA.A78DB18CD856E40AECD981E98  
5E1B77967BF2BD29DC5EA9579EB6DC016AB599C7C.D61E5585C477EC1E4B.C02B5ED3AB.C7CF9BFA25833A.D62A6E1A917145DD714CEC95EE11355C4B9C.C1ABAFB  
46E.A0E36C6D70F62CEB.B418BBE2C5A739001BDE7EC6859A7171206E2D.D728BB87CD95F70F102716.A4DB49DB.CD33921D44350D4DF618404537E9C5F21BDB27DE3EE  
98521E34C5081B556E6A9FF4D29A1D1E230E8F512DE7C4F6F69928A.CCD.A037378AD6BB148C039329167DD990D74109CC3A9AE7E295036F812625D.A39B04C610C  
F85F1E63453CB2C53B1531B412D48C2064BDC679811FE6250DF.A73D9A.E650C10C80A6E86032A37994C806008B0D3604D0778ADB9580F6E820B8981915E54C26FB64  
1E31766E48D3A910814D7DA5CBA4A8A6626CE8DC26CC817D0F49F1A14709C19483EC7E90A8FF0C1BA39B86FC5F.FA2E.CE.C4B933558F0F4838F813F4D8F37D2E66D  
1580A5684E4ED56D52F0A5036504FCEDCB169C214B5E3A3ADAB057CD45BF840C57A9AF67F7A883AB81F05DD370958C4163E0347C80117F6B6884A9FBECD71B72D  
C74A3E6DD88282A06CB2A9924E1B35D6DA0A22CE4F033C830203010001

**Basic Constraints** *IsCA: true - Path length: 2*

**Subject Key Identifier** *1E:C4:5A:8A:84:6F:11:90:58:B3:E2:09:D7:16:E6:EA:C3:24:E6:8D*

**Authority Key Identifier** *F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19*

**Authority Info Access**  
[http://www.camerfirma.com/certs/root\\_chambers-2008.crt](http://www.camerfirma.com/certs/root_chambers-2008.crt)  
<http://ocsp.camerfirma.com>

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersroot-2008.crl>  
<http://crl1.camerfirma.com/chambersroot-2008.crl>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** 2F:2B:32:E7:8F:C6:9D:2F:FC:64:5E:B6:06:8E:07:4E:74:97:74:49:5F:DC:25:10:93:B0:EE:E0:4E:FA:FD:17

## X509SubjectName

**Subject CN:** Camerfirma Certificados Camerales - 2009

**Subject L:** Madrid (see current address at <https://www.camerfirma.com/address>)

**Subject SERIAL NUMBER:** A82743287

**Subject O:** AC Camerfirma S.A.

**Subject C:** ES

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2017-07-21T00:00:00Z

### 11.2.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

### 11.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.2.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by the CA Camerfirma Camerales - 2009*

**Name** *[ es ]* *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

**Service digital identities****X509SubjectName**

**Subject CN:** *Camerfirma Certificados Camerales - 2009*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *HsRaioRvEZBYs+IJ1xbm6sMk5o0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**11.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

### 11.2.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.2.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified Certificates issued by the CA Camerfirma Camerales - 2009*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2009*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *Camerfirma Certificados Camerales - 2009*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *HsRaioRvEZBYs+IJ1xbm6sMk5o0=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2010-07-02T00:00:00Z*

### 11.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

#### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

## 11.3 - Service (withdrawn): Qualified Certificates issued by CA AC Camerfirma Certificados Camerales

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

<b>Name</b>	[ en ]	Qualified Certificates issued by CA AC Camerfirma Certificados Camerales
<b>Name</b>	[ es ]	Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales

### Service digital identities

#### Certificate fields details

<b>Version:</b>	3
<b>Serial Number:</b>	5



**Certificate Policies** Policy OID: 1.3.6.1.4.1.17326.10.9.1  
 CPS pointer: [http://cps.camerfirma.com/cps/ac\\_camerfirma\\_cc.html](http://cps.camerfirma.com/cps/ac_camerfirma_cc.html)

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** C7:D8:43:81:E1:1F:7C:57:46:77:1A:F5:B0:50:DC:51:FC:6F:DA:D6:F6:F3:5B:B5:3A:3D:E9:13:82:2E:A0:9E

**X509SubjectName**

**Subject CN:** AC Camerfirma Certificados Camerales

**Subject O:** AC Camerfirma SA

**Subject SERIAL NUMBER:** A82743287

**Subject L:** Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))

**Subject E:** ac\_camerfirma\_cc@camerfirma.com

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time** 2022-09-06T00:00:00Z

**11.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] undefined.  
 [es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

**Policy Identifier:**



**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

### 11.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.3.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

**Name** [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *AC Camerfirma Certificados Camerales*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *ac\_camerfirma\_cc@camerfirma.com*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *th9OnRxokS43cmDhRo9apSoxMbk=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2020-06-09T00:00:00Z*

### 11.3.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

**11.3.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.3.4 - History instance n.2 - Status: withdrawn**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Camerfirma Certificados Camerales*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *ac\_camerfirma\_cc@camerfirma.com*

**Subject C:** ES

**X509SKI**

**X509 SK I** th9OnRxokS43cmDhRo9apSoxMbk=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Status Starting Time** 2017-07-21T00:00:00Z

**11.3.4.3 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1
-------------------	------------	--------------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2
-------------------	------------	--------------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1
-------------------	------------	--------------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2
-------------------	------------	--------------------------------------

**11.3.4.4 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

**11.3.5 - History instance n.3 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by CA AC Camerfirma Certificados Camerales
-------------	------	--

**Name** [es] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

### Service digital identities

#### X509SubjectName

**Subject CN:** *AC Camerfirma Certificados Camerales*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *ac\_camerfirma\_cc@camerfirma.com*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *th9OnRxokS43cmDhRo9apSoxMbk=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 11.3.5.5 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2*

**11.3.5.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.3.6 - History instance n.4 - Status: undersupervision**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ en ] *Qualified Certificates issued by CA AC Camerfirma Certificados Camerales*

Name [ es ] *Certificados Reconocidos emitidos por la CA AC Camerfirma Certificados Camerales*

**Service digital identities****X509SubjectName**

Subject CN: *AC Camerfirma Certificados Camerales*

Subject O: *AC Camerfirma SA*

Subject SERIAL NUMBER: *A82743287*

Subject L: *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

Subject E: *ac\_camerfirma\_cc@camerfirma.com*

Subject C: *ES*

**X509SKI**

X509 SK I *th9OnRxokS43cmDhRo9apSoxMbk=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time *2004-11-25T00:00:00Z*

**11.3.6.7 - Extension (not critical): Qualifiers [QCForLegalPerson]**

Qualifier type description [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[ es ] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios reconocidos, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*



**Signature algorithm:** *SHA1withRSA*

**Issuer CN:** *AC Camerfirma*

**Issuer O:** *AC Camerfirma SA*

**Issuer L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Issuer SERIAL NUMBER:** *A82743287*

**Issuer E:** *ac\_camerfirma@camerfirma.com*

**Issuer C:** *ES*

**Subject CN:** *RACER*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *caracer@camerfirma.com*

**Subject C:** *ES*

**Valid from:** *Thu Dec 04 18:26:41 CET 2003*

**Valid to:** *Mon Dec 04 18:26:41 CET 2023*

**Public Key:** *3082011F300D06092A864886F70D01010105000382010C0030820107028201007B4DF2CB51D9C60B5D8356F6368717AA0D33BDF1E8D7F6920F5F79E704DEDFA3407589B2FA887A30AA03DC22104621CB9BFFD1CB2B9D0FAA540F42CD786AD1629705C3BC443985FF88C193217238B3E4B8B05DA02BE0CB1E1A98206281957A0231A7E3EC48CD00CB99633B25659DF15F238F5AC247D7D3E04DBF9A962A9B2183E5A714E5B519DD0C257307EAE36CB6FC776AA0B2F510D5D40D7A52B1CFE11B4DF8AE03E1F08106E97F99EC7B8A06BF472AD2903CE60744A0EF9F2CEC1167C0CE7C06956004E7A9F4EF61EC70618710EC0583C425F4E6256CE75ADB7942BC08ABF4ADECBFFAC5077E9B49A57C02680BB4C5E426ACA1DAE4B929232023D83FC3020103*

**Basic Constraints** *IsCA: true - Path length: 10*

**CRL Distribution Points** *<http://crl.camerfirma.com/racer.crl>*

**Subject Key Identifier** *BE:BC:08:D4:2E:BA:00:4C:80:DC:26:67:B4:A5:D8:DD:C3:4A:1A:F9*

**Authority Key Identifier** *70:C1:95:FA:5D:A5:16:BE:62:E8:A4:7D:E3:D4:64:5F:C4:E1:3E:9D*

**Authority Info Access** *[http://www.camerfirma.com/certs/ac\\_camerfirma.crt](http://www.camerfirma.com/certs/ac_camerfirma.crt)*

**Subject Alternative Name** *caracer@camerfirma.com*

**Issuer Alternative Name** *ac\_camerfirma@camerfirma.com*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.17326.10.8.1*  
*CPS pointer: <http://cps.camerfirma.com/cps/racer.html>*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F1:71:21:77:93:5D:BA:40:BD:BD:99:C5:F7:53:31:9C:F6:29:35:49:B7:28:47:41:E4:39:16:AD:3B:F  
B:DD:75*

**X509SubjectName**

**Subject CN:** *RACER*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at www.camerfirma.com/address)*

**Subject E:** *caracer@camerfirma.com*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2017-07-21T00:00:00Z*

**11.4.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*



**11.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.4.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA AC Racer*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA Racer*

**Service digital identities****X509SubjectName**

**Subject CN:** *RACER*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *caracer@camerfirma.com*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *vrwI1C66AEyA3CZntKXY3cNKGvk=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**11.4.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [ en ] *undefined.*

[ es ] *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

#### 11.4.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 11.4.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA AC Racer*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA Racer*

#### Service digital identities

**X509SubjectName**

**Subject CN:** *RACER*

**Subject O:** *AC Camerfirma SA*

**Subject SERIAL NUMBER:** *A82743287*

**Subject L:** *Madrid (see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address))*

**Subject E:** *caracer@camerfirma.com*

**Subject C:** *ES*

**X509SKI**

X509 SK I

vrwI1C66AEyA3CZntKXY3cNKGvk=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2010-07-02T00:00:00Z

**11.4.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

**11.5 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

**Name** [ en ] Qualified Certificates issued by the CA Camerfirma Public Administration

**Name** [ es ] Certificados Reconocidos emitidos por la CA Camerfirma AAPP

**Service digital identities**



**Subject Key Identifier** *E5:46:50:E8:43:A0:B2:F7:1C:E4:B6:FF:D8:00:04:20:F7:1F:A4:0B*

**Authority Key Identifier** *E3:94:F5:B1:4D:E9:DB:A1:29:5B:57:8B:4D:76:06:76:E1:D1:A2:8A*

**Authority Info Access**  
*http://www.camerfirma.com/certs/ROOT-CHAMBERS.crt*  
*http://ocsp.camerfirma.com*

**Subject Alternative Name** *[]*

**Issuer Alternative Name** *chambersroot@chambersign.org*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.17326.1.3.1*  
*CPS pointer: https://policy.camerfirma.com*  
*CPS text: [Certificado raíz. Consulte las condiciones de uso en https://policy.camerfirma.com]*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *83:90:E7:03:57:E9:B5:73:CA:3D:D2:9D:BD:DC:23:7E:CA:F9:36:78:2C:A3:38:9C:79:43:FB:C2:B7:FA:A0:B6*

**X509SubjectName**

**Subject CN:** *AC CAMERFIRMA AAPP*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA*

**Subject L:** *MADRID (Ver en https://www.camerfirma.com/address)*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time***2017-07-21T00:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**11.5.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

**11.5.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.5.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by the CA Camerfirma Public Administration*

**Name** [es] *Certificados Reconocidos emitidos por la CA Camerfirma AAPP*

**Service digital identities****X509SubjectName**

**Subject CN:** AC CAMERFIRMA AAPP

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA

**Subject L:** MADRID (Ver en <https://www.camerfirma.com/address>)

**Subject O:** AC CAMERFIRMA S.A.

**Subject C:** ES

**X509SKI**

**X509 SK I**

5UZQ6EOgsvcc5Lb/2AAEIPcfpAs=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time**

2016-06-30T22:00:00Z

**11.5.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.1.3.3.1
-------------------	------------	-----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.17326.1.3.3.2
-------------------	------------	-----------------------------------

**11.5.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

**11.5.4 - History instance n.2 - Status: undersupervision****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by the CA Camerfirma Public Administration
-------------	------	--

<b>Name</b>	[es]	Certificados Reconocidos emitidos por la CA Camerfirma AAPP
-------------	------	---

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	AC CAMERFIRMA AAPP
--------------------	--------------------

<b>Subject SERIAL NUMBER:</b>	A82743287
-------------------------------	-----------

<b>Subject OU:</b>	AC CAMERFIRMA
--------------------	---------------

**Subject L:** MADRID (Ver en <https://www.camerfirma.com/address>)

**Subject O:** AC CAMERFIRMA S.A.

**Subject C:** ES

X509SKI

**X509 SK I** 5UZQ6EOgsvcc5Lb/2AAEIPcfpAs=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2010-07-22T00:00:00Z

#### 11.5.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

#### 11.6 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [en] Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014

**Name** [es] Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014





**Public Key:**

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:C5:FB:63:F6:EB:C4:3A:19:BA:EC:7F:E7:4D:2B:D0:19:23:B9:EF:10:7B:3A:31:2B:34:81:B3:DC:42:DE:22:FE:9B:16:16:8A:1C:CD:1D:7E:C8:EE:27:36:3B:9F:A9:11:7B:47:76:0E:45:ED:A3:CE:78:B0:DB:7E:1B:46:F4:67:2C:BA:S3:1F:BE:36:AA:8D:47:01:03:C2:0F:C2:47:6D:78:D9:DF:53:86:99:56:64:0D:0A:84:30:C1:46:E3:84:74:3C:D4:DE:FE:0F:86:D2:ED:3B:C7:31:F9:46:2D:F9:67:79:A4:D5:1A:34:CT:88:7B:B5:0A:DA:36:89:38:59:96:6D:7E:BD:25:D3:4F:51:AD:2C:69:98:84:61:28:A3:0F:49:7D:24:25:84:16:13:76:71:88:9D:5B:F6:6C:0D:54:79:F9:99:F3:EF:3F:A2:40:55:DF:CD:2C:11:79:B4:F6:B8:41:43:73:54:8D:88:1E:23:67:4F:67:F3:70:80:2D:42:D9:3D:69:B5:25:F5:06:61:C7:A2:FA:74:00:D9:92:99:65:26:60:9A:6A:EA:B0:74:D4:56:AD:B6:27:35:71:90:26:F1:63:CB:D6:17:20:22:13:BC:24:57:54:B7:DA:F8:44:F0:08:C3:80:EA:A2:D1:F4:4F:C1:63:9F:77:E1:BC:AA:9D:16:A3:DA:1F:30:40:59:BF:0F:C3:12:43:81:CF:5B:CB:CE:8E:BD:94:E2:A5:C5:0C:8F:6D:D6:D1:52:F9:1F:BC:54:28:88:CD:29:86:CB:1B:1F:71:FF:82:A6:21:B3:B5:EB:30:34:DE:64:AS:CD:5F:50:2C:06:07:FD:DB:62:96:45:66:CF:43:89:F8:48:75:16:4E:66:38:7E:92:82:48:68:69:04:E8:CS:F7:2C:0E:E7:94:6A:94:CD:3E:FF:90:1E:20:1C:08:AS:8C:5D:B1:E6:59:51:63:48:61:B5:E6:72:21:E6:13:38:58:CD:E0:F6:58:82:E6:32:3B:89:42:21:97:CF:47:0D:94:89:2A:5F:1A:82:1E:1B:51:FA:18:E7:8A:9B:44:71:D3:85:85:51:C1:E6:1F:D2:9D:F0:2F:37:BC:CD:46:5E:B2:65:E:4:39:6F:0A:10:1B:BB:3C:9C:F8:57:0B:03:89:00:3F:75:13:30:AA:DA:CA:2F:8E:97:A8:31:08:40:08:1B:D3:24:DC:BD:BA:19:31:23:1C:3B:78:41:C9:CD:26:CF:AF:5D:A2:CC:0B:5C:26:BD:D0:6C:68:B0:7D:96:89:06:4E:0C:46:1F:C7:39:2B:36:7D:E1:39:F0:F7:2E:92:F3:F3:EE:EB:5D:F7:03:01:00:01

**Basic Constraints**

IsCA: true - Path length: 2

**Subject Key Identifier**

5D:A1:55:A4:DC:4A:AC:83:11:F9:AA:38:E5:F7:68:4A:FE:15:15:4C

**Authority Key Identifier**

F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19

**Authority Info Access**

[http://www.camerfirma.com/certs/root\\_chambers-2008.crt](http://www.camerfirma.com/certs/root_chambers-2008.crt)

<http://ocsp.camerfirma.com>

**Extended Key Usage**

id\_kp\_clientAuth - id\_kp\_serverAuth

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**

<http://crl.camerfirma.com/chambersroot-2008.crl>

<http://crl1.camerfirma.com/chambersroot-2008.crl>

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

72:39:D2:F7:70:FA:FF:3B:1C:F8:BE:2A:05:EC:03:ED:EA:AC:05:3B:55:4F:90:D3:69:21:15:5B:A8:05:19:81

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2017-07-21T00:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI**

[es]

<https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**11.6.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description**

[en]

undefined.

[es]

undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

### 11.6.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.6.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014*

**Name** [ es ] *Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *Camerfirma AAPP II - 2014*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject OU:** *AC CAMERFIRMA*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *XaFVpNxKriMR+ao45fdoSv4VFUw=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**11.6.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

**11.6.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.6.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by the CA Camerfirma Public Administration AAPP II-2014*

**Name** [es] *Certificados reconocidos emitidos por la CA Camerfirma AAPP II-2014*

**Service digital identities****X509SubjectName**

**Subject CN:** *Camerfirma AAPP II - 2014*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject OU:** *AC CAMERFIRMA*

**Subject C:** *ES*

**X509SKI**

X509 SK I

XaFVpNxKrIMR+ao45fdoSv4VFUw=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2015-07-07T00:00:00Z

**11.6.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.17326.1.3.3.1
------------	-------------	-----------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.17326.1.3.3.2
------------	-------------	-----------------------------------

**11.7 - Service (withdrawn): Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[ en ]	Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016
------	--------	--

Name	[ es ]	Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016
------	--------	--

**Service digital identities****Certificate fields details**

Version:	3
----------	---

Serial Number:	8837493713140842243
----------------	---------------------



**Valid to:** *Fri Jan 13 11:42:46 CET 2040*

**Public Key:**  
 30820222300D06092A864886F70D010105000382020F003082020A0282020100B01383130B A886EA12C03CCEC72C8A5D17E5B4ACF556BBFA1FC E9CS61F79B913A6E  
 73E38FB5D938B59A13C43FC0239B994A2E5C5A9834DD5902E08881AA008E65373C6A4D9BE6712F7A CCA88F161B3BE51565CBE2D0C7B3E1943B909F236C7E9E6A31F  
 ED331135187F8CAAD3538D7D3DA66E98FEC0A0D53DF8B0D74D2A7C7E6437B32536DDA97909323D543CA7FAE68CE F689A77C1832165687A2DD07AC0C0D01AB7E8  
 6BB C4CEFA8E1050C986DA736CD01A16C63C797A17388345A3F4358053EA54E46B178912DE B1E3EA58F32A9E2D5E0238E3752BFC A5BE D321866AAE87A3C150EE C7D  
 2ABFE87D463D2A2C93422678AA281EFC8BFD E0AF E2451E4406151F3ADE3C372C3E DD2B1C8B7A0E C0FF1F4DME25087868859259B9654D408BAF89A906A870CB C0CF  
 F18ECE6F5A89722E664AF04E8D2B436F81633FC3FB6C16AD9DFE7A18C71F440FE05369CFB C203C355EE0E12CE400E64ABFC E6046ACF51C3E1BFC A1262FD325837  
 FD F85C7D7E5BD1F8433F629A8C12EE7BC9BE1A19C482497B B29D6745AC9C1D81A7DD8B E326C7F5A2848E8FC20B6E474SD0D8C B75BA1F98760DFD F88C1F59476  
 B3E728836939408DFA122A5416738B D5DE736897BE5643D7AD E085A41121845BE4CC47A1A831793112112C89E77B555EC853A9EA90DA91DCB867C878D1D028E F186  
 B10347DF B03138CS32E7EB A475A67BD948527FB95A24FE110203010001

**Basic Constraints** *IsCA: true - Path length: 2*

**Subject Key Identifier** *8E:B6:48:04:67:95:0E:4F:99:1F:CA:25:32:C8:86:21:32:51:9A:1F*

**Authority Key Identifier** *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

**Authority Info Access**  
*http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crl*  
*http://ocsp.camerfirma.com*

**Extended Key Usage** *id\_kp\_clientAuth - id\_kp\_serverAuth*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: https://policy.camerfirma.com*

**CRL Distribution Points**  
*http://crl.camerfirma.com/chambersofcommerceroot-2016.crl*  
*http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *B9:CC:D2:5E:63:36:48:F4:56:21:53:16:31:8B:6C:F4:52:C8:E0:76:DB:C6:F2:B1:32:1F:D8:39:2A:91:72:66*

## X509SubjectName

**Subject CN:** *AC CAMERFIRMA AAPP - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA AAPP - 2016*

**Subject OU:** *see current address at https://www.camerfirma.com/address*

**Subject ST:** *MADRID*

**Subject L:** *MADRID*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

[es] undefined.

**Status Starting Time** 2017-07-21T00:00:00Z

### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 11.7.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

### 11.7.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.7.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016

**Name** [es] Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016

#### Service digital identities

#### X509SubjectName

**Subject CN:** AC CAMERFIRMA AAPP - 2016



Subject O: AC CAMERFIRMA S.A.

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA AAPP - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject ST: MADRID

Subject L: MADRID

Subject C: ES

**X509SKI**

X509 SK I *jrZIBGeVDk+ZH8olMsiGITJRmh8=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

**11.7.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.2

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.1.3.3.1

**11.7.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.7.4 - History instance n.2 - Status: undersupervision**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by the CA Camerfirma Public Administration AAPP-2016*

**Name** [es] *Certificados Reconocidos emitidos por la CA Camerfirma AAPP-2016*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC CAMERFIRMA AAPP - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA AAPP - 2016*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject ST:** *MADRID*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jrZIBGeVDk+ZH8olMsiGITJRmh8=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>*

**Status Starting Time**

*2016-04-01T00:00:00Z*

**11.7.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.1.3.3.2*

**Policy Identifier:**



**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject CN:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Thu Feb 18 12:02:18 CET 2016

**Valid to:** Fri Jan 13 12:02:18 CET 2040

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100B7E2809686064B4F7D22383480037A4D85DB46ED801E1E11DE0074FD5802F8DBBA1F4  
3D597B4208E0DAD53E2D07F237795E9D9BA8669D2521147D99CEB011A6172093CA55A2CC8FE6A6E9613F74A214F6A87BF6796061FD794CE6DCE3AED8262D06758  
D9B2930C59EAAC1F656446D64538818A5BF0A7A63C9804A45D8AFC980237F05D0B0C1F50DE7F1BC9D555E06CD476E7C7BF3E1EA390F505BBAB0E6E33AB8014B8  
25E6F566F6ED94E7F95B1DCA8F5D42B2BB8F22B94D0D1F4698304710685AC9F794B6E81648AD9D91C90EC63D428DFC0607877837AAS19F8E67913E64F88EEB13B84  
E4905CC6081A8AC65DA8F69D3A4BD834699F9EA4C910710ED7B446999AA12B482838F5ABAAAF32254DF5918ED8B34DA675FE5288A2911521180CD947AC2561AE  
884115E8A4710CDFABFCB37D22E231404FB3D83D9CD3CB1CB95DA1295FD066CD05A593CD8811592B6E499309D6E59C7545861D8855FC EE E4EE25E7F2D30  
3AA04CB C9F415CB2D3E7DC55B1F6178920CB6F740390696781973C17384247DB72FC8X24FB5B036E9A133704068C85666CB6F2A112A74C12F19A41C0C9883EBE4  
E750B842C52960B6CBEDAF41909B38A345D048CTFECEACB76A7047622C19B2D1539B56EB8B787C7C4B4D2A4EBA63D60942EBCF34022F020C262FAD50E920AF7  
7E5300E7C851CF5FBD2E8E8BEE3C99EC68324B23090203010001

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** 97:A3:58:24:76:6C:09:9F:1A:E4:9F:AE:26:29:77:34:D3:84:D4:EF

**Authority Key Identifier** 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B

**Authority Info Access** <http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points** <http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 42:38:89:2F:E2:D3:34:A1:18:40:86:55:D6:9B:9F:A5:5D:81:A2:53:B1:28:D5:22:54:89:46:F9:DB:0A:F6:69

## X509SubjectName

**Subject CN:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2017-07-21T00:00:00Z

### 11.8.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

**11.8.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.8.3 - History instance n.1 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ en ] *Qualified Certificates issued by the CA Camerfirma Camerales - 2016*

Name [ es ] *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016*

**Service digital identities****X509SubjectName**

Subject CN: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject O: *AC CAMERFIRMA S.A.*

Subject SERIAL NUMBER: *A82743287*

Subject OU: *AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016*

Subject OU: *see current address at <https://www.camerfirma.com/address>*

Subject L: *MADRID*

Subject ST: *MADRID*

Subject C: *ES*

**X509SKI**

X509 SK I *16NYJHZsCZ8a5J+uJi13NNOE1O8=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

**11.8.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description [ en ] *undefined.*

[ es ] *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

**11.8.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.8.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by the CA Camerfirma Camerales - 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA Camerfirma Certificados Camerales - 2016*

**Service digital identities****X509SubjectName**

**Subject CN:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA CERTIFICADOS CAMERALES - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

X509SKI

X509 SK I 16NYJHZsCZ8a5J+uJil3NNOE1O8=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2016-04-01T00:00:00Z

#### 11.8.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.1

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.1.2

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.1

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.9.4.2.2

#### 11.9 - Service (withdrawn): Qualified Certificates issued by CA AC Racer-2016

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.





**Subject OU:** RACER - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Thu Feb 18 17:10:18 CET 2016

**Valid to:** Wed Dec 14 17:10:18 CET 2039

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A48141D539E761BA4E1C8CEC4E8CC60BC7B792B304471D28FEBE5DF21E4588459F9FE  
C48B129EC3B289A63FE48DC340C938400514955A8D4099D0EE02FA464A88FF704BDF3FEA2812882BBA4947F3B718A35A8C7D27D9586A6DF289EBAE895D94D43085E  
DF9A2ADC8556F926BB039B5EA073727532C9823A4BAEAE8A8C521650368C71AC376E0E3FC054C51D21443B22AAB9CF5F95F5DA0989E8AB04160A8594337F60EA2F  
DEA35E7A37F5F1C0353544F7A6E59FD16125C811D4D173F907B612E26A9FCDB665E43A75C51604CED677D14A7EB660B9C0F1D4683A6F7AA14A366486330FD013FC  
1F1A606E39E7903A98C60AC417E711584BE7034E3B02770D2898F664E0736FFA6225821F3108C2E459FDB2305E1445F2E081843635D2AC9AA4227D547D585CE38C3D  
738D5DB625725669233E43D50D46E4A6696A4CCB4E3623CA7C81B17B862814F4DF50C37E6010E55CA571969D55CD729B503A783F53B6F19BA61ACFD5CB7D24B27  
A9E0A970212CB753AE760DA9DAEF69D2E3E6DF7C09AFDB38D395B78DBE737BAE8D4D1565F0D55FF4D24A42E1919DB2396B2ADB342546576ABB7F33DF66F4  
91543EA7A12C58AD8E9C70906598B469587D4367F9633C96D63CAF0A13CBAA1D7A6CC558911AF6EB0BEC0125E47E8866741C649F415E71F1028C452C4EABEBE8B  
C4595A3AC4F2D9C458C8E2BCF23B18B53ACD482C9F1F0203010001

**Basic Constraints** IsCA: true - Path length: 1

**Subject Key Identifier** BB:71:68:C8:7B:3F:A5:63:BC:06:E5:0A:AA:5B:3A:46:6A:62:68:4C

**Authority Key Identifier** 08:28:6E:C7:17:02:0D:DF:4D:EF:C9:A2:77:AD:59:68:2D:5D:DF:45

**Authority Info Access** [http://www.camerfirma.com/certs/ac\\_camerfirma-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma-2016.crt)  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points** [http://crl.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl.camerfirma.com/ac_camerfirma-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl1.camerfirma.com/ac_camerfirma-2016.crl)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** A7:9D:0E:26:DB:A2:4A:A6:FC:B0:A4:7C:44:C7:CA:F6:F4:F5:DD:DE:F0:34:11:59:2D:4B:21:07:  
E1:0A:C7:2B

**X509SubjectName**

**Subject CN:** RACER - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** *RACER - 2016*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2017-07-21T00:00:00Z*

#### 11.9.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2*

#### 11.9.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

#### 11.9.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** [en] *Qualified Certificates issued by CA AC Racer-2016*

**Name** [es] *Certificados Reconocidos emitidos por la CA Racer-2016*

## Service digital identities

### X509SubjectName

**Subject CN:** *RACER - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *RACER - 2016*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

### X509SKI

**X509 SK I** *u3FoyHs/pWO8BuUKqls6RmpiaEw=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

### 11.9.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2*

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

**11.9.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.9.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA AC Racer-2016*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA Racer-2016*

**Service digital identities****X509SubjectName**

**Subject CN:** *RACER - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *RACER - 2016*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *u3FoyHs/pWO8BuUKqls6RmpiaEw=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2016-04-01T00:00:00Z

#### 11.9.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.2

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.2.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.8.4.1.2

#### 11.10 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016

#### Service digital identities



**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject ST:** MADRID

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Thu Apr 14 10:48:09 CEST 2016

**Valid to:** Fri Mar 09 09:48:09 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D272B E57E DB3834B81C45C922EFB91C9D9D8093991E15C8C0B7160B091B194724CD7  
B8919023B BB CB A0EE7727236D73E142F7A21A D61BFFDAE85CAB3B2A96AD16EA3C324F79C7245D89BB5E6C70DA3FD1D195510003109D5C47725A5B E62334882BE  
404D6A3D0B6ACA6FF2632862D E4C93A63057D7C4D478CAF784B90CB1C7E8E4D9740946B6CF23838BDFDFCE75F875D2759AB721DD1384F0EF4201B66B9C4E5358  
ACBF3E201CS DC39C8A92D13D140B26D97C171095AA23081530608F86626FC935C08A8C71C2875CD DD159875D3D43C4E D320973E583717BD F98D72B5DB75BE82C  
2CC1D39C97A7B00D45615E60B2AFB58B83C4AA CD6E467A34DEDEE9D0268887042A848190D2CF5424DF493F2E7ECB4ACA9566AE EF1702D84D441252B76F7A2AF9  
C25E30F5EC CC790F10938E F2561017C1C81AA453785ABE F9FE6A6C8EC70D30C3EB9FC5E04B181B907C025F603F4723C280C29B86FE89D385782AF64435F20E3047B  
780ADF D591F9C28940E90488785E38B3721901C358B926245B0F1C74357ECB4FC4BF54836266FE2E33A4DS26F652D7AE0E5A98CD2BCFBFC63A4FA27D7444A83114AE  
B62E8518DA62CB887856CA3E4759D2CE786ED13D8878C71B25AA6999EC07BA2A170BA21CE9A75D330AF82160734241835D312E73B016FE4EA727E70ECDD0A2437A  
C3099C27D1F312B361647DE1AE5DD1592A634612C3C19020301001

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** 70:B8:F8:24:C7:51:CA:CE:22:80:92:08:C9:C0:68:2F:C1:47:58:51

**Authority Key Identifier** 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B

**Authority Info Access**  
<http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** EE:DD:45:7A:F1:35:3D:76:F4:8E:7C:61:23:F3:91:40:E5:F9:A0:69:CA:51:B4:3E:EA:86:15:C9:CE:C0:D4:BB

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287



**Subject OU:** AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject ST:** MADRID

**Subject L:** MADRID

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2016-06-30T22:00:00Z

#### 11.10.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 11.10.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.99.18.1

**Description**

#### 11.10.3 - History instance n.1 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Service digital identities**

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA FOR NATURAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject ST:** MADRID

**Subject L:** MADRID

**Subject C:** ES

**X509SKI**

**X509 SK I** cLj4JMdRys4igJIIycBoL8FHWFE=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2016-06-23T22:00:00Z

## 11.11 - Service (granted): Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Service digital identities****Certificate fields details**

**Version:** 3



**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Thu Apr 14 10:33:07 CEST 2016

**Valid to:** Fri Mar 09 09:33:07 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100CE5B D77F6452806E007E661B02C8D8A037EA FB83F9C20C73B1F3CC54FC E467A1184E8  
F22834CDE1ADE87F5E117EA22D1EA32CE41AD680B676866199A56D6FFFA718DDEB1EFC31D9CAAB89A9F08F5A3EC1302DF7A959E7856D26C9E2D301436976A329B  
13E3358A0079EB30F21721AE064DCE0FA35AFD1C2F1F906FF5C CD5151299380CE E48D0A A9F3DD8C65B4E0104156864DD7D6EDB8F69075F8219722931828F2717A0  
BE08E4D4591149BE29BB8461D7F26B6438A3488B6E6B716475DDFB8FB9159DF0C383B4034ECA D453722191EK4913D8B92744F7B7495C932AF4BD AE CD C40FAA4D4A  
24EAF110B4EC4F45D9DDED E A67C107A57954D5E2977DDA F5CB9773B1D13D41B068932D8358452148183E21079A31E815A32C409522D243687EAF E462840393F2  
795339808DB9561B61595F6F5F735D944064927370571E085417E986F06E48CE88A79FEC4B B0ED1E FE7C CC185203B69C231C D3CC A57DB2F239B0DDA018534F62FF250  
1C5A035B9F6A69A91054DC40EB24CFB19B41A C8E8FD5CF6288A22468187651F2FD324B1F812A09684DD536FEE13005328CD3193B81E BD AC7C10819A81DA4A9F66C  
E9C02BC32EC37E95EB0E6D510B0F18A51E797413C105196B14C78AA CA79586555C6DE42CD62B282D19B86AC366D86E614DA9122416C4B4244F23DAD1F02392801B  
0352D4E2B8245AE9EB52A1A4555740071B59A170203010001

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42

**Authority Key Identifier** 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B

**Authority Info Access**  
<http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 3A:80:66:26:6D:28:BD:28:CC:D0:F5:64:C8:FB:C1:21:9B:4F:FA:E4:03:E0:1E:50:39:D3:0F:24:00:F0:EB:09

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject ST:** MADRID

**Subject L:** MADRID

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2018-03-15T01:00:00Z

#### 11.11.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 11.11.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.99.18.1

**Description**

#### 11.11.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016

**Service digital identities**

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Subject O: AC CAMERFIRMA S.A.

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject ST: MADRID

Subject L: MADRID

Subject C: ES

**X509SKI**

X509 SK I *wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2017-07-21T00:00:00Z

**11.11.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.11.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**11.11.4 - History instance n.2 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ en ] *Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

Name [ es ] *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

**Service digital identities****X509SubjectName**

Subject CN: AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Subject O: AC CAMERFIRMA S.A.

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject ST: MADRID

Subject L: MADRID

Subject C: ES

**X509SKI**

X509 SK I wyeFk9cvlsUbrHYz2YaiSn1oFEI=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time**

2016-06-30T22:00:00Z

**11.11.4.3 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

**11.11.4.4 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.11.5 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

**Name** [es] *Certificados Reconocidos emitidos por AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject 2.5.4.97:** *VATES-A82743287*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA FOR LEGAL PERSONS - 2016*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject ST:** *MADRID*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *wyeFk9cvlsUbrHYz2YaiSn1oFEI=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2016-06-23T22:00:00Z*



**11.11.5.5 - Extension (not critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

**11.12 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Service digital identities****Certificate fields details**

**Version:** 3



**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Thu Apr 14 17:13:34 CEST 2016

**Valid to:** Wed Feb 08 16:13:34 CET 2040

**Public Key:**  
3082022230D06092A864886F70D010105000382020F003082020A0282020100AB336D8855EB1EFE4EAD37DBE5C887F1786EF6950A2B0E934CCB0695C326FA9A0A08  
44C2B3AE3B C23BF1306D1B9C541E1486AE850719BD79B9CECA B963D76A33C35F60A2A77696A3DB721443D2ECB5644B68A68CEE27D91CF469B8641E1DD2C291  
4B373E8F3854373200DB6B1CC7D0953753CEA4F6FB E68780416D21902DSD1055AA351D16D3E40EC2271ABCDBE7E29F2FD B013EB932C2C58641CEE6DA5BAAF6FAC3F  
386E336A56AF66E9C6EE5160460AD5FEDE99DFC4FDC6C4E2DDF5004B1439BE98BBE9CB91933199678E242EF6DE7A434330759BE6E0ADFD9660045E38D2910F8935B  
8809A DAF85B273D22C11265C853CB D5CF90A1B9B44E9C698C2998E89D238E9DAE7A3D A1B377DD89FA CD82CF1EB93844FE9575E784EA14721D64E5AE69BE BBAD1D  
A07E46BES4DC1F0244A245639225039CS B682BE504C28C5EDD34D3A2D3F650D7707A03D11A9866DDA DB5E401DB58BA09EF75271A55449B773D613FD5A9E5A0DC8  
6D BA12C0C1062170E03AEA517029079D9EC504258882F1B6277C DC1F8E3C43F1A354CD1D A2E207D4448A68601F7B35510C663ABE91E49D2CD68BD21C22AE3AA7B0  
0E86391C5C8D3A82CDDB829B4E4713CD A14CFED82E79BBEBDD797C5EFC2663B59B2E8FB013423907539DB76510193CED6B58E70164EA14B A7BF B3C9323D FB56D  
6193FD646DE C6651F13591BDCB9085B88931CA7D4DD593BF68D0203010001

**Basic Constraints** IsCA: true - Path length: 1

**Subject Key Identifier** 4E:36:56:A8:58:CE:1B:83:85:60:4C:D4:1B:A1:DF:72:3D:AF:7B:5F

**Authority Key Identifier** D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84

**Authority Info Access**  
[http://www.camerfirma.com/certs/ac\\_camerfirma-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma-2016.crt)  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
[http://crl.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl.camerfirma.com/ac_camerfirma-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl1.camerfirma.com/ac_camerfirma-2016.crl)

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** EF:41:1C:83:7A:C3:30:41:85:E5:39:13:FE:36:9B:F8:FF:65:98:C2:A5:2B:DB:1B:6E:2D:EA:B5:DC :C7:F0:6F

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2017-07-21T00:00:00Z

### 11.12.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.12.2 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Name** [es] Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

#### Service digital identities

##### X509SubjectName

**Subject CN:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

## X509SKI

**X509 SK I** TjZWqFjOG4OFYEzUG6Hfcj2ve18=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

### 11.12.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 11.12.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** [ en ] *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016*

## Service digital identities

### X509SubjectName

**Subject CN:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID



**Issuer CN:** AC CAMERFIRMA - 2016

**Issuer O:** AC CAMERFIRMA S.A.

**Issuer 2.5.4.97:** VATES-A82743287

**Issuer SERIAL NUMBER:** A82743287

**Issuer OU:** AC CAMERFIRMA - 2016

**Issuer OU:** see current address at <https://www.camerfirma.com/address>

**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject CN:** AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Thu Apr 14 16:58:36 CEST 2016

**Valid to:** Wed Feb 08 15:58:36 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C429BB37DD77A98403830ADE86B56042E9E886EDC868B920344E266EA133181FE84C54  
ADE554440B82D4E2C9832C29866154D51A7A23AD8798BD9377C8C2874180A368D953F4656DC88538448ADDE1A8C3B3F3C043B6F519D274843C6D54CB4B82A80  
EAD673BC9822F243E83F9E9F4F6C568A63AFD6D4665DC38B356B1B30F19C41EA8C D6D83FC2FD8AD4F8CS000E7D32C85E83F5112FB913560E974BD5DD98E81FBD2  
62017456965241DB099EE54340CADE37C3424332839671305481E982A50C60530298B7369C4C0C3FE7BA31B2302809C1EDC766658983E2CFDF623AA0F1580703  
F555C7F90A408EFC3ADC590F87670851F9B119449EA5747D2F1C840F5C53F03D64DBCC08D77936689BF92D9524F674D962E3D54CC61382FA3494D4AC66AD0E3E91E  
1F18AB3FD1C7AC65737AFDA35ACB22AD99296318D8D0FB64D012E08B8C9930673AFB984C2644630C959D631D31C86B2441440A76F4D0B3E61A7552EE91E471E  
B078358409A87DD516CBC93C6671C8C0FC9E3CDCT430D0C5A8A9E08882B98485C8E28AC58930AC8B63B1FEDC144C4E20FDC9EF568F0C6B8F597C92A92176D95F  
92103DEA2135021E38ED1C85CTE7E68856922DA83E8E8BAF53DF48196261E88130E39AE018D93DBF9E77329FB899437062B4D6FA0CCBDB1D325E0A06B8EFDS7EAA  
8159CD2C2F3C0986756769D5D7E7E2916F9AB004CD0203010001

**Basic Constraints** IsCA: true - Path length: 1

**Subject Key Identifier** 80:21:DF:71:F1:EF:D4:6B:DA:33:86:D1:0F:BE:C5:DD:65:4C:84:5E

**Authority Key Identifier** D2:84:97:44:4D:D9:88:EE:7C:25:BF:52:80:B3:29:48:9B:8B:18:84

**Authority Info Access** [http://www.camerfirma.com/certs/ac\\_camerfirma-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma-2016.crt)  
<http://ocsp.camerfirma.com>

**Extended Key Usage** *id\_kp\_clientAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: https://policy.camerfirma.com*

**CRL Distribution Points** [http://crl.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl.camerfirma.com/ac_camerfirma-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma-2016.crl](http://crl1.camerfirma.com/ac_camerfirma-2016.crl)

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *4D:20:C9:51:E1:34:89:3B:C5:90:1B:FA:F8:E2:40:A5:BE:7D:00:59:6D:D3:1C:40:42:92:52:F2:E0:4F:8B:46*

**X509SubjectName**

**Subject CN:** *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject 2.5.4.97:** *VATES-A82743287*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Subject OU:** *see current address at https://www.camerfirma.com/address*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2017-07-21T00:00:00Z*

**11.13.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*



**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2

**11.13.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.13.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Service digital identities****X509SubjectName**

**Subject CN:** AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**X509SKI**

**X509 SK I** *gCHfcfHv1GvaM4bRD77F3WVMhF4=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**11.13.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

**11.13.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**11.13.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Name** *[ es ]* *Certificados Reconocidos emitidos por AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016*

**Subject O:** *AC CAMERFIRMA S.A.*

Subject 2.5.4.97: VATES-A82743287

Subject SERIAL NUMBER: A82743287

Subject OU: AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016

Subject OU: see current address at <https://www.camerfirma.com/address>

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

**X509SKI**

X509 SK I *gCHfcHv1GvaM4bRD77F3WVMhF4=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2016-06-23T22:00:00Z

**11.13.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.1*

**Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.17326.20.16.1.2.1.1.2*

**11.14 - Service (withdrawn): Qualified Certificates issued by Camerfirma Corporate Server II - 2015**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>



**Valid from:** Thu Jan 15 10:21:16 CET 2015

**Valid to:** Tue Dec 15 10:21:16 CET 2037

**Public Key:**

```
30820222300D06092A864886F70D01010105000382020F003082020A0282020100B79D228D445B9F56AF6FB5E3D4684FDA15920C047C376C3F0D0BCB447E78CE4C3A4
DF9C38A43FE86A10C4D099CBE8B007A23C880B249176ACAA1F9231B308E5F5DB0F23482DE1B3B283F4BB3DB4733BA0DDF21D70E185DD4D18DA1C3F9E167A
17BD9F113758FD3210A3E0F6626330507BAFE0A897B6F7A23E4B2FE97924CF96AEAA9A4F31A6250FACB8F4012C198DB3384508F0F3B8FAD5B150A86FB2232E5BC
D7BB7DD57663303A345ED1275802260B4088B2A8918D744A37BBE7E0F145F16894915E1985FA3527E43BD4C68D031C7000ACBDE443E5A4B42CC7FEEDD96DA7B
6810B3C718993857E7E2034776A232C4A8100591B4F4E8782D3992F3A7B3869A3B5F8DBA8BA5866A3F98B377CE9998E952DB9BA789802B956E0A3191592DC
4D4BD0C31163C4B5952042CF8E74DE6CEB87B8E2536FDEE8840D4EAAAC28AB9156247148F627735F314B3B42D7F8BA023D2D95B19AF596D0EE0278FB67869D1A3
44FC680C3A94CC7B6E365E0D7C71427503104FE602A3874540A7BD15122956EE041134A33E5FCF79D4C1C595560AE6FE3920A935F812A9D97BEC8198A57A84511857
ED68561E4CCD3781E9E7CC4B81C9EEDC0AED44C142C585F5234B506EF44AA09DD277095D170962003D38499CF34F8BACB85B5D632C9ED74864B3DE0A1DB583
41A9822DA95C718307AE4973F4091D9E596870ABC59F0203010001
```

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** 63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34:65

**Authority Key Identifier** F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17:19

**Authority Info Access**  
[http://www.camerfirma.com/certs/root\\_chambers-2008.crt](http://www.camerfirma.com/certs/root_chambers-2008.crt)  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth - id\_kp\_serverAuth

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersroot-2008.crl>  
<http://crl1.camerfirma.com/chambersroot-2008.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 66:EA:E2:70:9B:54:CD:D1:69:31:77:B1:33:2F:F0:36:CD:D0:F7:23:DB:30:39:ED:31:15:55:A6:CB:F5:FF:3E

**X509SubjectName**

**Subject CN:** Camerfirma Corporate Server II - 2015

**Subject L:** Madrid (see current address at <https://www.camerfirma.com/address>)

**Subject SERIAL NUMBER:** A82743287

**Subject O:** AC Camerfirma S.A.

**Subject OU:** AC CAMERFIRMA

**Subject C:** ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

Status Starting Time 2021-11-16T02:00:00Z

**11.14.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**11.14.2 - History instance n.1 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service Name

Name [ en ] Qualified Certificates issued by Camerfirma Corporate Server II - 2015

Name [ es ] Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015

**Service digital identities**

**X509SubjectName**

Subject CN: Camerfirma Corporate Server II - 2015

Subject L: Madrid (see current address at <https://www.camerfirma.com/address>)

Subject SERIAL NUMBER: A82743287

Subject O: AC Camerfirma S.A.

Subject OU: AC CAMERFIRMA

Subject C: ES

**X509SKI**

X509 SK I Y+nw8FYAaGWwIWwOXNcZCJ0INGU=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2017-08-16T01:00:00Z

**11.14.2.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**11.14.3 - History instance n.2 - Status: withdrawn**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en]* *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

**Name** *[es]* *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

**Service digital identities****X509SubjectName**

**Subject CN:** *Camerfirma Corporate Server II - 2015*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject OU:** *AC CAMERFIRMA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Status Starting Time** *2017-07-21T00:00:00Z*

**11.14.3.2 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en]* *undefined.*

*[es]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1*

**Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2*

**11.14.3.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.14.4 - History instance n.3 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

**Name** [es] *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

**Service digital identities****X509SubjectName**

**Subject CN:** *Camerfirma Corporate Server II - 2015*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject OU:** *AC CAMERFIRMA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**11.14.4.4 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**



**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

#### 11.14.4.5 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 11.14.5 - History instance n.4 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

**Name** [ en ] *Qualified Certificates issued by Camerfirma Corporate Server II - 2015*

**Name** [ es ] *Certificados Reconocidos emitidos por Camerfirma Corporate Server II - 2015*

##### Service digital identities

##### X509SubjectName

**Subject CN:** *Camerfirma Corporate Server II - 2015*

**Subject L:** *Madrid (see current address at <https://www.camerfirma.com/address>)*

**Subject SERIAL NUMBER:** *A82743287*

**Subject O:** *AC Camerfirma S.A.*

**Subject OU:** *AC CAMERFIRMA*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *Y+nw8FYAaGWwIWwOXNcZCJ0INGU=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2016-06-23T22:00:00Z*

**11.14.5.6 - Extension (not critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.16.2.1.2

**11.15 - Service (withdrawn): Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016

**Name** [es] Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES - 2016

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 2579987068168128523



**Subject C:** ES

**Valid from:** Mon Apr 18 17:43:54 CEST 2016

**Valid to:** Tue Mar 13 16:43:54 CET 2040

**Public Key:**  
3082 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 02 0F 00 30 82 02 0A 02 82 02 01 00 D3 35 56 9F 5D AE 7A 67 3F D4 0F B4 57 B5 3E 68 F0 D6 8B CB E8 C2 6C C0 68 0F 6E A9 E1 19 CD 37 41 36 F6 49 DF 54 AB 6B D9 70 B0 0C 92 26 52 00 5C F3 96 09 FF D8 1E 22 70 7C CB DD BA 58 72 23 95 4E 1B C3 BB 31 E3 A0 8A 0E 97 3F 8A 79 3F 61 69 C9 18 08 78 60 7E 4A 65 A7 6C 70 EB 27 31 4D D8 74 FB 16 C8 8E 7E 26 E0 9F D4 E6 19 2A 53 1D F1 22 EA F9 0E E4 29 CE DB 35 48 F4 2F AA 31 A4 0A 4A A3 E4 32 8B 2D 4A F3 E7 4B FE 48 0E 1E 68 A5 8C 49 27 4A 3E EE BE 7A E7 12 A7 15 5C 4F 89 42 40 23 19 A2 CE 4F FB 15 BD AA 08 7A CA 1D 4E 12 68 30 A7 C4 D2 B4 87 2C 3C D0 0D 62 8A EF 00 6E AE 54 D0 0B 45 21 59 2B 97 0F B7 53 A1 46 CB 8E 4C 69 DD B0 89 07 CB 9E 8E 13 0D 27 FF A8 EC 5E B5 CC 2D 46 AE FE 5B 04 94 3B 88 82 AC 6A 48 E6 18 D8 24 D8 84 BE 55 78 43 5A A6 1E 05 46 2F CA E5 75 88 B7 59 1A BE EC 88 0A 25 9D 0F EF 6E 91 F1 7B 52 31 38 9D D9 58 8C 77 39 31 BC 08 06 04 06 9F 3C F3 8B 28 1 E D9 2E 99 86 49 39 98 F3 4B 1A F6 22 5D 49 51 60 2F 49 3E 08 42 09 02 D3 DE 99 5B A8 A2 CC 43 5D BD F2 0A 76 45 13 93 0C 5A 82 75 E7 10 EA 21 PC 97 ED 8E 2F 58 EF 43 D2 EA F9 2E 4A 07 F0 99 E7 C6 6 7 E2 11 67 17 51 CC 8D 0F 13 C5 55 8F 90 FC BE 20 61 74 84 47 D2 35 4B E9 50 5C B9 A8 1C 8C 99 BD 49 D2 92 A7 D5 A7 73 F3 EF 39 73 8C D9 E1 1B 1D F1 5A 27 03 45 F7 31 92 38 E9 61 5B 22 74 97 F1 87 FE D7 1D C3 1A A6 09 04 86 E5 15 A6 A5 1E CD C2 60 C9 BE 7C 21 42 AF F2 76 45 E9 8A A8 0A CE C3 2E 3B 49 72 C0 70 C8 64 08 B4 28 A7 62 F2 F9 F1 5A 85 ED 76 1F 12 A2 BD F2 9B 0E 0F C0 7C 66 82 52 2A 0 1 2D 0D E9 7D F0 5F 54 CD A9 61 6D 35 14 61 F2 39 F2 F1 02 03 01 00 01

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** EC:95:33:3B:71:C0:D2:B1:9C:58:23:0B:36:41:BC:54:9E:2C:92:1D

**Authority Key Identifier** 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B

**Authority Info Access**  
<http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_serverAuth

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 93:7D:7D:5D:0B:7F:B7:DB:03:93:99:BC:0B:67:0C:C2:03:C7:AB:4E:33:2F:AE:45:3C:C3:8E:C1:8 8:DD:EA:2B

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA FOR WEBSITES - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA FOR WEBSITES - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

## X509SKI

**X509 SK I** 7JUzO3HA0rGcWCMLNkG8VJ4skh0=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2021-11-16T02:00:00Z

### 11.15.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

### 11.15.2 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES - 2016

**Name** [es] Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES - 2016

#### Service digital identities

#### X509SubjectName

**Subject CN:** AC CAMERFIRMA FOR WEBSITES - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA FOR WEBSITES - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**X509SKI**

**X509 SK I** 7JUzO3HA0rGcWCMLNkG8VJ4skh0=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2018-03-15T01:00:00Z

#### 11.15.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

#### 11.16 - Service (withdrawn): Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [ en ] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[ es ] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

##### Service Name

**Name** [ en ] Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

**Name** [ es ] Sellos de tiempo cualificados emitidos por AC CAMERFIRMA TSA - 2016

##### Service digital identities

##### Certificate fields details

**Version:** 3

**Serial Number:** 1564901409084605058



**Subject C:** ES

**Valid from:** Thu Apr 14 12:42:09 CEST 2016

**Valid to:** Fri Mar 09 11:42:09 CET 2040

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100A6CCBF2518578E0963C094892E363D4FB3E3B1BD691D6E7BC5CF0264787A5EC8D7B35110449F9BD841049D26A63B75E821B330E22321BD75492354F6C3519B40B4FC3F88661B58CA9111C2E8A1C44059F399C13756FC5435BBD850FAE43DD7E7BAD19863FE9A4FB76EA038045503A5E459029C0484FD20FA4DAF0F22353BF1CDA4DB73ED4449FD8E013B8A78F1219DA4BE4B4AD046F1B03C2640DA0D8A015E27ED A8737C7660B2693C2A34C295D91A484FB982C077569CA2A6064F30413DC11B1635F41F663ABA99B4DC93856E6232BEAE9A9E21AAE73837EA7761575C8B0378626A BC9E883F54163F03E7E4C894D244918F18B9FAD115A9A5FCDD778C9ECA1CE17F3DFDA5D333F7205CE8E821B10E1EC15090D05C0611B024C5B3C5A2DC15E9F0A ;28D51EA6C89B7B9E619256A26E2C2BEB8A06E3FB7E682768C2F08680B0099C018376E36C9EBDB14D4728014B89C9CD9E4ACD06CEA665CEA0AC99EDB725AC2F7 8C4EEFF70CEDFBC945537D0588702CCCA30344BDE8339B4AB53B4B8F7552178363B1F4A66129AF369B7F634DFC4FB13BB3CC22D30F8D738FA8E75171AA485AA9B A2CD09692E5387CF7B59ADBF3F25D9BB0AE2D4248FA9912C5F6297AB32DF135ECA9934992DE7D887E75E7433BE337D3C2218DFFEA31E8E62E0BDB9A8B7E0723 E7410915EA9C1D82282EE66363726DF68A67BF937711B4BF10203010001

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** 1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C

**Authority Key Identifier** 9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B

**Authority Info Access**  
<http://www.camerfirma.com/certs/chambersofcommerceroot-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** id\_kp\_timeStamping

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points**  
<http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** BA:AE:2C:63:38:85:7D:50:20:0F:6F:73:DD:45:E6:5A:A2:D8:95:BE:D4:67:5B:6E:39:6B:72:22:E0 :18:A9:B8

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA TSA - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA TSA - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID



**Subject ST:** MADRID

**Subject C:** ES

## X509SKI

**X509 SK I** Hm21xj/vklVeN/rb/RCqtk7Tiw=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

## Status Starting Time

2023-10-24T00:00:00Z

## Scheme Service Definition URI

**URI** [en] [https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\\_Camerfirma.aspx](https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx)

**URI** [es] [https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\\_Camerfirma.aspx](https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU_Camerfirma.aspx)

### 11.16.1 - History instance n.1 - Status: granted

## Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

## Service Name

**Name** [en] Qualified timestamps issued by AC CAMERFIRMA TSA - 2016

**Name** [es] Sellos de tiempo cualificados emitidos por AC CAMERFIRMA TSA - 2016

## Service digital identities

### X509SubjectName

**Subject CN:** AC CAMERFIRMA TSA - 2016

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA TSA - 2016

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID



**Issuer CN:** CHAMBERS OF COMMERCE ROOT 2018

**Issuer O:** AC CAMERFIRMA S.A.

**Issuer 2.5.4.97:** VATES-A82743287

**Issuer SERIAL NUMBER:** A82743287

**Issuer OU:** CHAMBERS OF COMMERCE ROOT 2018

**Issuer OU:** see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address)

**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject CN:** AC CAMERFIRMA FOR WEBSITES 2018

**Subject O:** AC CAMERFIRMA S.A.

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** AC CAMERFIRMA FOR WEBSITES 2018

**Subject OU:** see current address at <https://www.camerfirma.com/address>

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Thu Oct 04 11:00:23 CEST 2018

**Valid to:** Thu Aug 28 11:00:23 CEST 2042

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100BF1672154B7F47CB1BDA2F172AB842B9CA8CCS3DA8BC2C5C7D50953388E8DD73FF9DD  
C80570CFC291DE587697BB490E3ED530616DB0DAF43DC7DF16E3B856A7029DC60BC66806E30FD27F30C886F9E40DD5D8DCEA11A42C8F5F9E595D438DC433  
2BF0C5CF7A1B833B9D859B383D88048A5B7DDA1C0A91BD823C2ED91867B941993416E757CA8DDBCB059BDFE1B822C0035E333EES36984E0668B071E4F8B8838  
6DC9F9D7B90A927F3F07D05D4EA609511684947E3F2D15F71BBFB6C7A2CCAFFAD79CC6A1276AE4D611456AB36F74D88421833D5029544BF1D1CE7B2DFF23615B3B  
5AEBCA8B614237BF47CC597B40FFDA5C101E815810DB63E3EAE34A7A937C77905C93C2DD197584034884188A80D28CD8790D4B42C453D42879910116E3F5A29  
D5ECC20AE85EF1079A7F706F75701646FDCB6D8FF6CEABD8803AAFC8E2FE97A317072E8EAD9B773118015179F738F9713D456DD115C152BF2A18F83FE5B87E324  
B7A5AFBDCCDD5C3552B66A3E8944461DCE7E7DA962909485CFB2086E846F7CB9D9D416CC52A67AFE677AD590A0C24C4817D1898194204B0308081FC3785B5BF06AF  
D505DA834C85BB8076906F13186ACB9178853E4B2C0DEBC184AB7017C94771D9C6956237689F5DDE7131A.F00C.AB1B.D3.5C.5E.D4.FF.28.74.D8.33.1D.61.B4.D4.0F.55.CB.8C.73.C9  
.EA.69.F3.25.2E.7F.0D.4C.4B.F8.2A.E8.C2.C5.94.20.BB.6C.F6.3B.0F.E1.49.48.2D.02.03.01.00.01

**Basic Constraints** IsCA: true - Path length: 2

**Subject Key Identifier** 50:47:5C:2F:BA:12:7B:5F:74:38:1B:07:12:31:FB:68:4C:A8:EF:DE

**Authority Key Identifier** B5:2E:59:20:B2:AF:43:BB:95:3D:C2:51:99:E3:75:55:34:48:B0:1C

**Authority Info Access** <http://www.camerfirma.com/certs/chambersofcommercerooroot2018.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: https://policy.camerfirma.com*

**CRL Distribution Points** <http://crl.camerfirma.com/chambersofcommercerooroot2018.crl>  
<http://crl1.camerfirma.com/chambersofcommercerooroot2018.crl>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *BF:0F:44:91:F3:71:48:9D:F2:EB:18:7B:DC:B4:B2:ED:D9:AB:2D:A0:16:CC:64:08:4C:AC:45:19:5E:F3:59:0D*

**X509SubjectName**

**Subject CN:** *AC CAMERFIRMA FOR WEBSITES 2018*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject 2.5.4.97:** *VATES-A82743287*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA FOR WEBSITES 2018*

**Subject OU:** *see current address at https://www.camerfirma.com/address*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *UEdCL7oSe1900BsHEjH7aEyo794=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2020-04-28T00:00:00Z*

**11.17.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**11.17.2 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by AC CAMERFIRMA FOR WEBSITES 2018*

**Name** [ es ] *Certificados Cualificados emitidos por AC CAMERFIRMA FOR WEBSITES 2018*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC CAMERFIRMA FOR WEBSITES 2018*

**Subject O:** *AC CAMERFIRMA S.A.*

**Subject 2.5.4.97:** *VATES-A82743287*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *AC CAMERFIRMA FOR WEBSITES 2018*

**Subject OU:** *see current address at <https://www.camerfirma.com/address>*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *UEdcL7oSe190OBsHEjH7aEyo794=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2019-09-15T22:00:00Z*

**11.17.2.1 - Extension (critical): additionalServiceInformation**



**Issuer ST:** MADRID

**Issuer C:** ES

**Subject CN:** AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** PKI SERVICES

**Subject O:** AC CAMERFIRMA S.A.

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Wed Oct 20 17:12:16 CEST 2021

**Valid to:** Fri Oct 16 17:12:16 CEST 2037

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100EF5615D8536F9EF15D6B02223DFC7AE0CEA16441B821C0E541344D62FE1167677574BA  
DBFB3A8A508AE45A60A38A1557790C345E72B06536DA6620C378AFEAFC1B16A46A400F9A1A8953AF143E7A7CCD8781244AA1652A97D2AEAF4551B35516803  
4558BF3EB1619E8698855A6C65BA902036FCDDCB80FA321014769AA4226D0E93791E0942462AB154BD0510E970559D9A251DB86DCA274BEC226B254CCF31E4F5B6  
5192D154CAD7CE8C9BA9FD4C74B0412811F28DF48B25835CE7AE403B06A5A36F9B22AF6EF2BBABE0F98EFEDD63C118F9C87BCEDE5D9DE7E85DAB5B2996B20B22  
BE6850A294E7EA3AB7B9CA7A215DCDAF5F52CE00343A16C7394D80DE70650CE0D6CFAKBB7F54ED09A2400B3435D255BA6CDDC759A53983DE9CB5774382E5F6FDS  
C91A683C42774EE6376CE22F2DC2ACC5B1C8B5IDAFAE507AA8ACE8A9DCFC83F9C37E02C354F80E2E3EE9B79E25EE5FE73D69AE41AF405C72B7E9FD84962F80D2F17  
AE6D463C7E5D6E7A85DA4CEB8F31A6AD9840E8390ED7B9B4717DAB9ACFE8451202D3957326C937610D34F232FD8FC93763A9335DB7BC021BBAA8A30E649EA786D1  
DABDF4B8126E0E0A929A870F1035E82265D493B10362253C0C33E602318A989FB93CA415390C74EC09CC12854A5B70E0B2AFBDA6C849A4179809AEC89F103F1372  
D2B9A38F189A1AB157A4EB6DF2FC9C921B5C16691104085D0203010001

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** C7:6F:2D:C4:10:8A:6E:DD:F3:11:65:69:C6:4A:43:7B:C3:0F:68:14

**Authority Key Identifier** 51:11:32:7A:10:D0:D8:8C:4C:09:84:97:B1:A9:3E:B2:54:BA:87:C9

**Authority Info Access**  
<http://ca.camerfirma.com/certs/camerfirmaroot2021.crt>  
<http://ocsp2021.camerfirma.com>

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy2021.camerfirma.com>

**CRL Distribution Points**  
<http://crl.ca.camerfirma.com/camerfirmaroot2021.crl>  
<http://crl1.ca.camerfirma.com/camerfirmaroot2021.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 4D:18:7D:4E:5B:BA:7B:BA:D4:22:B7:5B:EF:B4:DC:B2:17:9D:1C:CD:11:5A:18:D2:C8:35:0F:FF:AC:31:6B:34

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

**Subject 2.5.4.97:** VATES-A82743287

**Subject SERIAL NUMBER:** A82743287

**Subject OU:** PKI SERVICES

**Subject O:** AC CAMERFIRMA S.A.

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**X509SKI**

**X509 SK I** x28txBCKbt3zEWVpxkpDe8MPaBQ=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2023-01-31T00:00:00Z

**11.18.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.18.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.17326.10.21.1.2.3

**Policy Identifier:**



**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.3.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.4.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.5.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.6.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.7.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.8.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.1.3

### 11.18.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ es ] *Certificados Cualificados emitidos por AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021*

**Name** [ en ] *Qualified Certificates issued by AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021*

**Subject 2.5.4.97:** *VATES-A82743287*

**Subject SERIAL NUMBER:** *A82743287*

**Subject OU:** *PKI SERVICES*

Subject O: AC CAMERFIRMA S.A.  
 Subject L: MADRID  
 Subject ST: MADRID  
 Subject C: ES

X509SKI

X509 SK I x28txBCKbt3zEWVpxkpDe8MPaBQ=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2022-09-06T00:00:00Z

**11.18.3.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**11.18.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.  
 [es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.2.3

**Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.3.3

**Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.4.3

**Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.5.3

**Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.17326.10.21.1.6.3



**Issuer O:** AC Camerfirma S.A.

**Issuer OU:** AC CAMERFIRMA

**Issuer C:** ES

**Subject CN:** AC CAMERFIRMA QUALIFIED TSU - 2022

**Subject 2.5.4.97:** VATES-A82743287

**Subject O:** AC CAMERFIRMA S.A.

**Subject C:** ES

**Valid from:** Thu Jun 09 14:13:07 CEST 2022

**Valid to:** Wed Jun 07 14:13:07 CEST 2028

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100894532F53056B8743A3F67A4DB5F051D77623428E44187624A9EAC37A2E6D9972FFA3612A7E8611B939393314D8372A961DA6F10F20D5EBE7C0B845ED5072D444315D06F38333FB04644E9B6573EFA2D87AC7B853A2750BC5978349D70DB2B98332CA3BA5517CBBAEB98F36636D9460CB05F430435A2951906769E4BF7DBE67502DDBD35BA97CE924B8549E645193198EA25E83C741C6A6AD408EAD35562AF4E38719392E671F74E3DD8159EBD6D4E2E9EE7566E6A24514C4A8B759EF82547E2ABDB355113664D89010EDC3DBF7207E217B2D5108A0849FDB8D7E0328A0F5BD727CC9CAA2CE7F801DD3D2DD8872E1AA8831ACD53B3163A87BEFE893113C10203010001

**Basic Constraints** IsCA: false

**Extended Key Usage** id\_kp\_timeStamping

**Subject Key Identifier** 64:40:E1:6F:F9:CC:F3:CA:B2:3D:84:D0:3E:74:8C:C5:F0:A2:86:80

**Authority Info Access**  
[http://www.camerfirma.com/certs/camerfirma\\_tsaii-2014.crt](http://www.camerfirma.com/certs/camerfirma_tsaii-2014.crt)  
<http://ocsp.camerfirma.com>

**Authority Key Identifier** 17:C5:40:BC:2A:F8:45:B8:AB:33:BF:F8:6F:49:6C:F6:17:CA:B7:D4

**CRL Distribution Points**  
[http://crl.camerfirma.com/camerfirma\\_tsaii-2014.crl](http://crl.camerfirma.com/camerfirma_tsaii-2014.crl)  
[http://crl1.camerfirma.com/camerfirma\\_tsaii-2014.crl](http://crl1.camerfirma.com/camerfirma_tsaii-2014.crl)

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.17326.10.13.1.3  
CPS pointer: <https://policy.camerfirma.com>

**Key Usage:** digitalSignature - nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 4A:98:A7:75:E6:1B:2F:8A:A7:6B:EB:D4:64:3B:E0:53:F3:E5:A8:5D:4D:D7:06:2D:02:80:5B:C7:DB:2C:18:92

**X509SubjectName**

**Subject CN:** AC CAMERFIRMA QUALIFIED TSU - 2022

**Subject 2.5.4.97:** VATES-A82743287

**Subject O:** AC CAMERFIRMA S.A.

**Subject C:** ES

**X509SKI**

**X509 SK I** ZEDhb/nM88qyPYTQPnSMxfCihoA=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2022-10-10T00:00:00Z

## 12 - TSP: COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

### TSP Name

<b>Name</b>	[ en ]	COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA
<b>Name</b>	[ es ]	COLEGIO OFICIAL DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

### TSP Trade Name

<b>Name</b>	[ en ]	VATES-Q2863012G
<b>Name</b>	[ en ]	REGISTRADORES DE ESPAÑA
<b>Name</b>	[ es ]	REGISTRADORES DE ESPAÑA
<b>Name</b>	[ en ]	Colegio de Registradores de la Propiedad y Mercantiles de España
<b>Name</b>	[ en ]	Colegio de Registradores de la Propiedad y Mercantiles

### PostalAddress

<b>Street Address</b>	[ en ]	Calle Príncipe de Vergara, nº 70
<b>Locality</b>	[ en ]	Madrid
<b>State Or Province</b>	[ en ]	Madrid
<b>Postal Code</b>	[ en ]	28006
<b>Country Name</b>	[ en ]	ES

### PostalAddress

<b>Street Address</b>	[ es ]	Calle Príncipe de Vergara, nº 70
<b>Locality</b>	[ es ]	Madrid
<b>State Or Province</b>	[ es ]	Madrid
<b>Postal Code</b>	[ es ]	28006
<b>Country Name</b>	[ es ]	ES

### ElectronicAddress



**Issuer O:** *Colegio de Registradores de la Propiedad y Mercantiles de España*

**Issuer C:** *ES*

**Subject CN:** *Registradores de España - CA Interna*

**Subject OU:** *Certificado Propio*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles de España*

**Subject C:** *ES*

**Valid from:** *Wed Jan 31 11:03:38 CET 2007*

**Valid to:** *Thu Jan 31 09:31:10 CET 2019*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C50991DE03DD7981B8E03F8271732F50BD6A3AA6B73CDBACB2C80F0CF23CAEADB37  
C8764AE987B9F7D2B886B91E2D6539A7597885E15B37496CD2FA869C2E8049416D1D4046F311105043AFBA47F2FEF12C8BFD84136E2480CB7DC3F8ED0FF6BA678  
C8AF6248B02B0807D3BEA8FD59080D801288A943623064F8B48F4943D4F887F6A2F6D0649C95A2ECAS3CA7A9AC4980D2C287D7B460225DE6FDC8CF5627FB269  
D6F4F6B86A58D81AEC663A8822B65B4A124E2E14EADAF97363E819A65EAB97FF271CDBCACE5F183876CF0E663B0670173828B86794C6BCF3F205DE6F2E384164  
7157E12ECC8AAA452AE485726649D269F787F67DFCDB93A5F757B0203010001

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *8E:F0:63:77:74:70:20:BE:CB:94:84:95:31:15:2A:D9:0D:E5:9D:0B*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://pki.registradores.org/normativa/index.htm>*  
*CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]*

**Authority Info Access** *[http://pki.registradores.org/certificados/ca\\_raiz\\_scr.crt](http://pki.registradores.org/certificados/ca_raiz_scr.crt)*

**Authority Key Identifier** *1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5*

**CRL Distribution Points** *[http://pki.registradores.org/crls/ar1\\_scr.crl](http://pki.registradores.org/crls/ar1_scr.crl)*  
*<ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *3A:50:ED:C2:11:47:D8:67:37:75:C7:07:D3:2F:19:7D:DC:BE:34:75:BF:07:41:50:31:9E:11:61:DD:77:19:59*

**X509SubjectName**

**Subject CN:** *Registradores de España - CA Interna*

**Subject OU:** *Certificado Propio*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles de España*



**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2018-02-06T01:00:00Z

#### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 12.1.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 12.1.2 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Certificate issued by internal CA

**Name** [es] Certificado reconocido emitido por la CA certificados internos

#### Service digital identities

##### X509SubjectName

**Subject CN:** Registradores de España - CA Interna

**Subject OU:** Certificado Propio

**Subject O:** Colegio de Registradores de la Propiedad y Mercantiles de España

**Subject C:** ES

##### X509SKI

**X509 SK I** jvBjd3RwIL7LIISVMRUq2Q3lnQs=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

### 12.1.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 12.1.3 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Qualified Certificate issued by internal CA

Name [es] Certificado reconocido emitido por la CA certificados internos

#### Service digital identities

##### X509SubjectName

Subject CN: Registradores de España - CA Interna

Subject OU: Certificado Propio

Subject O: Colegio de Registradores de la Propiedad y Mercantiles de España

Subject C: ES

##### X509SKI

X509 SK I [jvBjd3RwIL7LIISVMRUq2Q3lnQs=](http://uri.etsi.org/TrstSvc/Svctype/CA/QC)

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2009-02-13T00:00:00Z

### 12.2 - Service (withdrawn): Qualified Certificate issued by external CA

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name



**Subject Key Identifier** 73:8A:03:F5:F4:B3:63:91:BC:4B:35:58:EA:A2:89:F3:19:1C:D3:94

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <http://pki.registradores.org/normativa/index.htm>  
 CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2006)]

**Authority Info Access** [http://pki.registradores.org/certificados/ca\\_raiz\\_scr.crt](http://pki.registradores.org/certificados/ca_raiz_scr.crt)

**Authority Key Identifier** 1B:8D:59:1C:B3:B7:58:62:64:66:AC:E2:E4:A4:F6:A2:19:12:F6:E5

**CRL Distribution Points**  
[http://pki.registradores.org/crls/ar1\\_scr.crl](http://pki.registradores.org/crls/ar1_scr.crl)  
 ldap://ldap.registradores.org/CN=CA%20RAIZ,OU=CERTIFICADO%20PROPIO,O=COLEGIO%20DE%20REGISTRADORES,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 13:51:F3:92:83:7A:73:9D:D8:53:D7:F8:E2:FE:FF:39:12:77:18:79:82:1F:A4:76:14:DB:87:A3:AF:03:5C:E6

**X509SubjectName**

**Subject CN:** Registradores de España - CA Externa

**Subject OU:** Certificado Propio

**Subject O:** Colegio de Registradores de la Propiedad y Mercantiles de España

**Subject C:** ES

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2018-02-06T01:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**12.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 12.2.2 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified Certificate issued by external CA*

**Name** [ es ] *Certificado reconocido emitido por la CA certificados externos*

#### Service digital identities

##### X509SubjectName

**Subject CN:** *Registradores de España - CA Externa*

**Subject OU:** *Certificado Propio*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles de España*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *c4oD9fSzY5G8SzVY6qKJ8xkc05Q=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

### 12.2.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 12.2.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified Certificate issued by external CA*

**Name** [ es ] *Certificado reconocido emitido por la CA certificados externos*

**Service digital identities****X509SubjectName**

**Subject CN:** *Registradores de España - CA Externa*

**Subject OU:** *Certificado Propio*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles de España*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *c4oD9fSzY5G8SzVY6qKJ8xkc05Q=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2009-02-13T00:00:00Z*

**12.3 - Service (granted): Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC****Interna****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[en]* *Qualified Certificate issued by Autoridad de Certificación de los Registradores - AC Interna*

**Name** *[es]* *Certificados cualificados emitidos por Autoridad de Certificación de los Registradores - AC Interna*

**Service digital identities****Certificate fields details**

**Version:** *3*

**Serial Number:** *33250107883580613301075761566452252203*



**Authority Key Identifier** *DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

**CRL Distribution Points**  
*http://pki.registradores.org/crls/arl\_psc\_corpme.crl*  
*ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

**X509SubjectName**

**Subject CN:** *Autoridad de Certificación de los Registradores - AC Interna*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles*

**Subject 2.5.4.97:** *VATES-Q2863012G*

**Subject C:** *ES*

**X509SKI**

**X509 SKI** *2LBZoZQFEituoRdXKNMRAVuvvQ0=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2017-02-22T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**12.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*





**Subject 2.5.4.97:** VATES-Q2863012G

**Subject C:** ES

**Valid from:** Mon Jun 06 17:06:11 CEST 2016

**Valid to:** Tue Jun 06 17:06:11 CEST 2028

**Public Key:**

30820222300D06092A864886F70D01010105000382020F003082020A0282020100AF558D12C7C897B8D267EA0570B2D4A78E9F582E20598EBF3CF458087FD7F8ED0A440FB99203C1655F01A02EAA1F7382D95F4B7D1F21D51C0DA54F26707AC19E3CE6C5C37606EFD80C42168B99A0B4D7BAA443936B0B37A821FC5078639B9512DCF90DC42DBCB3B7DC0B42D8935B6E048373DBB345651895205F0A63228AFE884DF56E8B0549D440118400B0075322AF0CB53476D6985CE0D3A0B7092C246FA4259D52D766B3C6C4E4AA7273C76CFCD245A8A3E16ED693E8C8DD5C935293440D108B0955BC9E9EA3EED12016A554537861127F42AC303467021DF8A3C9E0C9B9C7A605664B74B158740B84D9E702A2E903EB19A73C6EBAD59E5A5A87C35BF7275A3A70A1CA77C9C47A16D8DC4393469707557E627A745400843319886DCA0335FC2B01189D604D96F5ABF6695286BC4CB33DF26C586207567D174C5608A48E0C3BFC74F606A4B24DED35C3030C761D4811C6D2871E77A60BDA53DDC6128F7D0550E401B562C32ADCF1757AE60A36B33925F36C38CBA88F1B5ED81BB271D7B28CB60720BCD436BF6C63712C787BA391F1106A3A4SCAA0D72A842DD3A99C847A937DE2703A9A6FC75646AA BFC13D6393047968961DE5E97CE2D0C89384B2FC8D7B990D7D54A7641EA8273A6A22BF5D57462F8A886F2EF84021383C7C5338F793A5EC061C7C605387C44BF121D BC69AC80FADE97DF613331550E16F3FA6B39FA30203010001

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 35:B8:65:CD:35:A0:A2:0F:9A:AF:E2:75:FE:DB:0C:48:52:3D:03:40

**Certificate Policies** Policy OID: 2.5.29.32.0

CPS pointer: <http://pki.registradores.org/normativa/index.htm>

CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]

**Authority Info Access** [http://pki.registradores.org/certificados/ac\\_raiz\\_psc\\_corpme.crt](http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt)

**Authority Key Identifier** DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7

**CRL Distribution Points** [http://pki.registradores.org/crls/arl\\_psc\\_corpme.crl](http://pki.registradores.org/crls/arl_psc_corpme.crl)  
 ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** FB:7E:80:1D:60:D0:40:92:30:59:BD:31:CC:04:FA:49:C5:20:86:05:A0:09:C5:CB:D0:17:39:00:67:E6:57:17

**X509SubjectName**

**Subject CN:** Autoridad de Certificación de los Registradores - AC Externa

**Subject O:** Colegio de Registradores de la Propiedad y Mercantiles

**Subject 2.5.4.97:** VATES-Q2863012G

**Subject C:** ES

**X509SKI**

**X509 SK I** NbhIzTWgog+ar+JI/tsMSFI9A0A=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

<b>Service status description</b>	[en]	undefined.
	[es]	undefined.

**Status Starting Time** 2017-02-22T00:00:00Z

### Scheme Service Definition URI

<b>URI</b>	[en]	<a href="https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>
<b>URI</b>	[es]	<a href="https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>

#### 12.4.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

#### 12.5 - Service (granted): Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo para crear y firmar tokens tiempo sellos calificados.

### Service Name

<b>Name</b>	[en]	Qualified timestamps issued by Autoridad de Certificación de los Registradores - TSA - 01
<b>Name</b>	[es]	Sellos de tiempo cualificados emitidos por Autoridad de Certificación de los Registradores - TSA - 01

### Service digital identities

#### Certificate fields details

<b>Version:</b>	3
<b>Serial Number:</b>	21558290793992193382977497126169320943



**CRL Distribution Points** [http://pki.registradores.org/crls/crl\\_int\\_psc\\_corpme.crl](http://pki.registradores.org/crls/crl_int_psc_corpme.crl)  
<ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint>

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *33:5A:CB:56:33:A7:34:AB:EA:D2:34:93:AD:91:0E:FC:C9:D7:EB:C3:43:06:E1:E4:8C:7B:AF:07:0C:11:2D:57*

**X509SubjectName**

**Subject CN:** *Autoridad de Certificación de los Registradores - TSA - 01*

**Subject O:** *Colegio de Registradores de la Propiedad y Mercantiles*

**Subject 2.5.4.97:** *VATES-Q2863012G*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *xMg5TNW6/kTKFbW1SyzUhusP9Gk=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2018-02-06T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**12.6 - Service (granted): OCSP Responses issued by Autoridad de Certificación de los Registradores - VA****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>

**Service type description** *[en]* *A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.*  
*[es]* *A los servicios de estado de validez del certificado que expidan Protocolo de estado de certificados en línea (OCSP) firmaron respuestas y el funcionamiento de un servidor OCSP como parte de un servicio de un proveedor de servicios de confianza que expiden certificados reconocidos.*

**Service Name**

**Name** *[en]* *OCSP Responses issued by Autoridad de Certificación de los Registradores - VA*



**Subject Key Identifier** *D8:B0:59:A1:94:05:12:2B:6E:A1:17:57:28:D3:11:01:5B:AF:81:0D*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://pki.registradores.org/normativa/index.htm>*  
*CPS text: [Certificado sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)]*

**Authority Info Access**  
*[http://pki.registradores.org/certificados/ac\\_raiz\\_psc\\_corpme.crt](http://pki.registradores.org/certificados/ac_raiz_psc_corpme.crt)*

**Authority Key Identifier**  
*DA:72:38:61:40:06:97:E5:02:F1:6D:69:DB:04:01:E9:E7:0C:A3:E7*

**CRL Distribution Points**  
*[http://pki.registradores.org/crls/arl\\_psc\\_corpme.crl](http://pki.registradores.org/crls/arl_psc_corpme.crl)*  
*<ldap://ldap.registradores.org/CN=AC%20RAIZ,O=Colegio%20de%20Registradores%20-%20Q2863012G,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint>*

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*F6:7A:0C:98:7D:0D:7D:5E:7E:CC:4A:69:FD:20:00:5E:D2:BD:50:3B:6D:CA:05:24:92:B2:D5:A3:ED:0B:B3:D8*

**X509SubjectName**

**Subject CN:**  
*Autoridad de Certificación de los Registradores - AC Interna*

**Subject O:**  
*Colegio de Registradores de la Propiedad y Mercantiles*

**Subject 2.5.4.97:**  
*VATES-Q2863012G*

**Subject C:**  
*ES*

**X509SKI**

**X509 SK I**  
*2LBZoZQFEituoRdXKNMRAVuvgQ0=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2018-02-06T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[en] [http://pki.registradores.org/certificados/ac\\_va\\_psc\\_corpme.crt](http://pki.registradores.org/certificados/ac_va_psc_corpme.crt)*

URI [ es ] [http://pki.registradores.org/certificados/ac\\_va\\_psc\\_corpme.crt](http://pki.registradores.org/certificados/ac_va_psc_corpme.crt)

**12.6.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>



**13 - TSP: Banco Español de Crédito, S.A****TSP Name**

**Name** [ en ] *Banco Español de Crédito, S.A*

**Name** [ es ] *Banco Español de Crédito, S.A*

**TSP Trade Name**

**Name** [ en ] *VATES-A28000032*

**Name** [ en ] *Banesto CA*

**Name** [ es ] *Banesto CA*

**Name** [ en ] *Banesto S.A. - C.I.F. A28000032*

**Name** [ es ] *Banesto S.A. - C.I.F. A28000032*

**PostalAddress**

**Street Address** [ es ] *Avda. Gran Vía de Hortaleza, 3*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28043*

**Country Name** [ es ] *ES*

**PostalAddress**

**Street Address** [ en ] *Avda. Gran Vía de Hortaleza, 3*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28043*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://ca.banesto.es*

**URI** [ en ] *mailto:correo@banesto.es*



**Subject O:** *Banesto S.A. - C.I.F. A28000032*

**Subject L:** *Mesena 80 28033 - Madrid*

**Subject C:** *ES*

**Valid from:** *Fri Mar 15 13:10:53 CET 2002*

**Valid to:** *Thu Mar 15 00:00:00 CET 2012*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A02820101009D61444589190774D1D2500AEDB21F50ED9A1DDB9308880DC6AA175D002046FB8983553E97D50DAEDA7097BB231B41D45CAD1E1F4D6F466BE1BDB863624BD0C5621AA69D470930CB31309E9C62CE8F6B9D9C2BB30F736C170BCC188E480716939B492C4023A592A012B88D2C526A3806D475A49201075D39B42CD617E8F635AA3B3160F4A72E39A59E93070B6E3AD9878FB616420BE5140AB99D4759D477AA092557D1F5B4F627C888285DAE7888A9BBB7380B8FC0FA2AA6F5F8DB8EEB90A06B006F2F56D53AA76D89D4368B36A5B77248C2843717B175AFCA6E336B4A94C9D8986574B6D1C21C1F1C78CFB843CE4B92F23422F66B045B57735E6CAB38A30203010001

**Issuer Alternative Name** *ca@banesto.es*

**Subject Alternative Name** *ca@banesto.es*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *23:44:4C:6B:ED:72:4E:E4:71:1B:00:3B:74:23:D9:37:90:BB:03:A5*

**Authority Key Identifier** *EA:3A:16:3A:10:54:BB:1A:55:2E:0F:11:83:AB:A4:50:6A:2B:9B:89*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.11076.1.1*  
*CPS pointer: <http://ca.banesto.es/Repositorio/DPC/>*  
*CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]*

**CRL Distribution Points** *<http://ca.banesto.es/CRL/PSCRootBanesto.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *53:99:01:61:F9:3C:B7:9E:6E:75:13:06:74:A4:53:DE:7E:2D:22:C8:1B:51:10:40:68:8B:66:7E:3F:65:35:30*

**X509SubjectName**

**Subject CN:** *PSC Banesto Clientes*

**Subject O:** *Banesto S.A. - C.I.F. A28000032*

**Subject L:** *Mesena 80 28033 - Madrid*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** 2016-06-30T22:00:00Z

### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 13.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

**other Criteria List assert=at Least One Identifier** 1.3.6.1.4.1.18838.1.1

#### 13.1.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 13.1.3 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

### Service Name

**Name** [en] *Banesto Qualified Certificates of previous CA PSC Banesto Clientes*

**Name** [es] *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior*

### Service digital identities

#### X509SubjectName

**Subject CN:** *PSC Banesto Clientes*

**Subject O:** *Banesto S.A. - C.I.F. A28000032*

**Subject L:** *Mesena 80 28033 - Madrid*

**Subject C:** *ES*

#### X509SKI

**X509 SK I***I0RMa+1yTuRxGwA7dCPZN5C7A6U=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>**Status Starting Time**

2013-05-23T22:00:00Z

**13.1.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]****Qualifier type description***[en]**it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.**[es]**está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.***Criteria list assert=atLeastOne****other Criteria List assert=at Least  
One Identifier**

1.3.6.1.4.1.18838.1.1

**13.1.4 - History instance n.2 - Status: supervisionincessation****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name***[en]**Banesto Qualified Certificates of previous CA PSC Banesto Clientes***Name***[es]**Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior***Service digital identities****X509SubjectName****Subject CN:***PSC Banesto Clientes***Subject O:***Banesto S.A. - C.I.F. A28000032***Subject L:***Mesena 80 28033 - Madrid***Subject C:***ES***X509SKI****X509 SK I***I0RMa+1yTuRxGwA7dCPZN5C7A6U=***Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>**Status Starting Time**

2009-10-16T00:00:00Z

**13.1.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne**

**other Criteria List assert=at Least One Identifier** 1.3.6.1.4.1.18838.1.1

**13.1.5 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Banesto Qualified Certificates of previous CA PSC Banesto Clientes

**Name** [es] Certificados Reconocidos de Banesto de CA PSC Banesto Clientes anterior

**Service digital identities****X509SubjectName**

**Subject CN:** PSC Banesto Clientes

**Subject O:** Banesto S.A. - C.I.F. A28000032

**Subject L:** Mesena 80 28033 - Madrid

**Subject C:** ES

**X509SKI**

**X509 SK I** I0RMa+1yTuRxGwA7dCPZN5C7A6U=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2004-11-25T00:00:00Z

**13.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
-----------------------------------	------	--



**Issuer C:** ES

**Subject CN:** PSC Banesto Clientes

**Subject O:** Banesto S.A. - C.I.F. A28000032

**Subject L:** Mesena 80 28033 - Madrid

**Subject C:** ES

**Valid from:** Wed Nov 26 19:50:00 CET 2008

**Valid to:** Mon Dec 30 23:49:59 CET 2030

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100AC3B90F4FB3C4CFF8717186F20A8A5D0CE7BD9A58E34C04590463CC650164852F9A848E04353CDD0FE3D4707D213EEC27191293FA0C618B418A32C5F2BC7F021B8E831910BE983DFD12ED5F437F94015136DA39B74F27C2EE7A48B523ED80B75E900082D8E4CCFB4342DD4E5C1FC0A082CD85644B15323D654751680B68665DD79D9532520C2BEE5C9C790302DC8E2CED0C7D438554EF856E8517336F9D45B115329F3C5B449C3F35377EAD2E21961B9CA603B03DE899A605B9B5B5F9441F9431C6D81072443479F0BE08AA69BCFA48B680E3BE730D76555F2D5A5C62B32493EE780E575E000A0C177999A6BBA33AF94BD3C1454C8A734333210112F957EDBAA2BF6C0D98177380E57CFB2DF0199B0BA242B5911A305BBA159FF0180191659A894482A88EF9B459E96B35173522C53C54E1830C37260437F90F8552E2B966687B8D97E17171C2C38F43A9B5BA0730B2D31252E1D8432C30725A4C02317C0D6484A8D336ED6AFDC78FF543D19157B1DE3395DA13DAD37C03C9F9B66115F0B79DB76159282919B347BFFCF3D149B0048C469B22CF501F80F7932C46D3E85C32814C9605A641729DEFAD23F341904A788CB0172AD4A14E30749670960C671A9E948C49436A985776830E0D268C72C8D6F5DE61C997B683F64CB9E9BDA0166DE240CEA8379169C0239D1FC13E1AF0E7C400A57758A9AC44193717DF1B39CB2CFD193410E70203010001

**Issuer Alternative Name** ca@banesto.es

**Subject Alternative Name** ca@banesto.es

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 53:77:C9:90:55:A7:3A:34:65:97:14:7D:97:3E:F2:FC:02:2E:0E:AC

**Authority Key Identifier** 5A:BD:29:5D:C8:17:96:57:CD:6F:29:D3:E1:A2:F5:D4:4E:C4:CC:F2

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://ca.banesto.es/Repositorio/DPC/>  
CPS text: [Este certificado ha sido emitido por PSC Banesto Root y se encuentra regulado por las condiciones generales definidas en su Declaracion de Practicas de Certificacion.]

**CRL Distribution Points** <http://ca.banesto.es/CRL/PSCRootBanesto.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 46:6C:9A:9D:76:A6:A4:04:68:F9:18:BE:BD:9D:9F:10:41:78:A7:60:03:78:45:94:FF:94:3B:F7:8D:73:29:B9

**X509SubjectName**

**Subject CN:** PSC Banesto Clientes

**Subject O:** Banesto S.A. - C.I.F. A28000032

**Subject L:** Mesena 80 28033 - Madrid

**Subject C:** ES



**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** [en] *undefined.*  
[es] *undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

### **Scheme Service Definition URI**

**URI** [en] *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** [es] *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

### **13.2.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] *undefined.*  
[es] *undefined.*

#### **Criteria list assert=atLeastOne**

**other Criteria List assert=at Least One Identifier** *1.3.6.1.4.1.18838.1.1*

### **13.2.2 - Extension (critical): additionalServiceInformation**

#### **AdditionalServiceInformation**

**URI** [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### **13.2.3 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

### **Service Name**

**Name** [en] *Banesto Qualified Certificates of CA PSC Banesto Clientes*

**Name** [es] *Certificados Reconocidos de Banesto de CA PSC Banesto Clientes*

### **Service digital identities**

#### **X509SubjectName**

**Subject CN:** *PSC Banesto Clientes*

**Subject O:** *Banesto S.A. - C.I.F. A28000032*

**Subject L:** *Mesena 80 28033 - Madrid*

Subject C: ES

X509SKI

X509 SK I U3fJkFWnOjRllxR9lz7y/AIuDqw=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

Status Starting Time 2013-05-23T22:00:00Z

### 13.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]

<p>Qualifier type description</p>	<p>[en]</p>	<p>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</p>
	<p>[es]</p>	<p>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</p>

#### Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier 1.3.6.1.4.1.18838.1.1

### 13.2.4 - History instance n.2 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Banesto Qualified Certificates of CA PSC Banesto Clientes

Name [es] Certificados Reconocidos de Banesto de CA PSC Banesto Clientes

#### Service digital identities

##### X509SubjectName

Subject CN: PSC Banesto Clientes

Subject O: Banesto S.A. - C.I.F. A28000032

Subject L: Mesena 80 28033 - Madrid

Subject C: ES

X509SKI

X509 SK I U3fJkFWnOjRllxR9lz7y/AIuDqw=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time**

2009-10-16T00:00:00Z

**13.2.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]****Qualifier type description**

[en]

it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne**

**other Criteria List assert=at Least  
One Identifier**

1.3.6.1.4.1.18838.1.1

**14 - TSP: EDICOM CAPITAL, S.L.****TSP Name**

**Name** [ en ] *EDICOM CAPITAL, S.L.*

**Name** [ es ] *EDICOM CAPITAL, S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B96490867*

**Name** [ en ] *EDICOM*

**Name** [ es ] *EDICOM*

**Name** [ es ] *INTERCAMBIO ELECTRONICO DE DATOS Y COMUNICACIONES SL*

**Name** [ es ] *EDICOM CAPITAL SL*

**PostalAddress**

**Street Address** [ en ] *Calle Charles Robert Darwin, número 8*

**Locality** [ en ] *Paterna*

**State Or Province** [ en ] *Valencia*

**Postal Code** [ en ] *46980*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Calle Charles Robert Darwin, número 8*

**Locality** [ es ] *Paterna*

**State Or Province** [ es ] *Valencia*

**Postal Code** [ es ] *46980*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:acedicom@edicomgroup.com*

**URI** [ en ] *http://acedicom.edicomgroup.com*



**Subject O:** EDICOM

**Subject OU:** PKI

**Subject CN:** ACEDICOM Root

**Valid from:** Fri Apr 18 18:24:22 CEST 2008

**Valid to:** Thu Apr 13 18:24:22 CEST 2028

**Public Key:**

```
30820222300D06092A864886F70D01010105000382020F003082020A0282020100FF9295E1680676B42C85848CAFD805429556324FF90659B10757B C36ADB620201F2188
6B57C5A38B1E58B9FB13D82D9FBD3237BF2C156D8E85F421D21391D907AD0105D6F3BD77CE5F42810AF96AE38300A82B2E55136381CA471C7B9C16577A1B83600
43A3E653CD01DEDEA4D60CBA8EDED904EE1756229B8F63FD4D160B77B778CF925B5D16D99122E4F1A88E6EA0492AE3D11B951423D87B03185AF795A9CFE74E
5E924F43FCAB3AAD5122666B9E20CD798CE0458A595400AB7449D13742B C2A5EB22159810D88BC5049F1D8F60E5061B9BCTB979A03DA2233F423F6BFA1C037B30
SDCE6CC0BF6E1B5FBF67B88419D515EE78CB90363162C9BC02AB465F9BE1A6884343D908EAD16E41D097FAA88383FB667FD3496F51D8C3074CB38EE056CABD4F
CF400B7005B8532167633E9D8A5999D0500AA16E6F3817D6F7DAA866DAD1574D3C4A271AA44147DE732B81FBCD5F14EBD6F170239D70E98423AC7003E9266311E
A0BD14AFF189DB2D77B2F3AD996FB8E1E92AE1355C8D927F6DC481B8024C185E3779D9AA4A30C111D0DC8B414EEB5825709BF20587E2F2223D870CB796C94BF2
A92AC8FC872BD71A50F827E82F43E33ABDD85771FDCEA6525BF9DD4DED5F66F89EDBB939C762175F0924C29F72F9C012E5E50469E640C14B3075B5C2736CF1075
C45241435AE83F16A4D897FAFB3D82D66F03687F52B53020301001
```

**Basic Constraints** IsCA: true

**Authority Key Identifier** A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50

**Subject Key Identifier** A6:B3:E1:2B:2B:49:B6:D7:73:A1:AA:94:F5:01:E7:73:65:4C:AC:50

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <http://acedicom.edicomgroup.com/doc>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 03:95:0F:B4:9A:53:1F:3E:19:91:94:23:98:DF:A9:E0:EA:32:D7:BA:1C:DD:9B:C8:5D:B5:7E:D9:4  
0:0B:43:4A

## X509SubjectName

**Subject C:** ES

**Subject O:** EDICOM

**Subject OU:** PKI

**Subject CN:** ACEDICOM Root

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

## Status Starting Time

2017-12-01T01:00:00Z

## Scheme Service Definition URI

**URI** [en] <http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt>

**URI** [es] <http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt>

URI [en] <http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt>

URI [es] <http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt>

#### 14.1.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

#### 14.1.2 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.

[es] undefined.

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier 1.3.6.1.4.1.30051.3.1.1

#### 14.1.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 14.1.4 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

##### Service Name

Name [en] Qualified certificates issued by the AC ACEDICOM Root

Name [es] Certificados Reconocidos emitidos por la CA ACEDICOM Root

##### Service digital identities

##### X509SubjectName

Subject C: ES

Subject O: EDICOM

Subject OU: PKI

Subject CN: ACEDICOM Root

**X509SKI**

**X509 SKI** *prPhKytJttczoaqU9QHnc2VMrFA=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**14.1.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC*

**14.1.4.2 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**other Criteria List assert=at Least One Identifier** *1.3.6.1.4.1.30051.3.1.1*

**14.1.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**14.1.5 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by the AC ACEDICOM Root*

**Name** *[ es ]* *Certificados Reconocidos emitidos por la CA ACEDICOM Root*

**Service digital identities****X509SubjectName**

**Subject C:** *ES*

**Subject O:** *EDICOM*



Subject OU: PKI

Subject CN: ACEDICOM Root

X509SKI

X509 SK I prPhKytJttzdzoaqU9QHnc2VMrFA=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2008-11-07T00:00:00Z

#### 14.1.5.4 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC>

#### 14.1.5.5 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

Criteria list assert=atLeastOne

other Criteria List assert=at Least One Identifier 1.3.6.1.4.1.30051.3.1.1

#### 14.2 - Service (granted): Qualified certificates issued by the CAEDICOM01

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

Service Name

Name [ en ] Qualified certificates issued by the CAEDICOM01

Name [ es ] Certificados Reconocidos emitidos por la CA CAEDICOM01

#### Service digital identities



**Authority Key Identifier** *14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.30051.2.3.1.1*  
*CPS text: [Certification Practice Statement]*  
*CPS pointer: http://acedicom.edicomgroup.com*

**CRL Distribution Points** *http://acedicom.edicomgroup.com/caedicomroot.crl*

**Subject Alternative Name** *acedicom@edicomgroup.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *33:9D:15:B1:65:CA:81:61:E4:D3:79:26:18:C6:FD:E8:4E:49:04:D0:46:69:54:1C:EE:6B:D3:33:BC:D5:B5:F4*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Calle Charles Robert Darwin 8 - 46980 - Paterna*

**Subject O:** *EDICOM*

**Subject SERIAL NUMBER:** *B96490867*

**Subject CN:** *CAEDICOM01*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time***2017-12-01T01:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**14.2.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.4

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.5

**14.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**14.2.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**14.2.4 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates issued by the CAEDICOM01*

**Name** [ es ] *Certificados Reconocidos emitidos por la CA CAEDICOM01*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject L:** *Calle Charles Robert Darwin 8 - 46980 - Paterna*

**Subject O:** EDICOM

**Subject SERIAL NUMBER:** B96490867

**Subject CN:** CAEDICOM01

**X509SKI**

**X509 SK I** bWqI+C7qfy/NwPR2d5PmRTLviwU=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

#### 14.2.4.1 - Extension (critical): Qualifiers [NotQualified]

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

#### **Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.6
-------------------	------------	-----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.4
-------------------	------------	-----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.30051.2.3.2.5
-------------------	------------	-----------------------------------

#### 14.2.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

#### 14.2.5 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[en]	Qualified certificates issued by the CAEDICOM01
-------------	------	---

<b>Name</b>	[es]	Certificados Reconocidos emitidos por la CA CAEDICOM01
-------------	------	--

#### Service digital identities

**X509SubjectName**

**Subject C:** ES

**Subject L:** Calle Charles Robert Darwin 8 - 46980 - Paterna

**Subject O:** EDICOM

**Subject SERIAL NUMBER:** B96490867

**Subject CN:** CAEDICOM01

**X509SKI**

**X509 SK I** bWqI+C7qfy/NwPR2d5PmRTLviwU=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2014-12-31T23:00:00Z

**14.2.5.3 - Extension (not critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.4

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.30051.2.3.2.5

**14.3 - Service (withdrawn): Sellos cualificados de tiempo emitidos por EDICOM**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [ es ] *Sellos cualificados de tiempo emitidos por EDICOM*

**Name** [ en ] *Qualified timestamps issued by EDICOM*

**Service digital identities****Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [ en ] *undefined.*

[ es ] *undefined.*

**Status Starting Time**

*2019-12-10T01:00:00Z*

**Scheme Service Definition URI**

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [ es ] <https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**14.3.1 - History instance n.1 - Status: granted****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

**Name** [ es ] *Sellos cualificados de tiempo emitidos por EDICOM*

**Name** [ en ] *Qualified timestamps issued by EDICOM*

**Service digital identities****X509SubjectName****X509SKI**

**X509 SK I** *ziAzKLt9C4McA/Uq1OAJ6qYXaGY=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time**

*2017-12-01T01:00:00Z*

**14.4 - Service (withdrawn): Conservación de sellos electrónicos cualificados proporcionado por EDICOM****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

**Service type description** [ en ] *A preservation service for qualified electronic signatures.*

[es] *Un servicio de la preservación de las firmas electrónicas reconocidas.*

## Service Name

**Name** [es] *Conservación de sellos electrónicos cualificados proporcionado por EDICOM*

**Name** [en] *Preservation of qualified electronic seals provided by EDICOM*

## Service digital identities

### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] *undefined.*

[es] *undefined.*

### Status Starting Time

2023-12-21T00:00:00Z

### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

## 14.4.1 - Extension (critical): additionalServiceInformation

### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

## 14.4.2 - History instance n.1 - Status: granted

### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

## Service Name

**Name** [es] *Conservación de sellos electrónicos cualificados proporcionado por EDICOM*

**Name** [en] *Preservation of qualified electronic seals provided by EDICOM*

## Service digital identities

### X509SubjectName

### X509SKI

**X509 SK I** *f5On7ZPIbFzYVwO/qd9aELFd72Y=*

### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>



**Status Starting Time** 2017-12-01T01:00:00Z

#### 14.4.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 14.5 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada EDICOM

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

**Service type description** [ en ] *An electronic delivery service providing qualified electronic deliveries.*  
[ es ] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

##### **Service Name**

**Name** [ es ] *Servicio cualificado de entrega electrónica certificada EDICOM*

**Name** [ en ] *Qualified electronic registered delivery service EDICOM*

##### Service digital identities

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [ en ] *undefined.*  
[ es ] *undefined.*

**Status Starting Time** 2022-10-20T00:00:00Z

##### **Scheme Service Definition URI**

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 14.5.1 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

##### **Service Name**

**Name** [ es ] *Servicio cualificado de entrega electrónica certificada EDICOM*

**Name** [ en ] *Qualified electronic registered delivery service EDICOM*

**Service digital identities****X509SubjectName****X509SKI****X509 SK I** *f5On7ZPIbFzYVwO/qd9aELFd72Y=***Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time** *2019-02-28T01:00:00Z***14.6 - Service (withdrawn): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM****Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q***Service type description** *[en] undefined.**[es] undefined.***Service Name****Name** *[es] Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM***Name** *[en] Qualified validation service for qualified electronic signatures and qualified electronic seals by EDICOM***Service digital identities****Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description** *[en] undefined.**[es] undefined.***Status Starting Time** *2022-06-29T00:00:00Z***Scheme Service Definition URI****URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx***URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx***14.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**14.6.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**14.6.3 - History instance n.1 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q">http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q</a>
-------------------------	---

**Service Name**

Name	[ es ]	Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor EDICOM
------	--------	--

Name	[ en ]	Qualified validation service for qualified electronic signatures and qualified electronic seals by EDICOM
------	--------	---

**Service digital identities****X509SubjectName****X509SKI**

X509 SK I	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">f5On7ZPIbFzYVwO/qd9aELFd72Y=</a>
-----------	---

Service Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
----------------	---

Status Starting Time	2019-02-28T01:00:00Z
----------------------	----------------------

**14.6.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**14.6.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**14.7 - Service (granted): Sellos cualificados de tiempo emitidos por TSA EDICOM**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST">http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</a>
-------------------------	---



**Signature algorithm:** *SHA256withRSA*

**Issuer C:** *ES*

**Issuer O:** *EDICOM*

**Issuer CN:** *CAEDICOM Root*

**Subject C:** *ES*

**Subject L:** *PATERNA*

**Subject O:** *EDICOM CAPITAL SL*

**Subject 2.5.4.97:** *VATES-B96490867*

**Subject SERIAL NUMBER:** *B96490867*

**Subject CN:** *CAEDICOM04*

**Valid from:** *Thu Sep 23 15:50:20 CEST 2021*

**Valid to:** *Sun May 21 12:20:00 CEST 2034*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A028202010090908C72B532B590F98603A451A0DD8EAB0E7F53EF8E4B584279920377229C4E4A4BB C3  
40313B6E4659AE1A1233C449F2DC7527A1DCABD72357A2A648A23C71EB7B0561181D32E634B4D3BC70F2FC21A95363288902C85B676BB0DA4E015688F0982D214F  
92D76061B2D432CC1C095F4E85743B3CFE9B9A82283D154FC467E06471711FB3784D11AC678FCFCFA C42DB8686073504CB7883A7C049BDE275BA46A7B93E13F06  
CB131DA668809941177D76126763A4E58902B746C85999309F2A24CE5983CAE C46E BE C0FD20BD F035C62B B86C3FDB13E67A F97923B7BBDE67F2DECE12D01F68372A  
F0056666E8AF55B1C4CAE1B75736CF464A405242345CA316C7361EBBF12365D41F552D7CE5AACAAD12D1EA C53C6C31F3CF98162482984D45D5E3576E87CD075E  
F8A63D3B46D45BFCA8E09021E9225F5DFD2C4644FB67C582E80BA1CED1C21B7EC96C1B1EDAE2905A31A459218368B41A0A3B1C1BC530ECA D3C3E03FD23372C32  
0116C5541267410DEC5D1F7A0C7B802D2412A79F47A19F7F64218A14311DE11E44EF58596AE E72B1615BB D677C8B960B2EA95B3D39E5588F15CA39E40A84A92853CF  
37E38E D4967B54D600EF3F475A5DCT417599E B784C6D19F5954A5813D27318AA60A38C57D0A1406EE7A02D7A831768866EE14B0CB92F26644E963C193C91D2114  
FC6023BE6F4475EF7B2A30BC02727271582E231F0203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *14:CD:2A:59:78:63:AB:61:19:E8:B8:3D:A1:E0:5A:C0:75:E7:F9:CB*

**Authority Info Access**  
*http://acedicom.edicomgroup.com/certs/caedicomroot.cer*  
*http://ocsp.acedicom.edicomgroup.com/caedicomroot*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.30051.2.3.1.1*  
*CPS text: [Certification Practice Statement]*  
*CPS pointer: http://acedicom.edicomgroup.com*

**Extended Key Usage** *id\_kp\_serverAuth*

**CRL Distribution Points** *http://acedicom.edicomgroup.com/caedicomroot.crl*

**Subject Key Identifier** *06:CE:5F:AA:B1:96:26:CD:B5:3F:AD:8E:61:9A:F5:47:21:A7:F9:05*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *B2:11:C4:8C:2B:D4:50:66:DD:DC:3C:62:65:8B:13:5D:85:FE:13:05:89:6F:E3:2F:AA:2B:E7:0B:A4:AA:07:73*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *PATERNA*

**Subject O:** *EDICOM CAPITAL SL*

**Subject 2.5.4.97:** *VATES-B96490867*

**Subject SERIAL NUMBER:** *B96490867*

**Subject CN:** *CAEDICOM04*

**X509SKI**

**X509 SK I** *Bs5fqrGWJs21P62OYZr1RyGn+QU=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-01-11T02:00:00Z*

**14.8.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**14.8.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**14.9 - Service (granted): Servicio cualificado de conservación de sellos electrónicos cualificados 2022****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/PSES/Q*

**Service type description** *[en] A preservation service for qualified electronic signatures.*

*[es] Un servicio de la preservación de las firmas electrónicas reconocidas.*

**Service Name**

**Name** [ es ] *Servicio cualificado de conservación de sellos electrónicos cualificados 2022*

**Name** [ en ] *Preservation of qualified electronic seals 2022*

### Service digital identities

#### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [ en ] *undefined.*

[ es ] *undefined.*

**Status Starting Time** *2022-05-31T00:00:00Z*

#### Scheme Service Definition URI

**URI** [ en ] *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** [ es ] *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

#### 14.9.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>*

#### 14.10 - Service (granted): Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados emitido por CAEDICOM04

#### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

**Service type description** [ en ] *undefined.*

[ es ] *undefined.*

#### Service Name

**Name** [ es ] *Servicio cualificado de validación de firmas electrónicas cualificadas y sellos electrónicos cualificados emitido por CAEDICOM04*

**Name** [ en ] *Qualified validation service for qualified electronic signatures and qualified electronic seals by CAEDICOM04*

### Service digital identities

#### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [ en ] *undefined.*

[ es ] *undefined.*

**Status Starting Time** *2022-06-29T00:00:00Z*

**14.10.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**14.10.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**14.11 - Service (granted): Servicio cualificado de entrega electrónica certificada EDICOM (2022)****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description [ en ] *An electronic delivery service providing qualified electronic deliveries.*  
 [ es ] *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

**Service Name**

Name [ es ] *Servicio cualificado de entrega electrónica certificada EDICOM (2022)*

Name [ en ] *Qualified electronic registered delivery service EDICOM (2022)*

**Service digital identities****Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [ en ] *undefined.*  
 [ es ] *undefined.*

**Status Starting Time**

*2022-10-20T00:00:00Z*



## 15 - TSP: Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

### TSP Name

<b>Name</b>	[ en ]	<i>Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)</i>
<b>Name</b>	[ es ]	<i>Autoridad de Gestión de la PKI del Ministerio de Defensa (AGPMD) y Director del CESTIC. Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)</i>

### TSP Trade Name

<b>Name</b>	[ en ]	<i>Ministerio de Defensa de España</i>
<b>Name</b>	[ es ]	<i>Ministerio de Defensa de España</i>
<b>Name</b>	[ en ]	<i>MDEF</i>
<b>Name</b>	[ es ]	<i>MDEF</i>
<b>Name</b>	[ en ]	<i>VATES-S28002311</i>
<b>Name</b>	[ en ]	<i>MINISTERIO DE DEFENSA</i>
<b>Name</b>	[ es ]	<i>MINISTERIO DE DEFENSA</i>

### PostalAddress

<b>Street Address</b>	[ en ]	<i>C/ Arturo Soria, 289</i>
<b>Locality</b>	[ en ]	<i>Madrid</i>
<b>State Or Province</b>	[ en ]	<i>Madrid</i>
<b>Postal Code</b>	[ en ]	<i>28071</i>
<b>Country Name</b>	[ en ]	<i>ES</i>

### PostalAddress

<b>Street Address</b>	[ es ]	<i>C/ Arturo Soria, 289</i>
<b>Locality</b>	[ es ]	<i>Madrid</i>
<b>State Or Province</b>	[ es ]	<i>Madrid</i>
<b>Postal Code</b>	[ es ]	<i>28071</i>



**Issuer CN:** *MINISDEF-EC-RAIZ*

**Issuer OU:** *PKI*

**Issuer O:** *MDEF*

**Issuer C:** *ES*

**Subject CN:** *MINISDEF-EC-WPG*

**Subject OU:** *PKI*

**Subject O:** *MDEF*

**Subject C:** *ES*

**Valid from:** *Wed Sep 15 10:27:21 CEST 2010*

**Valid to:** *Wed Sep 15 10:27:21 CEST 2021*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C9565B53DB7007EC21868B08EC44CE246B418C4F4BF3C0F71D5F668C896FCECD87889  
39138RC7827D294F0C73C8F5A27FC8D361843C77D99CD27D01E2D3F8A3B4E024E815F85A1966FA7FB81C90B3AD04FFDF460DD15A253C4C206839507858535E0  
AB3427AC6C9571172A7E068B82E874AF2459C299C76E5F5B3D8FF20D1AC41A812DE9231BF4540749BD43F30C4757E038821469D7204CF8513AF25382B5A2A66391  
DBFEC6D2C3BC9478FD46F2AC2AA2737BC2C894A25B5A47C88D9A71465AD41571E69619A9CAD855FE2EC90BFA1FA12A8B275FA349F944C4C7082CD6769FF9351  
2E768FA2B83CBF9DBCE57DBCF71F272C8F5F6BCF1F366015CBB0203010001

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*

**Authority Key Identifier** *8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*

**Certificate Policies**  
*Policy OID: 2.16.724.1.1.1.1.1*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*  
*Policy OID: 2.16.724.1.1.1.1.2*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*  
*Policy OID: 2.16.724.1.1.1.1.3*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*  
*Policy OID: 2.16.724.1.1.1.1.4*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*

**Subject Alternative Name** *CN=Entidad de Certificacion Subordinada WPG, OU=Ministerio de Defensa de Espaa, OU=PKI, O=MDEF, C=ES*

**CRL Distribution Points**  
*ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*  
*ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*  
*<http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl>*

**Key Usage:** *keyCertSign - cRLSign*





**Subject CN:** *MINISDEF-EC-WPG*

**Subject OU:** *PKI*

**Subject O:** *MDEF*

**Subject C:** *ES*

**Valid from:** *Wed Sep 20 12:17:52 CEST 2006*

**Valid to:** *Thu Sep 20 12:17:52 CEST 2012*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100C9565B53DB7007EC21868B08EC44CE246B418C4F4BF3C0F71D5F668C896FCECD87889  
391368C7827D294F0C73C8F5A274C0D361843C77D99CD27D01E2D3F8A3B4E024E815F85A1966FA77FB8A1C90B3A0E4FFDF4460DD15A253C4C2068395078585A55ED  
AD3427AC6C9571172A7E068BB2E874AF2459C299C76EF5B3D8FF20D1AC41A812DE9231BF4540749BD43F30C4787E058821469D7204CF8313AF25382B5A2A66391  
DBFEC6D2C3BC9478FD46F2AC2AA2737BC2C894A25B5A47C88D9A71465AD41571E69619A9CAD855FE2EC90BFA1FA12A8B275FA349F944C4C7082CD6769FF9351  
2E768FFA2B83CBF9DBCE57DBCF71F272C8F5F6BCF1F366015CBB0203010001

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *AB:E3:B9:21:80:5B:FA:76:0F:C7:46:DB:B0:9B:88:0B:5A:B1:CA:B2*

**Authority Key Identifier** *8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D*

**Certificate Policies**  
*Policy OID: 2.16.724.1.1.1.1.2*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*  
*Policy OID: 2.16.724.1.1.1.1.3*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*  
*Policy OID: 2.16.724.1.1.1.1.4*  
*CPS pointer: <http://pki.mdef.es/cps/cps.htm>*

**CRL Distribution Points**  
*ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*  
*ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *49:D2:25:4C:1C:9F:02:F1:E6:B5:CC:DE:9C:2E:B7:79:CD:0D:A3:D9:93:90:8F:6D:8D:43:7B:57:C9:A2:D4:A7*

## X509SubjectName

**Subject CN:** *MINISDEF-EC-WPG*

**Subject OU:** *PKI*

**Subject O:** *MDEF*

**Subject C:** *ES*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2017-07-01T22:00:00Z

### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 15.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:2.16.724.1.1.1.1.2.14

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:2.16.724.1.1.1.1.3.14

### 15.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 15.1.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

### Service Name

**Name** [en] Qualified Certificates issued by Ministerio de Defensa de España

**Name** [es] Certificados reconocidos emitidos por CA MINISDEF-EC-WPG

### Service digital identities

#### X509SubjectName

**Subject CN:** *MINISDEF-EC-WPG*

**Subject OU:** *PKI*

**Subject O:** *MDEF*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *q+O5IYBb+nYPx0bbsJuIC1qxyrI=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 15.1.3.1 - Extension (critical): Qualifiers [NotQualified]

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

#### **Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:2.16.724.1.1.1.1.2.14*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:2.16.724.1.1.1.1.3.14*

#### 15.1.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 15.1.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by Ministerio de Defensa de España*

**Name** *[ es ]* *Certificados reconocidos emitidos por CA MINISDEF-EC-WPG*



**Service digital identities****X509SubjectName**Subject CN: *MINISDEF-EC-WPG*Subject OU: *PKI*Subject O: *MDEF*Subject C: *ES***X509SKI**X509 SK I *q+O5IYBb+nYPx0bbsJulC1qxyrI=*Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*Status Starting Time *2009-04-30T00:00:00Z***15.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA/ CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**Identifier *[ OIDsURN ]* *urn:oid:2.16.724.1.1.1.1.2.14***Policy Identifier:**Identifier *[ OIDsURN ]* *urn:oid:2.16.724.1.1.1.1.3.14***15.2 - Service (granted): Qualified Certificates issued by Ministerio de Defensa de España 2016**Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	[es]	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

**Service Name**



**Public Key:**

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:9A:8F:DA:ES:27:E9:F6:FF:BB:62:AD:D5:AA:9D:66:C5:21:EE:36:2E:B9:3B:AE:04:0B:49:1D:36:40:69:88:8C:4E:77:62:98:84:3F:72:64:97:FD:E2:4D:AF:11:49:58:03:5E:EA:A9:C2:2A:1A:ED:F8:85:25:26:9F:D2:AE:9D:55:D6:09:4D:B3:16:71:57:1B:4C:02:B9:F0:85:F8:D3:00:D6:74:DE:48:AF:C9:CF:DD:47:30:8F:7D:91:F3:48:5F:C1:55:F4:F6:EC:2B:F9:73:41:72:10:FB:7E:9E:C7:AB:D5:0F:E2:CB:39:C2:13:02:DE:54:35:9E:95:FA:58:05:9A:93:9B:3F:CF:89:08:10:E1:82:96:37:CB:6A:82:A7:AA:0A:DB:42:50:17:93:ED:7A:6E:A2:13:CD:35:00:19:6D:F1:24:76:66:11:B7:36:5D:1F:43:FE:D7:44:A4:18:AB:B5:5A:95:42:DD:F8:B3:26:80:20:44:C2:21:A7:2D:C6:DE:7E:1C:34:1D:C3:77:97:BF:DF:DC:31:C8:FD:D3:A9:5B:0E:6E:42:29:FF:0E:DC:CA:38:48:16:56:2C:FE:3A:2F:96:0A:F3:09:6C:3F:0E:AF:C5:8A:50:15:23:46:29:87:15:39:AC:5C:99:ED:4D:35:18:A2:42:4C:D3:BF:F2:84:B3:BD:12:94:DF:8D:08:38:58:05:C2:8A:43:05:08:4B:85:98:C8:3E:4D:5D:19:53:2C:7F:10:2A:A4:CD:C6:85:93:B3:D7:ED:3D:E9:21:95:F9:A6:8C:D8:1E:22:87:E7:6B:18:55:0F:BE:BC:32:7A:A6:0F:17:F8:2B:04:D4:FA:D3:24:D9:1C:0C:22:A4:E0:93:EB:6F:E3:27:4A:06:4A:71:C2:47:FA:FI:0C:91:C5:1A:69:CF:2F:3B:80:D9:FE:91:02:1F:61:56:5C:9F:3E:BC:90:D0:5B:6A:EB:6D:48:4C:5C:20:E8:6E:CC:4A:0B:9F:B1:59:8A:EA:30:0E:30:E6:F1:2E:32:A2:99:41:16:06:76:6E:F2:D0:2D:8B:CS:2D:EE:67:C5:F4:D0:B3:98:11:D6:02:35:0F:29:2A:B6:70:5C:95:09:7E:26:1D:55:6:2:93:EC:93:C8:39:AF:F0:28:7C:EF:76:A8:EB:19:07:D8:FA:16:72:9C:ED:DB:08:F6:D4:A7:01:37:B1:BE:6E:04:A5:5D:99:DE:B5:AA:8F:76:33:E4:60:C9:6D:A1:09:84:46:61:9B:E7:53:EB:6A:1A:BC:14:4C:E2:2D:FF:34:1A:CD:26:16:DA:1D:66:AD:19:39:F1:7B:1D:55:F0:EF:CD:9E:BD:05:41:02:03:01:00:01

**Basic Constraints**

IsCA: true - Path length: 0

**Subject Key Identifier**

91:54:98:88:CF:3E:55:96:34:8E:E5:77:BF:17:74:0F:EE:EA:08:D2

**Authority Key Identifier**

8C:2F:54:32:77:B8:73:00:FC:24:54:F0:DD:A1:07:74:00:28:44:3D

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS pointer: <http://pki.mde.es/dpc/>

CPS text: [Certificado de la Entidad de Certificacion Subordinada WPG2016 del Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).]

**Subject Alternative Name**

mail: [agpmd@oc.mde.es](mailto:agpmd@oc.mde.es)

CN=Entidad de Certificacion Subordinada WPG2016, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES

**CRL Distribution Points**

<http://pki.mde.es/crl/DEFENSA-CRL-EC-RAIZ.crl>

<ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint>

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

81:44:06:33:1B:97:9F:B1:4E:87:D1:CB:38:ED:0E:F2:BB:5B:EE:0A:1E:72:89:37:D6:BD:D5:D4:94:FC:D5:E6

**X509SubjectName****Subject CN:**

DEFENSA-EC-WPG2016

**Subject 2.5.4.97:**

VATES-S2800231I

**Subject OU:**

PKI

**Subject O:**

MINISTERIO DE DEFENSA

**Subject C:**

ES

**X509SKI****X509 SK I**

kVSYiM8+VZY0juV3vxd0D+7qCNI=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2018-10-08T01:00:00Z

**Scheme Service Definition URI**

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**15.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**15.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**15.2.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**15.2.4 - History instance n.1 - Status: withdrawn**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by Ministerio de Defensa de España 2016*

**Name** [ es ] *Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016*

**Service digital identities****X509SubjectName**

**Subject CN:** *DEFENSA-EC-WPG2016*

**Subject 2.5.4.97:** *VATES-S2800231I*

**Subject OU:** *PKI*

**Subject O:** MINISTERIO DE DEFENSA

**Subject C:** ES

**X509SKI**

**X509 SK I** kVSYiM8+VZY0juV3vxd0D+7qCNI=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Status Starting Time** 2017-07-01T22:00:00Z

**15.2.4.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**15.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] Qualified Certificates issued by Ministerio de Defensa de España 2016

**Name** [ es ] Certificados cualificados emitidos por CA DEFENSA-EC-WPG2016

**Service digital identities**

**X509SubjectName**

**Subject CN:** DEFENSA-EC-WPG2016

**Subject 2.5.4.97:** VATES-S2800231I

**Subject OU:** PKI

**Subject O:** MINISTERIO DE DEFENSA

**Subject C:** ES

**X509SKI**

**X509 SK I** kVSYiM8+VZY0juV3vxd0D+7qCNI=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time

2017-05-10T00:00:00Z

**15.2.5.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**16 - TSP: Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.****TSP Name**

**Name** [ en ] *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.*

**Name** [ es ] *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.*

**TSP Trade Name**

**Name** [ en ] *Izenpe, S.A*

**Name** [ es ] *Izenpe, S.A*

**Name** [ en ] *IZENPE S.A. - CIF A-01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8*

**Name** [ es ] *IZENPE S.A. - CIF A-01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8*

**Name** [ en ] *VATES-A01337260*

**Name** [ en ] *IZENPE S.A.*

**PostalAddress**

**Street Address** [ en ] *Avenida del Mediterráneo, 14*

**Locality** [ en ] *Vitoria-Gasteiz*

**State Or Province** [ en ] *Álava*

**Postal Code** [ en ] *1010*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Avenida del Mediterráneo, 14*

**Locality** [ es ] *Vitoria-Gasteiz*

**State Or Province** [ es ] *Álava*

**Postal Code** [ es ] *1010*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://www.izenpe.com*





**Issuer O:** IZENPE S.A.

**Issuer C:** ES

**Subject CN:** Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)

**Subject OU:** NZZ Ziurtagiri publikoa - Certificado publico SCI

**Subject O:** IZENPE S.A.

**Subject C:** ES

**Valid from:** Tue Feb 24 09:05:46 CET 2009

**Valid to:** Sun Dec 13 00:00:00 CET 2037

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100DFE77E8981F39BE2C283A32E94FCB210625942562614681B31DD2CFF8ED192BD6C7AD843D49C5CB225500FD39C8776B4A4F03D965F82DA70D43115AA7E64D9575723910C4E4A5A8363FDD6420E83DR23C68DE0AD9C9528D60194A9EE892E01EABCF4DE9D9DEDC8E8DC80987E0610E3748533F34D4116DE96E267EBCAE4213C6C8F7A7AD253EC1700982C383E4E8A8C16527554CEB433B5ACEF3E26756C7678D6F6B6AE94A2B9B6350DB7ABFD9D69ED0A0FC2592660F015E17405B3C7F7AD67CB2E393C2729B39304D388B869560EBEC9B2AB50C558839019590884677DF7E7F2843334B3E939435B40CDA78B09E812E4FC8BD4AD57363C55FD6F452A5E148D257CA838F82CB4677AB305DC9EC302B9E9E771752405C2CF995C07855F5B33625F5B5C43A8452E1440414CD78C663BD808C515F29EB7839CF4AS31E93425662450D1EA2A27284B54D35BEA01F66774BB8A03EC33694246B2CD27D3C22DE01EC4D361158E5FE3E3FF65968A05BBFA C62248E4DB4D1C66AF18DE16C51B122BD8B3FB38AAE11730178F38590E4B499C28CF1BF9D7229C5FF6079FF7F17E3D99AF2DB0F751F32B917B0A8B C379540EAF788E895177B5FCDDF9031983CA80DE9547B9BE3B063AA0BA33F2EF80BA0620846A28EDAFDBE0BE078F682DEC1B567264AD084816D6664BE096F3DC990A02C4D013D86B81538AC6C8CE9E5C32570E8F390203010001

**Subject Alternative Name**  
<http://www.izenpe.com>  
[info@izenpe.com](mailto:info@izenpe.com)  
 STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8

**Basic Constraints**  
 IsCA: true

**Subject Key Identifier**  
 A4:17:1D:4E:65:D7:EF:87:95:2E:7F:8E:B8:75:CB:05:8B:D3:8C:7D

**Authority Key Identifier**  
 1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <http://www.izenpe.com/cps>

**Authority Info Access**  
<http://ocsp.izenpe.com:8094>

**CRL Distribution Points**  
<http://crl.izenpe.com/cgi-bin/arl2>

**Key Usage:**  
 keyCertSign - cRLSign

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 26:26:B1:95:63:BC:78:D9:B1:44:2B:93:CE:98:D1:4A:1E:4B:74:26:4A:CC:90:22:2F:1F:3C:23:85:C2:73:37

**Certificate fields details**

**Version:** 3

**Serial Number:** 44226866073358392262219520495746478787



**CRL Distribution Points** *http://crl.izenpe.com/cgi-bin/arl2*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75*

**X509SubjectName**

**Subject CN:** *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)*

**Subject OU:** *NZZ Ziurtagiri publikoa - Certificado publico SCI*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time***2016-12-21T01:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**16.1.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.7*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.8*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.9*

**16.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**16.1.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**16.1.4 - History instance n.1 - Status: granted**

Service Type Identifier	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
-------------------------	---

**Service Name**

Name	[ en ]	Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)
------	--------	--

Name	[ es ]	Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)
------	--------	--

**Service digital identities****X509SubjectName**

Subject CN:	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)
-------------	---

Subject OU:	NZZ Ziurtagiri publikoa - Certificado publico SCI
-------------	---

Subject O:	IZENPE S.A.
------------	-------------

Subject C:	ES
------------	----

**X509SKI**

X509 SK I	pBcdTmXX74eVLn+OuHXLBYvTjH0=
-----------	------------------------------

Service Status	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
----------------	---

Status Starting Time	2016-06-30T22:00:00Z
----------------------	----------------------

**16.1.4.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[ en ]	undefined.
----------------------------	--------	------------

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.7**Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.8**Policy Identifier:****Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.9**16.1.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**16.1.5 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [en] *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)***Name** [es] *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) (PKI 2007)***Service digital identities****X509SubjectName****Subject CN:** *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)***Subject OU:** *NZZ Ziurtagiri publikoa - Certificado publico SCI***Subject O:** *IZENPE S.A.***Subject C:** *ES***X509SKI****X509 SK I** *pBcdTmXX74eVLn+OuHXLBYvTjH0=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2009-07-17T00:00:00Z

### 16.1.5.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.7

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.8

##### Policy Identifier:

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.9

### 16.2 - Service (granted): Qualified certificates issued by CA EAeko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [ en ] Qualified certificates issued by CA EAeko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

**Name** [ es ] Certificados reconocidos emitidos por CA EAeko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

#### Service digital identities

#### Certificate fields details

**Version:** 3







**Subject Alternative Name** *http://www.izenpe.com*  
*info@izenpe.com*  
*STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8*

**Basic Constraints** *IsCA: true*

**Subject Key Identifier** *C6:AF:96:68:50:BE:6F:A1:E5:14:DC:B9:9D:97:3D:8D:73:E7:7E:9A*

**Authority Key Identifier** *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.izenpe.com/cps*

**Authority Info Access** *http://ocsp.izenpe.com:8094*

**CRL Distribution Points** *http://crl.izenpe.com/cgi-bin/arl2*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8*

**X509SubjectName**

**Subject CN:** *EAEko HAetako langileen CA - CA personal de AAPP vascas (2)*

**Subject OU:** *AZZ Ziurtagiri publikoa - Certificado publico SCA*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2016-06-30T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**16.2.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.4.3

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.4.4

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.4.5

### 16.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 16.2.3 - History instance n.1 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified certificates issued by CA EAeko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

**Name** [es] Certificados reconocidos emitidos por CA EAeko HAetako langileen CA - CA personal de AAPP vascas (2) (PKI 2007)

#### Service digital identities

##### X509SubjectName

**Subject CN:** EAeko HAetako langileen CA - CA personal de AAPP vascas (2)

**Subject OU:** AZZ Ziurtagiri publikoa - Certificado publico SCA

**Subject O:** IZENPE S.A.

**Subject C:** ES

##### X509SKI

X509 SK I

xq+WaFC+b6HIFNy5nZc9jXPnfpo=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2009-07-17T00:00:00Z

**16.2.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne**

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.4.3

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.4.4

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.4.5

**16.3 - Service (withdrawn): Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [ en ] Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

Name [ es ] Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)

**Service digital identities****Certificate fields details**

Version: 3

Serial Number: 12

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIGJTCCBQ2AwIBAgIBDDANBgkqhkiG9w0BAQUFA...
-----END CERTIFICATE-----

Signature algorithm: SHA1withRSA

Issuer E: Info@izenpe.com

Issuer CN: Izenpe.com

Issuer L: Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz

Issuer O: IZENPE S.A. - CIF A-01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8

Issuer C: ES

Subject E: Info@izenpe.com

Subject CN: Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades

Subject OU: NZZ Ziurtagiri publikoa - Certificado publico SCI

Subject L: Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz

Subject O: IZENPE S.A. - CIF A-01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8

Subject C: ES

Valid from: Tue Feb 04 18:46:25 CET 2003

Valid to: Mon Feb 04 00:00:00 CET 2013

Public Key: 30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:3D:82:01:0A:02:82:01:01:00:DB:00:67:D9:BC:0C:26:DA:0A:12:C8:85:25:C4:81:F0:47:BF:3D:83:C0:CA:5A:CB:17:8A:E8:EC:6E:6D:E2:BC:80:5...

Subject Alternative Name http://www.izenpe.com

Basic Constraints IsCA: true

Subject Key Identifier D5:3D:B6:B8:27:6D:84:3A:A8:25:07:4C:D0:D3:4E:EB:36:DB:95:B2

**Authority Key Identifier** *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*

**CRL Distribution Points** *http://www.izenpe.com/cgi-bin/arl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *5C:68:F4:98:B2:38:B3:B2:AD:F8:A7:04:74:CF:24:F6:32:67:58:1B:ED:47:96:9F:B1:8B:5E:1B:4A:AB:80:A9*

**X509SubjectName**

**Subject E:** *Info@izenpe.com*

**Subject CN:** *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

**Subject OU:** *NZZ Ziurtagiri publikoa - Certificado publico SCI*

**Subject L:** *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

**Subject O:** *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2016-06-30T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**16.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.14777.2.8*

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.9

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.7

### 16.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 16.3.3 - History instance n.1 - Status: supervisionceased

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

**Name** [ es ] *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

#### Service digital identities

##### X509SubjectName

**Subject E:** *Info@izenpe.com*

**Subject CN:** *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

**Subject OU:** *NZZ Ziurtagiri publikoa - Certificado publico SCI*

**Subject L:** *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

**Subject O:** *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

**Subject C:** *ES*

##### X509SKI

**X509 SK I** *1T22uCdthDqoJQdM0NNO6zbbIbI=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2009-07-17T00:00:00Z*

**16.3.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.8

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.9

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.7

**16.3.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Certificados reconocidos emitido por CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

**Name** [es] *Qualified certificates issued by CA Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (PKI 2003)*

**Service digital identities****X509SubjectName**

**Subject E:** *Info@izenpe.com*

**Subject CN:** *Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades*

**Subject OU:** *NZZ Ziurtagiri publikoa - Certificado publico SCI*

**Subject L:** *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

**Subject O:** *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

**Subject C:** *ES*

X509SKI

X509 SK I

1T22uCdthDqoJQdM0NNO6zbbIbI=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2005-03-03T00:00:00Z

**16.3.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.8

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.7

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.14777.2.9

**16.4 - Service (withdrawn): Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [ en ] Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)

**Name** [ es ] Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)

**Service digital identities**





**Subject Key Identifier** *A2:94:8F:B3:68:E8:5F:6D:C1:FB:5A:56:9B:2C:14:68:D8:23:27:CA*

**Authority Key Identifier** *EA:56:4F:EC:3C:83:A1:14:88:78:81:B2:2B:05:22:C0:07:41:5B:42*

**CRL Distribution Points** *http://www.izenpe.com/cgi-bin/arl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *0A:07:55:F0:F8:78:EB:9C:D3:13:48:8B:6C:79:91:90:C0:4E:59:27:54:16:30:63:83:02:4D:E7:8A:F8:47:38*

**X509SubjectName**

**Subject E:** *Info@izenpe.com*

**Subject CN:** *EAEko HAetako langileen CA - CA personal de AAPP vascas*

**Subject OU:** *AZZ Ziurtagiri publikoa - Certificado publico SCA*

**Subject L:** *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

**Subject O:** *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time***2016-06-30T22:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**16.4.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.14777.4.3*

**16.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**16.4.3 - History instance n.1 - Status: supervisionceased**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified certificates issued by CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

**Name** [es] *Certificados reconocidos emitidos por CA EAEko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)*

**Service digital identities****X509SubjectName**

**Subject E:** *Info@izenpe.com*

**Subject CN:** *EAEko HAetako langileen CA - CA personal de AAPP vascas*

**Subject OU:** *AZZ Ziurtagiri publikoa - Certificado publico SCA*

**Subject L:** *Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz*

**Subject O:** *IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *opSPs2joX23B+IpWmywUaNgjJ8o=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased>

**Status Starting Time** *2009-07-17T00:00:00Z*

**16.4.3.1 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es]

está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

## Criteria list assert=atLeastOne

### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.4.3

### 16.4.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

### Service Name

**Name** [en] Qualified certificates issued by CA EAeko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)

**Name** [es] Certificados reconocidos emitidos por CA EAeko HAetako langileen CA - CA personal de AAPP vascas (PKI 2003)

### Service digital identities

#### X509SubjectName

**Subject E:** Info@izenpe.com

**Subject CN:** EAeko HAetako langileen CA - CA personal de AAPP vascas

**Subject OU:** AZZ Ziurtagiri publikoa - Certificado publico SCA

**Subject L:** Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz

**Subject O:** IZENPE S.A. - CIF A-01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8

**Subject C:** ES

#### X509SKI

**X509 SK I** opSPs2joX23B+1pWmywUaNgjJ8o=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2005-03-03T00:00:00Z

### 16.4.4.2 - Extension (critical): Qualifiers [QCForLegalPerson]

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.14777.4.3

**16.5 - Service (withdrawn): Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [en] *Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

[es] *Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

**Service digital identities**

**Certificate fields details**

**Version:** 3

**Serial Number:** 56124756630010648903621069610385544548

**X509 Certificate**

```
-----BEGIN CERTIFICATE-----
MIHPTCCBCwAwIBAgIQk8JSCZz0SLc99vH4VZDANBgkqhkiG9w0BAQUFAADA4MQUswCQYDVQQG
EwJ1ZmEUMBIkGAIUECgwLSVpTIBFIFMacQ84EzARBgNVBAMMCK6ZwSwzS5j62wHbcNMTAwMjEs
MFAOMCQwWbcNNFAwMjEsMFAOMCQwWbcZELMAGGAJUEFBAMRVMkTDS8gVBEacMCkubU:SQRSBT
LKEaMTwMAYDVQQLC2aaXVydGFnaXpHBIYmspa29hICQeO2YvdGlnaWVhZG90ZG8gCHVibGijbGF
MEQGAJUEAw9RXYza29gSmF1cm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90
82jzX40yRwYXN0b3cASStuPOYkccZbncNAQEBRQYDQgEJFADCCCAQoGqgEALPkmPwAklp19iq
6K7S8mj2NRyur13oL0cljH0wE9+IL8LqEA90EteybwbZS9L+PIFLXRp5ILRJ1V5yH
SgmK4SWDwXkR2mj+KqG996WJhhfufJazBd0N4UjVwoDX2pZed7goKNAZnbwki9pp
NksvE8SRCE8E8H4uZf6ec97260fMvYgBL7c2yLzF7kxmbS84fz8Nbv7PM4PTB8BU
G3m2LwTKZ2qTMhJgNPWMFP3TfscOBRwXDR9QadryVofhoPX+UvPageMDTbRAMphU6G65HR
HhKmpo8Nj1MSVw4+43IMCawEAaAOCAdkqgHVMHhBgnVHREg8b8ghvGFWh0HAgLys3dScu
aXnlbHlcmWdYEFw5m80f8pmVscGlUy29qJGRMGOMIeyR0YDYQKQJDSWAVOLUJy5BLkU
IENJRiBMDzAmcyNjAUIk1cmMvMm0b5jYpSYHYXN0ZWI6FQMDU1HEY2MBTDFDMEGAJUE
C0wQXZYSBkZWgTWVkaXBlcm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90Zm90
dGYPEA4PgvVIRMBAREBFDQAJHMAKGAJUEFBwQEAwBBAdBpVH04FqVUsaevYzVopq
fPwJddqswAduagHwYDVR0BBGwFAUJHRdDjpvJxufkcsbHmvV0bAUwOgYDVR0BDmMTAv
BGRVSAAMCcwQYJKwYBBQUHAQEFVGVW08dHAELy93dScuXpImBILmN659chAwNwYKwYBBQUH
AQEKezAmCcc3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3
KJAoocagJYiaHR0cDovL2Nyb3c3cmVuaGluY291L2NnaSIaW4vYXU5MjA5MjA5MjA5MjA5MjA5
AAOCAGEAxiOgT25glc7YzhaY1NO8szDMK2aD0e2ASNIIT3ARF4CS7ooF2Lhh0Iq9P0ZD
KlH+EF8wRk7ba4YVPI066WGO8cmru+WlgTzVYoe3naR4e4h7yG25vY04Vxka0by
Tj3glDx3AaDWHYogE7Q7W3f36qN+eyEC=MWM08ZRZJ78pdNhh1Umu14vU0q25VpsN7Pu
PrZngWmb9aIlyYkqgQcIcfaDz0BingXZbNKZKZKZKZKZKZKZKZKZKZKZKZKZKZKZKZKZKZK
PZvYmuSIHMGtP3Sf9psSkoforaIHLnbl1B0WTimzH0qU7z6sGDL3v8vA Wm1L6G89zK
IwkyGm9bmc2KdapV4Fcy1gf8G5EhbVUacopia0geoBXNAdbmLmC8j0NCcaZK743n3ZMmgNK7PI
HhDqLJZHZRCcC6b8dp7J6YSL1pHd68KOpw5Cag0mclLzmsKjY35PSEY1XVR9BciglVVR
9m8sG0WakfswWcH1v+vuNlJg8hbkKQZawNSYVAgQDfHB8n65G6G65784m+czu0R4kxw
BpBCmdMcaFIWA1XR8St6V8UkG1rp7j0e49smXCRmIavCzvINvWlzGkyf8PUpH5CQe4zx
54:by0=
-----END CERTIFICATE-----
```

**Signature algorithm:** SHA1withRSA

**Issuer CN:** *Izenpe.com*

**Issuer O:** *IZENPE S.A.*

**Issuer C:** *ES*

**Subject CN:** *Eusko Jaurilaritzako langileen CA - CA personal Gobierno Vasco*

**Subject OU:** *Ziurtagiri publikoa - Certificado publico*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**Valid from:** *Thu Feb 11 11:43:40 CET 2010*

**Valid to:** *Tue Feb 11 11:43:40 CET 2020*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B3E498F5AE294A53F75A8E8A22BB4929A3DA835162EAF237B682CE7258DD1D0C04F7E20BF0B8A8403DD048AD7B26706C5665E82F4BF8F2052D7951A79D4B449D554AFC87E62826478FD25AD0C9C17C51DB79A3F8AA86B7D9D6BC885B7E1E483DAC1BB4378523570A085FBDA9D9E0FEE8E0A0A3406659DBC248EDCA8A633632AFD044A0F11DAS90213CC8E1BDA8C2D648E9E8A08BBF3AA5C99762004BEDEDB2894CC54E3931981DA2F38173361BF3FA30FE07C0541B79B62F04CA66DDAA4C86580D3D6305169DD3B1B70E051C1F5C3F50C9A76B798A058683D7F94BCF6A0B5C3034DBB51326A6152B1BAE4746C1D71E49A36E8B0D8E3D4CE55C38F88DF530203010001

**Subject Alternative Name**  
*http://www.izenpe.com*  
*info@izenpe.com*  
*STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc. Vitoria-Gasteiz TI055 F62 S8*

**Basic Constraints**  
*IsCA: true*

**Subject Key Identifier**  
*F1:A3:1E:55:8C:D5:A2:9B:5E:7C:5A:56:C4:87:6A:E7:00:1D:B9:A8*

**Authority Key Identifier**  
*1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.izenpe.com/cps*

**Authority Info Access**  
*http://ocsp.izenpe.com:8094*

**CRL Distribution Points**  
*http://crl.izenpe.com/cgi-bin/arl2*

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*0B:C3:6A:9B:6E:42:DD:BF:07:4C:FE:38:83:4F:20:0C:D4:4C:1D:28:E2:35:29:CF:E6:29:BC:48:4B:98:98:B9*

**X509SubjectName**

**Subject CN:** *Eusko Jaurilaritzako langileen CA - CA personal Gobierno Vasco*

**Subject OU:** *Ziurtagiri publikoa - Certificado publico*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2018-03-15T01:00:00Z*

#### **Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

#### **16.5.1 - Extension (critical): additionalServiceInformation**

##### **AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### **16.5.2 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** *[en] Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

**Name** *[es] Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

#### **Service digital identities**

##### **X509SubjectName**

**Subject CN:** *Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco*

**Subject OU:** *Ziurtagiri publikoa - Certificado publico*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I***8aMeVYzVoptefFpWxIdq5wAduag=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2016-06-30T22:00:00Z***16.5.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***16.5.3 - History instance n.2 - Status: undersupervision****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name***[ en ]**Qualified certificates issued by CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco***Name***[ es ]**Certificados reconocidos emitido por CA Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco***Service digital identities****X509SubjectName****Subject CN:***Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco***Subject OU:***Ziurtagiri publikoa - Certificado publico***Subject O:***IZENPE S.A.***Subject C:***ES***X509SKI****X509 SK I***8aMeVYzVoptefFpWxIdq5wAduag=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision***Status Starting Time***2010-07-30T00:00:00Z***16.6 - Service (withdrawn): Qualified timestamps issued by tsa.izenpe.com****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*





**Issuer Alternative Name** *info@izenpe.com*

**Extended Key Usage** *id\_kp\_timeStamping*

**Subject Key Identifier** *E7:C7:69:33:A9:2F:D0:61:32:7E:77:23:3D:06:9F:0C:85:81:E1:76*

**Authority Key Identifier** *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.14777.3.3*  
*CPS pointer: <http://www.izenpe.com/cps>*  
*CPS text: [Bermeen mugak ezagutzeko [www.izenpe.com](http://www.izenpe.com) Ziurtagirian konfiantza izan aurretik kontratua irakurri.Limitaciones de garantias en [www.izenpe.com](http://www.izenpe.com) Consulte el contrato antes de confiar en el certificado]*

**CRL Distribution Points** *<http://crl.izenpe.com/cgi-bin/arl2>*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *CD:77:0A:3B:A5:00:5B:AC:3F:6E:F2:9E:7F:A4:C7:BE:A1:EF:41:BE:52:12:53:56:DA:0D:D1:8F:04:5C:92:19*

**X509SubjectName**

**Subject CN:** *tsa.izenpe.com*

**Subject 2.5.4.97:** *VATES-A01337260*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *58dpM6kv0GEyfnCjPQafDIWB4XY=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-10-10T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**16.6.1 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

**Name** *[ en ]* *Qualified timestamps issued by tsa.izenpe.com*

**Name** *[ es ]* *Sellos de tiempo cualificados emitidos por tsa.izenpe.com*

**Service digital identities****X509SubjectName**

**Subject CN:** *tsa.izenpe.com*

**Subject 2.5.4.97:** *VATES-A01337260*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *58dpM6kv0GEyfcjPQafDIWB4XY=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2017-07-21T00:00:00Z*

**16.7 - Service (withdrawn): Qualified certificates issued by CA de certificados SSL EV**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** *[ en ]* *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[ es ]* *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by CA de certificados SSL EV*

**Name** *[ es ]* *Certificados cualificados emitidos por CA de certificados SSL EV*

**Service digital identities****Certificate fields details**

**Version:** *3*

Serial Number:

145477172158191020923658859389206702465

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHfCCBQCcAwIBAgIQ6XHW3u2qZMvqgh46SpgTALBkqkhiG9w0BAQwODELMAKGA1UEBMBM...

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

Izenpe.com

Issuer O:

IZENPE S.A.

Issuer C:

ES

Subject CN:

CA de Certificados SSL EV

Subject OU:

BZ Ziaritagiri publikoa - Certificado publico EV

Subject O:

IZENPE S.A.

Subject C:

ES

Valid from:

Wed Oct 20 10:28:56 CEST 2010

Valid to:

Tue Oct 20 10:28:56 CEST 2020

Public Key:

30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:EB:B2:9D:4D:4A:FF:14:9F:D5:68:16:8B:D4:12:60:9A:6E:AE:F2:86:A8:12:59:34:7A:C7:73:7A:87:FB:D2:CB:0A:38:F7:57:CA:FA:DD:3D:63:DI:41:D2:3B:3F:8F:C4:BF:6B:3B:7E:4C:A7:7B:48:ES:34:9A:5B:D3:0D:35:76:85:22:01:A7:A6:A1:D9:54:A1:52:E6:07:CB:D3:81:6C:C0:C7:B6:9E:4D:18:11:CC:C7:E7:62:EI:35:7F:76:C1:F8:C7:D1:6D:C0:F7:45:75:DI:43:3E:DB:95:5D:A5:29:42:94:15:86:EB:18:C2:09:27:EB:35:31:64:11:EB:28:18:0D:A2:8C:C8:0B:85:6D:F8:C0:1C:2E:83:71:22:43:2E:2A:32:95:91:07:D9:6A:05:FE:CD:22:41:82:105:57:C1:58:C9:A:C:E1:8F:89:D9:EB:1B:9D:B7:22:EE:10:37:D2:AF:74:D0:8E:01:4B:4E:37:81:75:53:57:92:E8:27:46:7A:ED:D4:AD:0B:A2:6C:26:13:3D:69:3B:7A:F7:B0:93:9E:D8:AA:38:A4:8A:0D:83:61:75:A3:D7:D9:3C:59:35:EE:F4:0C:4:08:B3:E9:66:05:E0:BF:B1:F7:47:20:C8:F9:8B:7E:0E:AB:0F:15:51:FB:EK:70:F9:DB:DC:14:F7:34:36:CD:8F:9C:93:2E:3D:78:61:BF:1C:01:A0:85:71:5E:AC:5:28:10:9D:0C:E7:83:D7:B6:70:94:0C:54:88:02:1E:BB:4F:48:80:7E:4B:15:77:2A:2E:81:48:AD:3E:17:83:7E:3E:A6:3E:5A:16:DF:8:9C:1E:92:4C:71:1A:DF:3D:F6:35:2B:8B:95:DB:AE:A1:92:DF:9F:80:48:4D:6D:4F:0D:85:10:8E:9:09:51:A:25:40:53:1B:2C:C1:C1:28:1C:9C:92:3D:6D:4C:50:6D:EB:26:B5:74:61:FE:EF:E9:0E:24:A2:2C:33:9D:29:21:66:F3:66:EF:35:E0:8D:98:A1:58:04:B4:D2:5C:BC:29:96:75:8F:00:BC:85:0B:0C:EE:88:A0:6B:34:82:82:1D:2D:09:A9:85:8F:D1:FF:B5:4A:15:D6:BF:4:BC:10:E7:63:58:EB:B3:7E:21:07:4F:4D:89:A9:37:16:2A:70:93:0C:E2:D0:BF:3A:73:83:5A:FF:85:49:D0:45:A3:C8:1B:CC:92:15:DE:97:45:38:A0:9E:60:45:F5:42:8A:17:42:71:A0:5A:8C:5B:73:37:88:26:8F:B6:19:E9:F2:DD:C3:A5:95:D8:96:45:AF:98:50:0C:3C:FF:72:D1:D8:52:3F:65:C5:02:03:01:00:01

Subject Alternative Name

http://www.izenpe.com

info@izenpe.com

STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz, O=IZENPE S.A. - CIF A01337260-RMerc. Vitoria-Gasteiz T1055 F62 S8

Basic Constraints

IsCA: true

Subject Key Identifier

A6:CE:69:69:2E:A6:21:35:3B:3A:CF:0A:F1:2E:3F:15:AC:19:90:27

Authority Key Identifier

1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05

Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: http://www.izenpe.com/cps

**Authority Info Access** <http://ocsp.izenpe.com>

**CRL Distribution Points** <http://crl.izenpe.com/cgi-bin/arl2>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *B0:8C:19:6A:2E:D1:E8:4F:98:92:DB:1B:61:21:9C:EB:64:28:82:47:8F:39:B0:87:19:60:3D:07:35:FA:03:D1*

**X509SubjectName**

**Subject CN:** *CA de Certificados SSL EV*

**Subject OU:** *BZ Ziurtagiri publikoa - Certificado publico EV*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *ps5paS6mITU7Os8K8S4/FawZkCc=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-10-10T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**16.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**16.7.2 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[ en ]	Qualified certificates issued by CA de certificados SSL EV
<b>Name</b>	[ es ]	Certificados cualificados emitidos por CA de certificados SSL EV

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	CA de Certificados SSL EV
<b>Subject OU:</b>	BZ Ziurtagiri publikoa - Certificado publico EV
<b>Subject O:</b>	IZENPE S.A.
<b>Subject C:</b>	ES

**X509SKI**

<b>X509 SK I</b>	ps5paS6mITU7Os8K8S4/FawZkCc=
------------------	------------------------------

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time**

2018-03-15T01:00:00Z

**16.7.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
------------	--------	---

**16.8 - Service (granted): Qualified certificates issued by CA de certificados SSL EV (new)****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[ en ]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[ es ]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

<b>Name</b>	[ en ]	Qualified certificates issued by CA de certificados SSL EV (new)
<b>Name</b>	[ es ]	Certificados cualificados emitidos por CA de certificados SSL EV (nueva)

**Service digital identities**



**Authority Key Identifier** *1D:1C:65:0E:A8:F2:25:7B:B4:91:CF:E4:B1:B1:E6:BD:55:74:6C:05*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.izenpe.com/cps*

**Authority Info Access** *http://ocsp.izenpe.com*

**CRL Distribution Points** *http://crl.izenpe.com/cgi-bin/arl2*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37*

**X509SubjectName**

**Subject CN:** *CA de Certificados SSL EV*

**Subject OU:** *BZ Ziurtagiri publikoa - Certificado publico EV*

**Subject O:** *IZENPE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *xu3+d/tRVk38q9XjsQwTo79U45s=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2019-07-15T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**16.8.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*





**Valid from:** Wed Sep 23 13:29:29 CEST 2020

**Valid to:** Sat Sep 23 12:57:18 CEST 2045

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100AE931DC68300B5D4FEFEFEFE96AF3A9E497A1FB01DA27507A0BA8F93A79D1C15772  
392981EAT85900B8F4758877F66A49E46956B0E96746BC196546A9ED4E4F851E2A10E41F1845DB38696BD8DE25A291591451B7E5CBECF4C56C970F614D9F242B98E2  
0FC5FDBB36CAFEF65DC12D1DE5A5706325BC74EF0D2517E320E334C4229935B954596051E9C24C7A8DA5099FA6F2D500840CAF5BC3954727689EC523EFC80F  
CFEAFCE83723AB06C77A1B8BD00DD20A8D20C3BEEA78A1934973EC422622F27835910E1150F67A333F0D265BBE8C939C7E44B1D158B7F1DB9AA162C24798570C4  
96C26E908C50DFA18310254E846AC28ABD2F1D1DD77242228250378055879B0E1DE878F2CDB89194050D3D9F04C191E4D834AA CA BE F7BBDA73CA075E489D19123  
22D568991B69D5DA1DF8477087D0E873245D4FCBF1251FF44AC2E1299281FB3E629425B7635DE073563D0454A65A83AFB72AD70CE7CA7E504496BCA2F1C264F3F2  
38C074EF46DC1609E7BAAD1545E818CB469842F167F23B9361DDB61E525900492A9DF58F30FE9B09CC1413163FA6563B7A262328238C78659D2A0CC130E3D65557912  
D2273EFCDBF9688677416F106601255C9E4E1E98918A2012B1476ED212BA702BF1D8B9090B23D761E9A78678753B41D8EB53E703EA466D397F66A804D68788C8  
B5AC5D3BC8F446EB0513B4147596B4732F07750203010001

**Authority Key Identifier** A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97

**Subject Key Identifier** D3:E1:D0:00:10:E4:37:DB:20:C0:6E:CD:92:F5:9C:7F:0A:6B:2E:40

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.izenpe.eu/cps>

**Authority Info Access** [http://www.izenpe.eu/contenidos/informacion/cas\\_izenpe/es\\_cas/adjuntos/IZENPE\\_ROOT\\_QC.crt](http://www.izenpe.eu/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt)

**Basic Constraints** IsCA: true - Path length: 0

**CRL Distribution Points** <http://crl.izenpe.eu/cgi-bin/izrootqc>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 1A:48:85:AC:77:F5:55:9B:29:BF:AE:13:C4:86:FF:09:31:21:FA:C2:68:A8:EC:BB:2B:AB:30:3F:5D:A9:42:F9

**X509SubjectName**

**Subject CN:** SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA

**Subject 2.5.4.97:** VATES-A01337260

**Subject O:** IZENPE S.A.

**Subject C:** ES

**X509SKI**

**X509 SK I** 0+HQABDkN9sgwG7NkvWcwfprLkA=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2021-04-21T00:00:00Z

**Scheme Service Definition URI**

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 16.9.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 16.9.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 16.10 - Service (granted): Qualified certificates issued by SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA

#### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

Name [en] *Qualified certificates issued by SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

Name [es] *Certificados cualificados de firma y sello expedidos por SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA*

#### Service digital identities

#### Certificate fields details

Version: 3

Serial Number: 45119263425281848757751757719133867194

## X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIGADCCBICgAwIBAgIQHfGn69EYdQlfaZfP9XMuJANBgkqhkiG9w0BAQsFADMOswCOYDVQ0G
EwJFZU1UMGIGAUUECgwLSPVpTBFIFMuQs4GjAYBgNVBAMMEVPTIQ0eQeLUUMgSVpFTBIFMBAX
DTWMDkyMzEsMj01MDQyMzEwNTc0Zm9yYyZAZG9uYVBAIjA1YTMROGEGYDVQ0GDAJ
WAVOUUElglSBURVJSSVRBUjBSyBFVEEgRURUSOUAVTOS1DSVVEOUeRBTkIBFkgRU1OUkVTOUCCAIw
DOYKozlveN4OEBBQA0DggpADCCAgQgZGIBALGEPXISGD3SWSP4FL3KzGzAmkSipk6wCcaZw
YNoLcw9WABIP47hearXHns667MUUGs8dWUwZDK1MI-7OSH6GimHCWys4t4s4t4Yywas4
YXISogMSEGRzZp97ydrKk+bCOym+skglR6GD07obOHN+L2PSKH7H92mWThPpyLLpMTZ
VesHfKcWewMNAkEgeJadC2gpmajYnNpYZZbgWaggyf10uqkMUGL2H9C7dIXRjgkRfHJLzwB
h6DduwY9Q9xwO39kAOlhy9yZfDWGfGceEwOpemYp9pGyVeuHfZGR3CCQK8wJZesWg3
G4A7gchC9HvH1z5p9HWYp2vrc1kAODdbJgk0u+KzZk1xWwAunSHGhbFPXvScGcIDUf=ecn
ZgqDFC0Mh03p0DGR3CXYS-HuaZ20w6wXON94X7RqjXkCB1b6uZgGpSh6cVA49HfE
XZT39KscmlzRNLSSzm6p2PzYm45u1eSHAFV+vxpGAFwC3oBHMVSUWp9HfHf-A1MZGp
TUabX+qhrJbF8jFWz34D6fK7QSM6qubkUBSPVTY18dUxccc=YYJdNALC06PZSOsb36T5
pgVv9p6tLXkLkTqE1U5pmmZ7C9w9AMBA4GgepWMBUJABRNVHSMELDWAq8SpadXC
afG1L1pRXUG9b84GzAdBpNVH04EFQYarIL4LJ7HWPEdTauBECKbcGqOwOwDVR9gBDOw
MjAwBgRVHSAAMCgwwJkYwYBQOUHAgEwCmhbdlBzO8v4d3Lm6ZwswZS5dXmVY3BzMHYGCcsG
AOUFwEBEGGowaD8mBggRgeE7BwAwZauRRODwL543chSpemVucLuzVvzLVNvmlh6m3Mv
wW5mb3jYwNp24vY2fZ2k6ZwswZS9lc19YXmYWRadW50b3MsSVpFTBIFX1JPTTRUUMuY30
MBGAIUdeWbEwQMAYBARCAQAwDgYDVR0PQHBAQDAEGMDcGA1UdhwQwMC4wLKApoCjGImb0
dHAI4y9emwuaYpmbILwVicy9ZkYm1d28cm9yHfMAOCcSgOSpQ0EBwIA4EACQAQ
0eH44z8wDhu0Rn0wRWAgk15p36Tq40N98=3Yew83A2SCpcc=0h3QVPS-VVNhcC3
SPZmJdE2FalarCjgO2MjppIzI2mCOQ7C78D9pWvzRXyXUx60kW0wC1GhBL73DK
slngYfKcMwmbWk52aY+DRsd3Y8cy=SB1CDP2svWHz2K0ZLNpwwVUwLkApeUjppf
OqpScVYcG0As=CsX11WVsGMmqapYevbz7QhBUExX15MfvcRpdVZ30HHz0KpDXU+ww
jw+oM4Mglo88BzCRbNc2kq5Dwed4bDFX4R6CxyS6S7RkWRMOH0gz7FasDa+GHAz2Llf
+qVQX3RYycMhu04B0xw8hcNKZ8aLZLQ0-0SAPMPzcsK6ButDrLunWwqmKCIDNGR
clYtswEE1bTwJaARhcM0eyglaLgkhl8NSvnetTASpbMRCMITHVY8dgyFVwzZsbErdTo
+UgV74YAO8sbYPL63dscqu0bVWVWVNjelm553cAKAO5VpCsupnuoB8H0IYXUOkalxVCLN
+qUr157uMqm01skKlVgBfwAg0BGC290h1vz2jDW1W9ooPh3uKk+yllupG2Wm5vJ2E30Q==

```

-----END CERTIFICATE-----

## Signature algorithm:

SHA256withRSA

## Issuer CN:

ROOT CA QC IZENPE

## Issuer O:

IZENPE S.A.

## Issuer C:

ES

## Subject CN:

SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA

## Subject 2.5.4.97:

VATES-A01337260

## Subject O:

IZENPE S.A.

## Subject C:

ES

## Valid from:

Wed Sep 23 13:28:41 CEST 2020

## Valid to:

Sat Sep 23 12:57:18 CEST 2025

## Public Key:

```

3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B9:46:3C:43:D7:1D:21:83:DE:34:96:48:5E:05:53:32:A7:1B:66:A6:93:97:69:93:AC:02:71:A6:70:60:DE:94:7B:06:FD:
5B:F9:01:94:EB:09:FE:17:91:AD:7F:FA:AE:27:EC:C7:1A:AA:9D:7D:65:30:D8:38:82:D4:C2:3E:EC:F4:87:D0:68:66:D1:F0:96:CB:2E:08:DD:D3:9C:12:A6:30:89:AB:00:61:77:D2:FE:88:0C:F0:41:91:79:9A:8D:A7:B
C:9D:AC:A6:FE:6C:24:32:9B:E6:BC:96:A2:D1:E8:6D:03:D3:BC:9B:20:E1:CD:F9:4D:BF:3F:9E:E4:1F:BF:1D:DA:65:85:86:53:F2:C8:82:DF:A4:C4:D9:55:EA:F8:1CA:1:9E:5B:1B:C3:34:AD:9B:80:40:23:74:2D:A0:6A:98:
AC:68:9C:AD:37:AA:58:65:BC:63:59:A8:32:AD:8D:09:6A:4A:8C:38:62:DC:07:A0:BF:0D:D2:17:46:3B:20:44:51:E3:53:1C:01:85:FA:03:B8:9C:18:F5:0E:A3:C6:78:8E:DF:D9:00:3A:5C:AF:F7:3C:DF:0D:61:89:7F:6A:1E:0
7:04:29:A2:66:2B:3E:98:06:C9:51:2E:36:DF:19:1D:C2:09:07:8A:47:0D:7B:82:CC:6D:5A:0D:F1:1B:80:3B:A9:E8:42:F8:7B:DF:1F:5C:F9:AE:92:47:59:8A:76:BE:87:25:62:29:22:01:00:E2:6F:5A:8A:D1:AF:A4:79:97:E4
:D7:15:02:74:87:19:B8:49:3D:7B:EB:49:C1:9E:24:35:05:EB:17:27:66:01:AS:3C:31:3C:FF:43:2B:23:79:23:A3:10:C6:46:1D:F1:5D:84:BE:20:2B:80:DD:9F:34:C3:0B:74:5C:7D:E1:7E:D1:7A:35:E1:08:1D:73:D1:A1:B
3:1A:94:88:BB:87:15:00:02:3D:84:58:04:C7:6A:D3:DF:D2:91:B1:C9:88:7F:3C:51:34:BA:D2:B3:39:B8:AA:7D:8F:CD:88:A6:E3:98:A2:12:24:87:00:55:7E:CB:1A:46:00:8B:FD:0A:DB:28:20:13:15:E5:45:A9:04:73:5D:F8:0F:
CC:53:31:A9:4D:4C:61:EF:7F:AA:86:B2:61:A8:94:A3:15:6C:F7:8D:36:C3:97:84:39:7C:75:8A:5C:0A:25:F0:52:3E:F4:D8:D7:C7:54:C5:77:9E:F9:66:09:C5:F3:40:2F:12:DE:45:A3:D9:48:EB:1B:DF:A4:P9:A6:05:15:CD:
A8:FA:8A:B2:E3:5E:1D:44:91:3A:84:7D:48:F9:06:99:AD:DB:B2:06:AF:D5:DF:02:03:01:00:01

```

## Authority Key Identifier

A9:68:35:C2:80:B1:A5:D4:BA:52:21:15:17:1B:D8:9B:E3:86:86:97

## Subject Key Identifier

61:AA:C8:2F:82:E4:8F:B1:D6:3C:50:D3:01:A0:44:0A:46:DE:1A:A4

## Certificate Policies

Policy OID: 2.5.29.32.0

CPS pointer: <https://www.izenpe.eu/cps>

## Authority Info Access

[http://www.izenpe.eu/contenidos/informacion/cas\\_izenpe/es\\_cas/adjuntos/IZENPE\\_ROOT\\_QC.crt](http://www.izenpe.eu/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt)

## Basic Constraints

IsCA: true - Path length: 0

## CRL Distribution Points

<http://crl.izenpe.eu/cgi-bin/izrootqc>

## Key Usage:

keyCertSign - cRLSign

## Thumbprint algorithm:

SHA-256

**Thumbprint:** 5C:29:9D:31:59:49:42:41:38:14:5E:5E:E1:DA:67:7D:93:4F:09:5D:8A:5B:F7:86:C7:AB:B8:CB:4F:C6:D6:5A

## X509SubjectName

**Subject CN:** SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA

**Subject 2.5.4.97:** VATES-A01337260

**Subject O:** IZENPE S.A.

**Subject C:** ES

## X509SKI

**X509 SK I** YarIL4Lkj7HWPFDTAaBECKbeGqQ=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

## Status Starting Time

2021-04-21T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 16.10.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 16.10.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 16.11 - Service (granted): Qualified TimeStamp issued by SUBCA QC IZENPE - TSA

#### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.



<b>Public Key:</b>	30820222300D06092A864886F70D010105000382020F003082020A0282020100C83B18B45D2C83AD529038381B8923CB49601FD5B71392E58B3AAE4E9E866F9C6E74FF75D0036C2D1A7FE36A4C8F980A4146BCA5483B0D4D68C54E322D52A46F3606A443AF94D3BCEFE771FD59C387E7E61C225977021DE69C866AD702A0EFFB5C2B60655005C7E703DC08F014637A95D3DC02205C77AB14850B05BD792A1208014E8C1F09C4B61669DE68B9CD5A1F69864F63E8787DB923799171E3954484B58F0525C74C968205D5A5BB2C0304AEFB41AFBD5229ED23EF844DD6EF7C9C7DE5743628A13AAB91B09B102F64369E23B717E52998679961E2B057DABE47EB9A8D81804AEF7E9C208F5D8DE792252FC26F8BE489F9C86A60317D416B7F53ADE764033B70851CD24301C5A13824670D5E4AF13BE9CE1DA540D2FF3AE277B1528A72361C39A0AB415183FFCDE6963A4407CT9D8CA82375DD61235B75F7DDA200648959403824CD8ED972C05D6D2AD91DE789C58B892CE51B3117717802C1AC56F8EDF620E0505E3C36A6BFB4AB7E9F1B3D7B237C321D2D4110B07C52C07002C551A4F98A933E8A8229D538E0067F5EAS83B9B960D2658F10E74DA50C3E619C7A47AE76E3281C8D94886A7826CD121C5AD353E8E33FCDE7D92AB999C4EBB5E640A3EAE9DFB9E53994AC81940AFBCD5CB2B461E8F776E17AA0B23C7C953B7B466F3E7700206E55E08203E16A0854C4AD482CS50F43F78F5BA3F91903B0203010001	
<b>Extended Key Usage</b>	<i>id_kp_timeStamping</i>	
<b>Subject Key Identifier</b>	6E:72:03:7C:9F:66:79:AD:E9:6B:5A:3B:B8:71:3F:8D:6F:BC:ED:CC	
<b>Authority Key Identifier</b>	EA:84:45:BA:7F:5C:49:FB:15:0B:A3:0F:0E:8D:9C:E4:3F:AB:A2:C1	
<b>Certificate Policies</b>	Policy OID: 1.3.6.1.4.1.14777.10.1	
	CPS pointer: <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>	
	CPS text: [Kontsulta <a href="http://www.izenpe.eus-en">www.izenpe.eus-en</a> baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado]	
<b>Authority Info Access</b>	<a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SUBCA_QC_TSA.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SUBCA_QC_TSA.crt</a>	
<b>CRL Distribution Points</b>	<a href="http://crl.izenpe.eus/cgi-bin/izenpeTSA">http://crl.izenpe.eus/cgi-bin/izenpeTSA</a>	
<b>Key Usage:</b>	<i>digitalSignature</i>	
<b>Thumbprint algorithm:</b>	SHA-256	
<b>Thumbprint:</b>	D0:96:8A:07:3A:C6:46:F6:86:AC:CD:A8:44:BB:A6:CE:83:0C:D0:E1:A2:F4:E2:28:DB:A6:73:47:C9:F3:61:7C	
<b>X509SubjectName</b>		
<b>Subject CN:</b>	<i>tsa.izenpe.com</i>	
<b>Subject 2.5.4.97:</b>	VATES-A01337260	
<b>Subject O:</b>	<i>IZENPE S.A.</i>	
<b>Subject C:</b>	ES	
<b>X509SKI</b>		
<b>X509 SK I</b>	<i>bnIDfJ9mea3pa1o7uHE/jW+87cw=</i>	
<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>	
<b>Service status description</b>	[en]	undefined.
	[es]	undefined.
<b>Status Starting Time</b>	2021-04-21T00:00:00Z	
<b>Scheme Service Definition URI</b>		
<b>URI</b>	[en]	<a href="https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx">https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx</a>

**URI**

[ es ]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>



**17 - TSP: Firmaprofesional, S.A.****TSP Name**

**Name** [ en ] *Firmaprofesional, S.A.*

**Name** [ es ] *Firmaprofesional, S.A.*

**TSP Trade Name**

**Name** [ en ] *Firmaprofesional, S.A.*

**Name** [ es ] *Firmaprofesional, S.A.*

**Name** [ en ] *VATES-A62634068*

**Name** [ en ] *Firmaprofesional S.A. NIF A-62634068*

**Name** [ en ] *Firmaprofesional SA*

**Name** [ en ] *Firmaprofesional S.A.*

**PostalAddress**

**Street Address** [ en ] *Paseo de la Bonanova, 47*

**Locality** [ en ] *Barcelona*

**State Or Province** [ en ] *Barcelona*

**Postal Code** [ en ] *8017*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Paseo de la Bonanova, 47*

**Locality** [ es ] *Barcelona*

**State Or Province** [ es ] *Barcelona*

**Postal Code** [ es ] *8017*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info@firmaprofesional.com*





**Signature algorithm:** *SHA1withRSA*

**Issuer E:** *ca@firmaprofesional.com*

**Issuer CN:** *Autoridad de Certificacion Firmaprofesional CIF A62634068*

**Issuer L:** *C/ Muntaner 244 Barcelona*

**Issuer C:** *ES*

**Subject CN:** *AC Firmaprofesional - CA1*

**Subject O:** *Firmaprofesional S.A. NIF A-62634068*

**Subject OU:** *Jerarquia de Certificacion Firmaprofesional*

**Subject OU:** *Consulte <http://www.firmaprofesional.com>*

**Subject L:** *C/ Muntaner 244 Barcelona*

**Subject E:** *ca1@firmaprofesional.com*

**Subject C:** *ES*

**Valid from:** *Thu Mar 27 12:51:38 CET 2003*

**Valid to:** *Tue Mar 26 00:00:00 CET 2013*

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C7:AB:9E:30:93:63:6F:A8:BA:B5:DC:6A:F1:A9:5A:05:66:E3:95:9D:B7:8C:41:5A:A5:0C:86:75:82:E8:95:00:18:F7:8  
C4:2:3D:A5:FF:8B:75:C4:24:4A:9A:9F:0A:A5:7C:6E:B7:A2:4F:3F:3D:64:65:EE:57:BC:43:A4:21:25:54:CD:47:8C:8E:69:5C:5B:1A:5B:C5:F6:72:24:F5:3E:F8:DB:96:02:86:0A:A8:AE:ED:13:FE:8F:22:53:A2:2D:64:9F:1BC  
9:94:87:8A:E6:67:C9:C3:B0:10:55:59:E9:E4:17:F4:2C:AF:27:FB:CD:84:23:16:D6:25:D3:B9:02:8B:72:45:37:09:24:80:3C:72:98:10:4D:26:D4:53:21:6C:0A:D6:6B:36:C8:D1:E1:64:F3:FE:55:1C:57:FD:FD:9C:B2:C9:A4:E1:6  
4:4C:84:F8:E1:6C:DA:2F:2B:ED:F0:03:B1:DE:F0:CD:E1:71:4A:36:A3:56:8B:85:3A:73:AD:BB:46:14:57:AB:E9:97:88:42:70:DA:AC:37:80:39:4E:EA:51:09:FB:4F:C7:D9:79:AF:87:4E:82:E0:89:2C:D0:6A:E8:91:0F:7A:36:  
FB:DE:C1:54:DC:71:6F:89:74:DC:56:95:61:5D:4C:69:2D:0C:CE:7F:AC:4D:64:3D:1B:53:02:03:01:00:01

**Issuer Alternative Name** *<http://www.firmaprofesional.com>*

**Subject Alternative Name** *<http://www.firmaprofesional.com>*

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *8B:50:57:5A:C1:BD:92:00:A6:B7:E5:85:5D:C3:DD:B6:B5:86:90:D2*

**Authority Key Identifier** *33:0B:A0:66:D1:EA:DA:CE:DE:62:93:04:28:52:B5:14:7F:38:68:B7*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.13177.10.10.1*  
*CPS pointer: <http://www.firmaprofesional.com/cps/cps.htm>*

**CRL Distribution Points** *<http://crl.firmaprofesional.com/firmaprofesional.crl>*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** 65:BA:8F:C0:CE:3C:43:41:64:DC:40:81:5A:6C:A6:FB:44:C7:27:20:46:FC:D3:03:A2:9D:A8:F4:1C:A2:07:5D

## X509SubjectName

**Subject CN:** AC Firmaprofesional - CA1

**Subject O:** Firmaprofesional S.A. NIF A-62634068

**Subject OU:** Jerarquia de Certificacion Firmaprofesional

**Subject OU:** Consulte <http://www.firmaprofesional.com>

**Subject L:** C/ Muntaner 244 Barcelona

**Subject E:** ca1@firmaprofesional.com

**Subject C:** ES

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

## Status Starting Time

2017-11-16T00:00:00Z

### 17.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.5.2

### 17.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 17.1.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

**Name** [en] *Qualified Certificates issued by "AC Firmaprofesional - CA1"*

**Name** [es] *Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

## Service digital identities

### X509SubjectName

**Subject CN:** *AC Firmaprofesional - CA1*

**Subject O:** *Firmaprofesional S.A. NIF A-62634068*

**Subject OU:** *Jerarquia de Certificacion Firmaprofesional*

**Subject OU:** *Consulte <http://www.firmaprofesional.com>*

**Subject L:** *C/ Muntaner 244 Barcelona*

**Subject E:** *ca1@firmaprofesional.com*

**Subject C:** *ES*

### X509SKI

**X509 SK I** *i1BXWsG9kgCmt+WFxcPdrWGkNI=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

### 17.1.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.5.1*

#### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.13177.10.1.5.2*

**17.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**17.1.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by "AC Firmaprofesional - CA1"*

**Name** [ es ] *Certificados reconocidos emitidos por "AC Firmaprofesional - CA1"*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - CA1*

**Subject O:** *Firmaprofesional S.A. NIF A-62634068*

**Subject OU:** *Jerarquia de Certificacion Firmaprofesional*

**Subject OU:** *Consulte <http://www.firmaprofesional.com>*

**Subject L:** *C/ Muntaner 244 Barcelona*

**Subject E:** *ca1@firmaprofesional.com*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *i1BXWsG9kgCmt+WFxcPdtrWGkNI=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2004-11-25T00:00:00Z*

**17.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [ en ] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*





**Issuer C:** ES

**Subject CN:** AC Firmaprofesional - AAPP

**Subject SERIAL NUMBER:** A62634068

**Subject OU:** Certificados Digitales para la Administracion Publica

**Subject O:** Firmaprofesional SA

**Subject C:** ES

**Valid from:** Wed Jul 07 11:35:43 CEST 2010

**Valid to:** Thu Jul 07 11:35:43 CEST 2022

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082019A0282010100AB96E90E053D6E40F3B2081EFA092F89C7C63768396FB15555C0F72E2101A8A5F9F774  
4B44DFEA898377494F50A9FB445F4080CE7E7E243C8C2076E892E3E7A752F70A6559EF92AA7A0FC6AA03AD960335B159C01884225E9A15B7E025A10A355E1A91  
85E9F8503A87FB09345FCA4765CE015EAA0A60B88F5E88E70BAF1B8CAD59098CB514A6C65045D42CACED2B6FD5F365AC36EC0245BA757D48AA5151E0364030D0  
46F119AA756AEF0713C2590D22844B951FCDA635F1410746A00F2616854CA4A3322393FC4676987042402A9753CE73427F13C31D604CA0ED4E19D7C3C3F149FF40D8  
F8A57856A5357BF5F0676642D2D6E4408841464BD84FA69050203010001

**Authority Info Access** <http://servicios.firmaprofesional.com/ocsp>

**Subject Key Identifier** A6:2E:EA:4D:25:2B:25:BA:A4:B5:DA:20:D2:1D:AE:E7:96:FD:99:F7

**Basic Constraints** IsCA: true - Path length: 0

**Authority Key Identifier** 65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.13177.10.10.1  
CPS pointer: <http://www.firmaprofesional.com/cps>  
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <http://www.firmaprofesional.com/cps>]

**CRL Distribution Points** <https://crl.firmaprofesional.com/fpoot.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 83:F6:F0:17:C2:53:6D:74:54:B7:B9:84:86:74:F3:64:01:29:CF:55:5D:D0:7D:83:D3:62:A1:7C:81:B7:52:5F

**Certificate fields details**

**Version:** 3

**Serial Number:** 7893570382112079418



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *63:65:B2:5E:92:99:B5:F3:82:EB:00:66:85:06:29:08:8E:BC:D9:BC:B3:98:F2:86:22:10:76:03:C3:C1:C2:7E*

**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - AAPP*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Digitales para la Administracion Publica*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-12-21T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[es] https://avancedigital.mineco.gob.es/es-Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[en] https://avancedigital.mineco.gob.es/en-Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**17.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

**Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

**17.2.2 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

17.2.3 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

17.2.4 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Emisión de certificados reconocidos (AAPP)*

**Name** [ en ] *Qualified Certificates Issuance (AAPP)*

Service digital identities**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - AAPP*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Digitales para la Administracion Publica*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *pi7qTSUrJbqktdog0h2u55b9mfc=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2017-11-16T00:00:00Z*

17.2.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** [ en ] *undefined.*

[ es ] *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] *urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

**Policy Identifier:**

**Identifier** [ OIDsURN ] *urn:oid:1.3.6.1.4.1.13177.10.1.21.3*

**17.2.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**17.2.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**17.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** [ es ] *Emisión de certificados reconocidos (AAPP)*

**Name** [ en ] *Qualified Certificates Issuance (AAPP)*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - AAPP*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Digitales para la Administracion Publica*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *pi7qTSUrJbqktdog0h2u55b9mfc=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**17.2.5.4 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.21.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.21.2*

**17.2.5.5 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.22.3*

**17.2.5.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**17.2.6 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ es ] Emisión de certificados reconocidos (AAPP)*

Name [en] Qualified Certificates Issuance (AAPP)

### Service digital identities

#### X509SubjectName

Subject CN: AC Firmaprofesional - AAPP

Subject SERIAL NUMBER: A62634068

Subject OU: Certificados Digitales para la Administracion Publica

Subject O: Firmaprofesional SA

Subject C: ES

#### X509SKI

X509 SK I pi7qTSUrJbqktdog0h2u55b9mfc=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2011-04-28T00:00:00Z

#### 17.2.6.7 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

#### Criteria list assert=atLeastOne

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.1

Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.2

#### 17.3 - Service (granted): Qualified certificates issued by "AC Firmaprofesional – CUALIFICADOS"

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
--------------------------	------	--







**Subject OU:** *Certificados Cualificados*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**Valid from:** *Fri Dec 14 11:13:23 CET 2018*

**Valid to:** *Tue Dec 31 05:02:00 CET 2030*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100BA70895409A09ED7680C9C5B1515E3DEFF59E76CE7F9B3FF277D14AE1347D07E2F9F2E954BBA1539DF9A310BEFA96F49993AD8200D62E168E9E139D6347AB444D9503338D1FAE4247984883AB42148731E8DA874CB1FB252E2E858349739D89A57E0828CDFA7BDC083531256FA39A237F5156641F34112B733471B4111913400DE28FB2B52B074D36F0E8418323CE4C4CE92C77048C57CFCFAF69975ED94592482D5583AD53CCF24F838CF9CEA63C49A758BFAE1E9B8B8EDC973BD9F546B3BECA7CAE6B9E211A48788A28EDD5ADCF79C81D63BD4F457E196C2163129D7BCA39E63ABBAF85F82924C70AA244E31BC21155D8D4E6C81CF81738DD56162332F1BE50203010001

**Authority Info Access** *http://crl.firmaprofesional.com/caroot.crt*

*http://ocsp.firmaprofesional.com*

**Subject Key Identifier** *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

**Certificate Policies** *Policy OID: 2.5.29.32.0*

*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]*

*CPS pointer: http://www.firmaprofesional.com/cps*

**CRL Distribution Points** *http://crl.firmaprofesional.com/fpoot.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *4C:CF:17:C0:C8:C1:C1:0D:58:76:EC:5E:32:80:FE:8D:13:4D:F3:6A:ED:D8:44:42:89:B9:90:BC:37:41:E7:4F*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

<b>Service status description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Status Starting Time** *2023-04-20T00:00:00Z*

### 17.3.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

<b>URI</b>	<i>[ en ]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	---------------	--

**17.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**17.3.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.13.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.22.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.21.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.1.3
------------	-------------	------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.11.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.2.3
------------	-------------	------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.12.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.40.3
------------	-------------	-------------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.13177.10.1.10.3
------------	-------------	-------------------------------------

**17.3.4 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”*

**Name** *[ es ]* *Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - CUALIFICADOS*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Cualificados*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2022-09-13T00:00:00Z*

**17.3.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**17.3.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**17.3.4.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.13.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.11.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.12.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.40.3

**17.3.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”

**Name** [es] Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”

**Service digital identities****X509SubjectName**

**Subject CN:** AC Firmaprofesional - CUALIFICADOS  
**Subject SERIAL NUMBER:** A62634068  
**Subject OU:** Certificados Cualificados  
**Subject O:** Firmaprofesional S.A.  
**Subject C:** ES

**X509SKI**

**X509 SK I** jHHMkwdv0dWGaH2COkHZTAL4ll0=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2019-10-28T01:00:00Z

**17.3.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.13.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.11.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.2.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.12.3

#### 17.3.5.5 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 17.3.5.6 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 17.3.6 - History instance n.3 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### **Service Name**

**Name** [ en ] *Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”*

**Name** [ es ] *Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *AC Firmaprofesional - CUALIFICADOS*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Cualificados*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2017-11-16T00:00:00Z*

**17.3.6.7 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.13.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.22.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.21.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.11.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.12.3

**17.3.6.8 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**17.3.6.9 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>



**17.3.7 - History instance n.4 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”*

**Name** *[ es ]* *Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - CUALIFICADOS*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Cualificados*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**17.3.7.10 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.13177.10.1.10.2*

**17.3.7.11 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.13177.10.1.1.3

**17.3.7.12 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**17.3.8 - History instance n.5 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates issued by “AC Firmaprofesional – CUALIFICADOS”*

**Name** [ es ] *Certificados reconocidos emitidos por la “AC Firmaprofesional - CUALIFICADOS”*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - CUALIFICADOS*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Certificados Cualificados*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jHHMkwdv0dWGaH2COkHZTAL4ll0=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2015-07-26T22:00:00Z*

**17.3.8.13 - Extension (critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** [en] *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

[es] *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.13177.10.1.10.2

**17.4 - Service (withdrawn): AC Firmaprofesional – CLOUD QUALIFIED TSA**

**Service Type Identifier** http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

**Service type description** [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[es] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

**Service Name**

**Name** [en] AC Firmaprofesional – CLOUD QUALIFIED TSA

**Name** [es] AC Firmaprofesional – CLOUD QUALIFIED TSA

**Service digital identities**

**Certificate fields details**

**Version:** 3

**Serial Number:** 6161211743113377719

**X509 Certificate**

```

-----BEGIN CERTIFICATE-----
MIIFnCCBlegAwIBAgIYVFB9Y897cwDOYJKozIhvcNAOELBOAwgY0xCzAJBgNVBAYTAkVTMR4w
HAYDVQQKBG9GZXRhYyByZ2Zlc2I2bW9fMjFMc0NkSjA1Ym9uVBA5MEVNYjY3a3R5NFkzZyZVZ
MRWwEAYDQOQFwBjBjZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
QUlVTVFVQVIRVURkEwIHRlc2EwMjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
U2EzMBGAlUECMBRm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
NjE0LTA1BgNVBAMTEUJlbnR1b3R1b3R1b3R1b3R1b3R1b3R1b3R1b3R1b3R1b3R1b3R1b3R1
KozIhvcNAOELBOAwgY0xCzAJBgNVBAYTAkVTMR4wHAYDVQQKBG9GZXRhYyByZ2Zlc2I2bW9
CTlRkSAdUOEIYVFB9Y897cwDOYJKozIhvcNAOELBOAwgY0xCzAJBgNVBAYTAkVTMR4w
NSAoYWFkZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
yKSeIc09n7zIBRbNasBfcMH6kYabB5kck9usZfYp30AgSk1U1DwdODELH008q4WM2pjl
Ias6dW5eagPHIV7DyaldCZzskTzYVCS4dMqk5S5pYSMYqVbhw0zZMBKSCIEAwEA
AeQCAbcwgeTUMHGGCCGAOUFBwEIBHEwbaA3BgeRgEgFB0cwoA1ZaHRaGDevL2N9c5maXXYXBy
bZzlc2I2bW9fMjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
dHRwOjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
VRR0AQHBAUwADAIBgNVHSMGDAWBgRFAuIw9pYFf-gNk878kH8c1AuBgNVHRAEEARG08y
MDIwMDIyNzEzMTkzMl0wOYDVR0gBHIVwDByBgsRgEgEAETBMKCCCGAOUFBwEIBHEwba
cmYzLmZpcmlhcHVhZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
AgBAMBGAUUIQEBwQMMAGCCGAOUFBwEIBHEwbaA3BgeRgEgFB0cwoA1ZaHRaGDevL2N9c5ma
OC6DEeEzWvXQR8PUEqBz0zWwdsyRZSNQGB9hmovOzZge2IJZ0K84amHWnY0ZbhcZ
upZAcNvXT6WKe5tH2E10Z2T1-7NvY1YSPKv4Bjupc3a0AazNEEdA0S2p0Y19PLX
Plz1AADDESYPW21ZTC57jAipOAsb6qLzjY0vCY0L1-9Ecz1msru-PYxg03ma4va37qZj
storRuhYRIEQHW7370SGrUQxabbC46NFqgNDiowsG33RU0hXc8hsHqg8L8pmDh33oXVYceZ
0E++vV9ac9IN3AgUc-9Dmz
-----END CERTIFICATE-----

```

**Signature algorithm:** SHA256withRSA

**Issuer CN:** AC Firmaprofesional - INFRAESTRUCTURA

**Issuer SERIAL NUMBER:** A62634068

**Issuer OU:** Security Services

**Issuer O:** Firmaprofesional S.A.

**Issuer C:** ES

**Subject CN:** FIRMAPROFESIONAL CLOUD QUALIFIED TSU

**Subject 2.5.4.97:** VATES-A62634068

**Subject O:** Firmaprofesional S.A.

**Subject C:** ES

**Valid from:** Mon Feb 27 14:19:33 CET 2017

**Valid to:** Sun Feb 26 14:19:33 CET 2023

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B0B5A68096F4358367FED9E9EDF3F9EE8C0753354B96CB2AA5C58AD89858FF790937D  
F339022D1473413FF466B7024D7DA1FDD9F10E4F4B377D07BADA94209129054EC31C10B997C9800E266276F0031AE7F229034FC9715379C684585A5145D63670E  
6C7383CC66AD5C5C20188C0B3FBB3258B25752C63E8909F7CECAE6F6DA2296585EBEBC2A2F9BE7048C9793B14DCE9292B3F95CD3D9FB6941461340B011SC307E  
887586816F92A07A4F6EB33175C8FD40204A47355136F074E0C4507D0E8BCAB858CDA9AA595AE5B7C659FB2D12A3C78E34D5E33BD421E0C2D599E8293CEB542F3  
888CA8A7B9277E69612318A88BCD86AC22EF36493014A508810205010001

**Authority Info Access**  
<http://crl.firmaprofesional.com/infraestructura.crt>  
<http://ocsp.firmaprofesional.com>

**Subject Key Identifier**  
F0:4D:42:4A:5E:32:C1:02:FE:61:82:AD:EC:25:50:86:07:0D:FB:B1

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.13177.10.1.4.1  
CPS pointer: <http://www.firmaprofesional.com/cps>  
CPS text: [Certificado de Servicio Seguro TSA]

**CRL Distribution Points**  
<http://crl.firmaprofesional.com/infraestructura.crl>  
<http://crl2.firmaprofesional.com/infraestructura.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Key Usage:**  
digitalSignature - nonRepudiation

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
85:AF:F8:9B:8E:90:39:70:02:70:BB:83:6C:F5:35:8E:B8:85:A9:4F:FA:B4:6E:0E:94:15:F1:6C:5D:2  
1:62:89

X509SubjectName

**Subject CN:** *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *8E1CSl4ywQL+YYKt7CVQhgcN+7E=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-12-21T00:00:00Z*

### 17.4.1 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

## Service Name

**Name** *[en] AC Firmaprofesional – CLOUD QUALIFIED TSA*

**Name** *[es] AC Firmaprofesional – CLOUD QUALIFIED TSA*

## Service digital identities

### X509SubjectName

**Subject CN:** *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *8E1CSl4ywQL+YYKt7CVQhgcN+7E=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2017-11-16T00:00:00Z*



Valid to: Tue Dec 31 05:02:55 CET 2030

Public Key: 30820122300D06092A864886F70D01010105000382010F003082010A0282010100BA:A5:FB:57:D4:4F:1E:66:7E:4A:91:A5:85:74:9F:44:41:2D:3A:28:91:4B:C4:9D:24:2D:50:B8:E0:76:11:82:E2:14:47:3B:D9:01:59:1C:84:4F:20:76:6E:FA:36:CB:67:BB:9C:F8:6C:3E:57:86:9A:4F:38:43:D0:60:44:8D:87:5C:3E:04:F4:7F:82:42:1F:9E:9E:D9:E7:A4:34:50:97:1E:DC:22:45:F9:CE:DE:F9:D3:15:DF:8C:0A:E2:7D:54:88:21:41:D1:7E:2C:9F:66:63:6E:CA:7D:EA:A8:1E:4E:FE:7C:FS:2B:F6:1E:94:A4:99:B5:B8:DC:D5:4A:AS:C1:75:38:B1:FA:D9:44:52:60:9B:43:C5:EA:8C:49:AA:BA:14:F1:55:44:8C:1C:DD:6D:55:AC:1B:D2:84:73:DD:60:1B:4B:99:50:96:72:D:61:89:3F:67:FB:23:FC:EB:92:2D:96:39:FF:52:3D:FA:C0:D3:5B:E2:63:0D:8F:49:EF:FC:D5:9E:CE:B4:00:CA:CB:4E:FA:37:A6:78:93:2E:07:69:2D:5A:36:CA:B1:C7:F2:D3:CA:55:21:FB:D3:B4:71:C1:8A:49:04:A9:3B:CE:CB:15:BA:CA:36:29:46:BC:84:50:63:3A:E3:22:D5:1A:C0:6B:05:D0:AB:94:13:02:05:01:00:01

Authority Info Access http://crl.firmaprofesional.com/caroot.crt

http://ocsp.firmaprofesional.com

Subject Key Identifier 62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79

Basic Constraints IsCA: true - Path length: 0

Authority Key Identifier 65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

Certificate Policies Policy OID: 2.5.29.32.0

CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]

CPS pointer: http://www.firmaprofesional.com/cps

CRL Distribution Points http://crl.firmaprofesional.com/fpoot.crl

Extended Key Usage id\_kp\_clientAuth - id\_kp\_serverAuth - id\_kp\_OCSPSigning - id\_kp\_timeStamping

Key Usage: keyCertSign - cRLSign

Thumbprint algorithm: SHA-256

Thumbprint: CD:74:19:8D:4C:23:E4:70:1D:EA:57:98:92:32:1B:9E:4F:47:A0:8B:D8:37:47:10:B8:99:AA:D1:49:5A:4B:35

Certificate fields details

Version: 3

Serial Number: 1069733489479276534

X509 Certificate -----BEGIN CERTIFICATE-----

MIGTCCBE2gAwIBAgITDh080TAVYwDQYJKoZIhvcNAQELBQAwUTELMAKGA1UEBmMCRVVMsQjBA... (Base64 encoded certificate content)

-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer CN: Autoridad de Certificación Firmaprofesional CIF A62634068

**Issuer C:** ES

**Subject CN:** AC Firmaprofesional - INFRAESTRUCTURA

**Subject SERIAL NUMBER:** A62634068

**Subject OU:** Security Services

**Subject O:** Firmaprofesional S.A.

**Subject C:** ES

**Valid from:** Thu Jul 09 13:10:55 CEST 2020

**Valid to:** Tue Dec 31 05:02:55 CET 2030

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100BA:A5FB:57D44F1E667F4A91A585749F44412D3A28914BC49D242D50B8E0761182E21447  
8B D9 01 59 1C 84 4F E0 70 66 F8 26 CB 67 BB 9C F8 62 C3 E5 73 86 59 AF 38 43 D0 60 44 SD 87 5C 3E 04 F4 F7 A2 42 1F 9E 8E D9 E7 A4 54 50 97 1E DC 22 45 F9 CE DE F9 D3 15 DF 8C 0A E2 7D 54 B8 21 41  
D1 7E 2C 9F 66 63 6E CA 7D EA A8 1E 4E FE 7C FS 2B F6 1E 94 A4 99 B5 B8 DC D3 4A AS C1 75 38 B1 FA D9 44 52 60 9B 43 C3 EA 8C 49 A8 BA 14 F1 55 44 8C 1C DD 6D 55 AC 1B D2 84 73 DD 60 1B 4B B9  
50 96 72 2D 61 89 3F 67 FB 23 FC EB 92 2D 96 39 FF 52 3D FA C0 D3 5B E2 63 0D 8F 49 EF FC D5 9E CE B4 00 CA CB 4E FA 37 A6 7C 93 2E 07 69 2D 5A 36 CA B1 C7 F2 D3 CA 55 21 FB D3 B4 71 C1 8A 49 0  
4 A9 3B CE CB 15 BA CA 36 29 46 BC 84 50 63 3A E3 22 D5 1A C0 6B 05 D0 AB 94 13 02 03 01 00 01

**Authority Info Access**  
<http://crl.firmaprofesional.com/caroot.crt>  
<http://ocsp.firmaprofesional.com>

**Subject Key Identifier**  
62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en  
<http://www.firmaprofesional.com/cps>]  
CPS pointer: <http://www.firmaprofesional.com/cps>

**CRL Distribution Points**  
<http://crl.firmaprofesional.com/fpoot.crl>

**Extended Key Usage**  
id\_kp\_serverAuth - id\_kp\_timeStamping

**Key Usage:**  
keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
84:8C:03:AB:64:7D:5B:D7:E0:D0:C4:3C:0B:5D:67:4C:C9:89:3F:83:6A:B8:63:AF:8F:3F:13:84:B5  
:44:D8:33

**X509SubjectName**

**Subject CN:** AC Firmaprofesional - INFRAESTRUCTURA

**Subject SERIAL NUMBER:** A62634068



**Subject OU:** *Security Services*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *YhWrtbMleaWH/oDZivCO/I8R/Xk=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2021-01-26T01:00:00Z*

**17.5.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**17.5.2 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ] AC Firmaprofesional –INFRAESTRUCTURA*

**Name** *[ es ] AC Firmaprofesional –INFRAESTRUCTURA*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - INFRAESTRUCTURA*

**Subject SERIAL NUMBER:** *A62634068*

**Subject OU:** *Security Services*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

X509 SK I

YhWrtbMleaWH/oDZiVCO/I8R/Xk=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time

2017-11-16T00:00:00Z

**17.5.2.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**17.6 - Service (granted): Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description

[ en ]

A time-stamping generation service creating and signing qualified time-stamps tokens.

[ es ]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

Service Name

Name

[ es ]

Sellos cualificados de tiempo emitidos por FIRMAPROFESIONAL CLOUD QUALIFIED TSU

Name

[ en ]

Qualified timestamps issued by FIRMAPROFESIONAL CLOUD QUALIFIED TSU

Service digital identities

Certificate fields details

Version:

3

Serial Number:

150936115047910965630931689977272272981

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIFyzCCL0gAwIBAgIQY09BY5QCdWgA131MIVTANBqkphkG9w0BAQsFADCBTELMAKGA1UE
BHMCRVZMhjaEgBNVBAoMFUZZpzmIhcHJmVzaW9uYVWwgl1y5BLjEaMBEGA1UECwwRU2VjdXpdHkg
U2VydmlZMkxkaEgBNVBAUUTzE2MjY2NDk0ZDZlMjE2MjY2NDk0ZDZlMjE2MjY2NDk0ZDZlMjE2
bCAEIQRURVBRVUUVDFVFSQTAeFw0MDA5MDYyOTM5MTNaFw0yNjAyMDQwOTM5MTNaMHYxCzAJ
BgNVBAYTAkVTRMR4wHAAYDVQQKExVGe2xAYXByb2Zic2VhbnRlZm9udG9wZDZlMjE2MjY2NDk0
ZDZlMjE2MjY2NDk0ZDZlMjE2MjY2NDk0ZDZlMjE2MjY2NDk0ZDZlMjE2MjY2NDk0ZDZlMjE2
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAIWgXhdXr07wBaz297KvmSR.LR.2A6D
VfC.F180XBLW-DWwWqjG.HuR.TuE+-sbU.XRR.PV.FnEn.Ven.SHY.09gl.Y.YHW.Icgnk.BzX.usbX.7LS
v.FH.Pz.F.C.B.R.Z.D.S.R.P.77m.P.M.Z.Y.N.+Q.N.D.L.3IF.S.T.H.K.R.+1.v.0.h.z.k.k.p.S.O.X.E.0.w.r.L.I.R.
Ac.V.hgr.+8.A.B.K.M.o.R.Z.D.J.U.G.p.a.n.L.W4.E.o.6.3.9.r.n.k.O.m.6.3.6.4.v.k.U.n.c.l.A.3.U.W.6.I.Y.f.b.H.s.d.v.p.k.T.6.n.2.X.z.z
bE.Y.V.6.A.l.n.v.c.u.x.c.s.t.r.-W.a.u.w.6.Y.d.s.-D.J.M.Y.S.e.m.p.h.H.m.h.k.Z.D.a.d.b.D.e.v.g.H.R.H.L.b.Z.Q.F.R.s.L.o.w.p.C.T.8.O.D
o.z.a.n.f.i.d.A.Q.A.R.o.f.C.O.c.K.A.s.c.w.D.A.Y.D.V.R.O.T.A.Q.H.B.A.w.A.D.A.B.R.N.V.H.S.M.E.G.D.A.W.g.R.R.I.t.a.u.s.w.p.Y.f.g.N.k.i
8I.78.j.H.9.E.T.B.9.B.g.g.R.g.E.F.B.Q.C.B.A.Q.R.A.M.G.S.w.P.w.Y.I.K.w.Y.B.B.O.U.H.M.A.K.G.M.2.h.0.H.A.6.l.y.9.c.m.w.z.m.l.y.b.W.f.w.c.m.9.m
Z.N.p.h.2.h.0.C.5.j.6.2.l.o.v.a.W.s.c.m.f.c.3.R.y.d.W.N.d.X.H.l.m.N.y.d.A.S.B.g.g.R.g.E.F.B.Q.C.A.Y.Y.g.a.H.R.O.D.o.V.L.2.9.c.3.A.u
Z.m.l.y.W.f.w.c.m.9.m.Z.N.p.h.2.h.0.C.5.j.6.2.l.o.v.a.Y.G.A.U.L.I.A.S.B.I.C.+B.L.K.+E.Q.U.L.A.w.Y.B.A.I.E.m.e.Q.B.R.A.E.w.s.Y.A.B.g.g.R.
g.E.F.B.Q.C.A.R.Y.j.a.H.R.O.D.o.V.L.3.d.5.a.5.m.a.X.Y.X.B.y.b.Z.l.c.2.v.h.m.F.S.L.m.N.v.S.9.g.H.M.w.P.w.Y.I.K.w.Y.B.B.O.U.H.A.g.l.w
M.w.w.Q.2.Y.v.d.G.i.m.a.W.N.Z.G.S.g.Z.G.l.g.U.2.V.y.d.m.l.a.W.g.l.2.V.n.d.X.v.G.R.H.F.R.I.Q.S.B.d.W.F.s.a.W.z.p.Y.F.K.Y.T.A.W.B.g.N.V.
H.S.I.B.A.I.E.D.A.K.B.g.g.R.g.E.F.B.Q.C.T.C.B.a.Y.D.V.R.O.H.w.A.S.o.f.S.p.Y.Y.a.H.R.O.D.o.V.L.2.N.y.C.5.m.a.M.Y.X.B.y
b.Z.l.c.2.v.h.m.F.S.L.m.N.v.S.9.p.h.m.z.Y.W.V.z.H.I.J.Y.3.R.I.c.m.E.U.Y.3.J.S.M.D.g.G.A.2.h.R.o.d.H.R.w.O.8.v.3.J.M.5.m.a.X.f
Y.X.B.y.b.Z.l.c.2.v.h.m.F.S.L.m.N.v.S.9.p.h.m.z.Y.W.V.z.H.I.J.Y.3.R.I.c.m.E.U.Y.3.J.S.M.B.O.G.A.I.U.D.D.G.O.W.B.B.R.p.C.W.3.K.C.V.G.2.o
S.K.a.E.m.o.x.g.p.c.A.r.g.B.V.R.L.E.I.G.A.S.M.D.I.M.O.w.N.S.M.E.M.I.B.D.2.o.M.O.w.M.G.I.M.D.R.O.T.E.W.O
B.g.N.V.H.Q.8.B.A.I.E.B.A.M.C.B.s.A.w.D.O.Y.J.K.o.Z.l.b.v.c.N.A.Q.E.L.B.O.A.D.g.g.E.A.E.Z.P.U.W.j.v.W.Q.z.g.H.w.O.z.m.S.M.s.l.a
I.Z.S.2.7.o.0.6.0.U.G.c.F.O.E.H.A.E.3.V.l.a.l.y.s.T.L.z.o.U.U.-M.D.I.3.I.E.g.p.O.E.L.G.V.L.N.I.C.g.M.L.F.W.N.A.2.7.5.-y.4.S.H.Q.Q.T
o.I.C.A.e.Q.w.e.y.C.m.w.s.B.V.g.H.l.b.H.L.L.a.z.e.f.f.o.W.U.Z.I.H.S.O.C.N.g.H.p.N.m.S.I.g.p.T.Z.S.T.C.Q.K.w.2
8.J.f.C.F.0.9.g.H.D.I.D.I.V.T.n.k.o.W.s.j.k.U.Z.Z.l.e.d.g.R.M.b.7.o.M.S.4.B.H.4.Q.a.I.P.p.H.c.S.T.B.H.D.A.Z.7.T.Q.D.C.N.K.C.g.6.3.N.B.V.h
J.G.h.a.Y.I.n.=T.=a.V.0.3.H.A.R.M.q.R.A.e.h.o.y.K.J.V.R.i.g.W.a.r.L.C.A.O.Z.P.G.a.=V.F.3.H.W.H.I.a.9.C.Y.K.p.F.W.k.a.P.e.s.e.6.M
n.a.A.X.B.E.=
-----END CERTIFICATE-----
```

Signature algorithm:

SHA256withRSA

Issuer CN:

AC Firmaprofesional - INFRAESTRUCTURA

**Issuer SERIAL NUMBER:** A62634068

**Issuer OU:** Security Services

**Issuer O:** Firmaprofesional S.A.

**Issuer C:** ES

**Subject CN:** FIRMAPROFESIONAL CLOUD QUALIFIED TSU

**Subject 2.5.4.97:** VATES-A62634068

**Subject O:** Firmaprofesional S.A.

**Subject C:** ES

**Valid from:** Thu Feb 06 10:39:13 CET 2020

**Valid to:** Wed Feb 04 10:39:13 CET 2026

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009568171DD5EB74E7F0241699BFEDECA8E6491FCB4767C0E8357F16D08523C397054F835  
A759E8DB1B522E2514E7244FB76D0F5174513D51671275649F71D8E8D8225186075A20A09EA901C0D7527B1B5F82D2BD36CF71DE663ED007D3D90F744FFA2EDFB6778  
F31961BB7E4313432F79458397D31DB2ADFB5BEC3A875BCC8A92DA52B36D225DF110C26D7525101C5626E0B7E7F006CA32845FD838E5506A409C8B8128EB77CAED  
9109BA0DD2E88EA9F149DC240DD45BA958ADB1FCFEC76FA644FA367D97C736C4615E809659F1FDCBB1C7F7B14F969DAC3A61D692F8324C639B26A6B1DB9A1449643  
69D6C3EAF807463E2D2DB66540546CD49A30A424FC383A33BAD7F0203010001

**Basic Constraints** IsCA: false

**Authority Key Identifier** 62:15:AB:B5:B3:08:79:A5:87:FE:80:D9:22:F0:8E:FC:8F:11:FD:79

**Authority Info Access**  
<http://crl.firmaprofesional.com/infraestructura.crt>  
<http://ocsp.firmaprofesional.com>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.13177.10.1.4.1  
CPS pointer: <http://www.firmaprofesional.com/cps>  
CPS text: [Certificado de Servicio Seguro de TSA cualificada]

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl.firmaprofesional.com/infraestructura.crl>  
<http://crl2.firmaprofesional.com/infraestructura.crl>

**Subject Key Identifier** 69:19:6D:E5:29:00:95:AC:6D:E8:48:A6:B7:9A:8C:59:82:9D:A7:73

**Key Usage:** digitalSignature - nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** CC:93:E2:7B:3D:2B:C8:FF:4E:4D:0E:65:2F:A2:18:7F:E3:AB:5D:FA:65:28:72:5C:FE:E3:70:E0:79:9C:E1:4A

X509SubjectName

**Subject CN:** *FIRMAPROFESIONAL CLOUD QUALIFIED TSU*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *aRlt5SkAlaxt6Eimt5qMWYKdp3M=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2020-04-28T00:00:00Z*

## 17.7 - Service (withdrawn): Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

## Service Name

**Name** *[en] Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020*

**Name** *[es] Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2020*

## Service digital identities

### Certificate fields details

**Version:** *3*

**Serial Number:** *133529187700912422781168782320038630024*



**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *93:3B:80:F7:B9:72:55:DF:5C:F1:D9:5A:12:3E:90:17:22:DD:B3:0B:48:1A:F3:AA:83:54:82:01:11:9E:D3:03*

**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - Secure Web 2020*

**Subject OU:** *Security Services*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *vZcOZ4ho7Skbm6tqCoo2io0uFik=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-02-06T00:00:00Z*

**17.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**17.7.2 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en]* *Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2020*

**Name** *[es]* *Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2020*

**Service digital identities****X509SubjectName**

**Subject CN:** *AC Firmaprofesional - Secure Web 2020*

**Subject OU:** *Security Services*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *vZcOZ4ho7Skbm6tqCoo2io0uFik=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**17.7.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**17.8 - Service (granted): AC Firmaprofesional CLOUD QUALIFIED TSU-2020****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description**

*[ en ]*

*A time-stamping generation service creating and signing qualified time-stamps tokens.*

*[ es ]*

*Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

**Service Name****Name**

*[ en ]*

*AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

**Name**

*[ es ]*

*AC Firmaprofesional CLOUD QUALIFIED TSU-2020*

**Service digital identities****Certificate fields details****Version:**

*3*

**Serial Number:**

*96352306425787635861384208292947363613*





**CRL Distribution Points** *http://crl.firmaprofesional.com/cualificados.crl*

**Subject Key Identifier** *FD:7B:45:0E:E9:80:02:FD:3E:EB:55:8A:AA:C8:E1:9B:DD:3F:55:56*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *E9:F0:94:3D:FC:4D:49:33:39:62:8A:18:3B:1F:89:09:B4:FD:B8:7B:C1:D9:1B:0C:BC:D1:7B:F3:83:3C:20:22*

**X509SubjectName**

**Subject CN:** *FIRMAPROFESIONAL CLOUD QUALIFIED TSU - 2020*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** */XtFDumAAv0+61WKqsjhm90/VVY=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

## 17.9 - Service (granted): Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2021

**Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[en] Qualified website authentication certificates issued by AC Firmaprofesional Secure Web 2021*

**Name** *[es] Certificados cualificados de autenticación de sitio web emitidos por AC Firmaprofesional Secure Web 2021*

**Service digital identities****Certificate fields details**



**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <http://www.firmaprofesional.com/cps>]  
 CPS pointer: <http://www.firmaprofesional.com/cps>

**CRL Distribution Points** <http://crl.firmaprofesional.com/fpoot.crl>

**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *59:22:85:35:D1:14:E8:D2:9F:9B:92:D4:22:51:8B:C6:3D:DC:B5:70:97:42:8D:8C:C9:87:77:D9:07:C6:EE:FE*

**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - Secure Web 2021*

**Subject OU:** *Security Services*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *C2rs67KoIGs617dZbkoqLc3efG8=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-03-17T01:00:00Z*

**17.9.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**17.10 - Service (granted): Qualified timestamps issued by "AC Firmaprofesional Timestamp 2021"****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens. [es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified timestamps issued by "AC Firmaprofesional Timestamp 2021"

Name [es] Sellos cualificados de tiempo emitidos por "AC Firmaprofesional Timestamp 2021"

Service digital identities

Certificate fields details

Version: 3

Serial Number: 11513680408172624437582487283217860548

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHhCCBvagAwIBAgIQCKR3ZBlN0iCYhYHsDANBgkqhkiG9w0BAQsFAADBRMgQwCQYDVQQG... [Certificate Base64 Encoded Content]

-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer CN: Autoridad de Certificación Firmaprofesional CIF A62634068

Issuer C: ES

Subject CN: AC Firmaprofesional - Timestamp 2021

Subject OU: Security Services

Subject 2.5.4.97: VATES-A62634068

Subject O: Firmaprofesional S.A.

Subject C: ES

Valid from: Tue Apr 13 11:32:20 CEST 2021

Valid to: Tue Dec 31 05:02:00 CET 2030

Public Key:

30820222300d06092a8e4886e70d01010105000382020f00303082020a0282020100cd089c... [Public Key Base64 Encoded Content]

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F*

**Authority Info Access**  
*http://crl.firmaprofesional.com/caroot.crt*  
*http://ocsp.firmaprofesional.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]*  
*CPS pointer: http://www.firmaprofesional.com/cps*

**Extended Key Usage** *id\_kp\_timeStamping*

**CRL Distribution Points** *http://crl.firmaprofesional.com/fpoot.crl*

**Subject Key Identifier** *16:A6:B4:B1:6C:C4:DB:DF:38:47:4C:1A:C0:46:36:58:DE:2C:EB:62*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *75:B1:4D:4D:63:80:6F:30:F5:38:06:0F:2E:B6:5C:13:65:BF:C0:CD:7F:3E:CD:C6:C0:07:02:18:B6:E4:67:59*

**X509SubjectName**

**Subject CN:** *AC Firmaprofesional - Timestamp 2021*

**Subject OU:** *Security Services*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Fqa0sWzE2984R0wawEY2WN4s62I=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-09-01T01:00:00Z*

**Scheme Service Definition URI**



**Subject 2.5.4.97:** VATES-A62634068

**Subject O:** Firmaprofesional S.A.

**Subject C:** ES

**Valid from:** Fri Mar 04 12:03:58 CET 2022

**Valid to:** Mon Mar 03 12:03:58 CET 2025

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100A7197231B622624D7A505795D7CD A94E D0F2199B CF8C1D F65646ACBA2840ED A78C5D AD12EC080013C90F1209367C8E8B8BC9E74BEC28A0EE579298906F088CF4812C69995A0AC46BA5B070D84E18E9EC9780287A5B867213F4F76EA37AA6596295F3220A E1CDD E63E C434FB E58F D0FB C82979EA E8B8977B CA ED9595 C3DC31373AF775892B560E47E77E E19E3D95587D DF837C6E F37072586919 ED0C564E53200641DA B56E5 D F1 E2 DE B04101 CB DF6197 EF44FA500E29612D E3692AF7A4446B3B33363787721E8C3E6490D17C3F40ED8D77707B3F96391B B95B0629F87E4D1C6C7B C9B6DE68B5D2 518C92405A5C9DF0D38F2F75E711D9953D7AAA18EA0AB0C5AD70203010001

**Basic Constraints** IsCA: true - Path length: 0

**Authority Key Identifier** 65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

**Authority Info Access**  
<http://crl.firmaprofesional.com/caroot.crt>  
<http://ocsp.firmaprofesional.com>

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <http://www.firmaprofesional.com/cps>]  
 CPS pointer: <http://www.firmaprofesional.com/cps>

**Extended Key Usage** id\_kp\_serverAuth

**CRL Distribution Points** <http://crl.firmaprofesional.com/fpoot.crl>

**Subject Key Identifier** 9B:8D:B1:FE:46:22:0F:35:90:50:3B:24:41:F9:F3:3A:EC:EC:BC:F1

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** C0:68:D7:76:78:42:55:77:2B:BC:6A:E9:F7:0A:53:6A:41:0A:D6:88:A5:0D:DE:AF:BF:66:BC:C5:25:47:96:F6

**X509SubjectName**

**Subject CN:** AC Firmaprofesional - Secure Web 2022

**Subject OU:** Security Services

**Subject 2.5.4.97:** VATES-A62634068

**Subject O:** Firmaprofesional S.A.

**Subject C:** ES





**Issuer CN:** *FIRMAPROFESIONAL CA ROOT-B GP*

**Issuer 2.5.4.97:** *VATES-A62634068*

**Issuer O:** *Firmaprofesional SA*

**Issuer C:** *ES*

**Subject CN:** *FIRMAPROFESIONAL ICA B01 QUALIFIED 2022*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**Valid from:** *Tue Jul 19 13:03:59 CEST 2022*

**Valid to:** *Sun Mar 31 11:04:41 CEST 2047*

**Public Key:**  
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:5E:75:DC:47:58:A3:70:57:81:53:E6:AB:3A:D1:98:04:DB:AA:A0:FE:74:AE:AA:59:02:32:1F:B9:A7:48:EF:5E:DA:32:54:FF:72:D9:71:45:2D:BS:2B:24:6E:89:91:0F:F4:47:61:63:E4:1B:28:C6:03:FC:0D:69:54:04:C7:83:0F:CC:EA:4E:87:74:19:42:2E:35:05:3F:DC:E5:4E:5F:23:CD:SE:C2:2A:F6:49:C8:9F:A6:7E:D0:C5:F5:55:E7

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *AA:E3:A4:94:F3:B0:B1:7F:A9:74:83:7B:B1:03:ED:6E:7D:2A:78:7E*

**Authority Info Access**  
[http://crl.firmaprofesional.com/caroot-b\\_gp.crt](http://crl.firmaprofesional.com/caroot-b_gp.crt)  
<http://ocsp.firmaprofesional.com>

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps]*

**CRL Distribution Points** *http://crl.firmaprofesional.com/caroot-b\_gp.crl*

**Subject Key Identifier** *4B:CD:B9:DA:13:26:56:AA:8C:7E:88:78:80:84:7E:CE:89:92:93:80*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *4A:86:F3:33:7C:EC:89:A6:78:96:B8:A6:CB:BA:DA:84:AC:18:1E:B0:09:67:9E:15:04:15:6C:34:BC:9F:8A:A1*

**X509SubjectName**

**Subject CN:** *FIRMAPROFESIONAL ICA B01 QUALIFIED 2022*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional SA*

Subject C: ES

X509SKI

X509 SK I S8252hMmVqqMföh4gIR+zomSk4A=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.  
[es] undefined.

Status Starting Time 2022-11-24T00:00:00Z

**17.12.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**17.12.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**17.12.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

Identifier [OIDAsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.13.3>

**Policy Identifier:**

Identifier [OIDAsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.22.3>

**Policy Identifier:**

Identifier [OIDAsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.21.3>

**Policy Identifier:**

Identifier [OIDAsURN] <urn:oid:1.3.6.1.4.1.13177.10.1.1.3>



**Issuer CN:** *FIRMAPROFESIONAL CA ROOT-A WEB*

**Issuer 2.5.4.97:** *VATES-A62634068*

**Issuer O:** *Firmaprofesional SA*

**Issuer C:** *ES*

**Subject CN:** *FIRMAPROFESIONAL ICA A01 QWAC 2022*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**Valid from:** *Tue Jul 19 14:16:44 CEST 2022*

**Valid to:** *Sun Jul 18 14:16:44 CEST 2027*

**Public Key:**  
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:BE:EB:B5:18:51:6B:F9:5C:56:F1:EA:1E:BD:38:2D:82:EE:6C:EF:2D:DF:E4:51:11:86:28:C7:72:4D:FA:19:11:18:0A:F8:CC:48:46:D3:6A:82:75:B  
D:A5:37:1E:BA:27:9F:13:26:02:EA:CS:F8:3D:8A:B8:BB:DE:06:64:C3:F2:C4:78:96:F7:D4:1F:43:A7:2B:D7:9F:CD:D6:7A:37:32:67:F6:F7:5F:41:98:0B:7A:BE:9A:94:C9:77:FD:BC:DE

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *93:E1:43:63:5C:3C:9D:D6:27:F3:52:EC:17:B2:A9:AF:2C:F7:76:F8*

**Authority Info Access**  
*http://crl.firmaprofesional.com/caroot-a\_web.crt*  
*http://ocsp.firmaprofesional.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en  
http://www.firmaprofesional.com/cps]*

**Extended Key Usage** *id\_kp\_serverAuth*

**CRL Distribution Points** *http://crl.firmaprofesional.com/caroot-a\_web.crl*

**Subject Key Identifier** *FD:3C:A7:E7:A2:68:D6:28:1A:3A:CF:7D:16:10:C4:FE:42:01:5B:C3*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:**  
*CC:1B:9F:9E:43:70:FB:68:14:1D:28:A1:15:EA:A8:63:F8:EA:DB:7A:04:E2:BD:23:B3:C6:2F:9D:9  
F:17:C2:63*

**X509SubjectName**

**Subject CN:** *FIRMAPROFESIONAL ICA A01 QWAC 2022*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** */Tyn56Jo1igaOs99FhDE/kIBW8M=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-11-24T00:00:00Z*

#### 17.13.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

#### 17.14 - Service (granted): Sellos cualificados de tiempo emitidos por "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*

*[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.*

**Service Name**

**Name** *[ es ]* *Sellos cualificados de tiempo emitidos por "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"*

**Name** *[ en ]* *Qualified timestamps issued by "AC FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022"*

Service digital identities

**Certificate fields details**

**Version:** *3*

**Serial Number:** *121555216222559795344142852949412708983*



**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *1F:3F:44:97:DF:9B:AC:9D:72:F9:99:75:B3:7D:ED:7D:5D:B9:30:05:B1:BF:80:E0:71:02:76:6F:3A:E4:05:B9*

### X509SubjectName

**Subject CN:** *FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022*

**Subject 2.5.4.97:** *VATES-A62634068*

**Subject O:** *Firmaprofesional SA*

**Subject C:** *ES*

### X509SKI

**X509 SK I** *YoYVvej9IfRJE/Z/D60Gs1WhH7s=*

### Service Status

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

### Status Starting Time

*2022-11-24T00:00:00Z*

### Scheme Service Definition URI

**URI** *[en] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\_Firmaprofesional.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\_Firmaprofesional.aspx*

**18 - TSP: Tesorería General de la Seguridad Social****TSP Name**

**Name** [ en ] *Tesorería General de la Seguridad Social*

**Name** [ es ] *Tesorería General de la Seguridad Social*

**TSP Trade Name**

**Name** [ en ] *Gerencia de Informática de la Seguridad Social*

**Name** [ es ] *Gerencia de Informática de la Seguridad Social*

**Name** [ en ] *Tesoreria General de la Seguridad Social*

**Name** [ es ] *Tesoreria General de la Seguridad Social*

**Name** [ en ] *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

**Name** [ en ] *VATES-Q2827003A*

**Name** [ en ] *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

**Name** [ es ] *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

**Name** [ en ] *Seg-social*

**Name** [ es ] *Seg-social*

**PostalAddress**

**Street Address** [ en ] *Calle Doctor Tolosa Latour*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28041*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Calle Doctor Tolosa Latour*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*





**Issuer C:** *ES*

**Subject OU:** *SGI*

**Subject O:** *Seg-social*

**Subject C:** *ES*

**Valid from:** *Fri Feb 14 13:03:28 CET 2003*

**Valid to:** *Tue Feb 14 13:33:28 CET 2023*

**Public Key:**  
30819F300D06092A864886F70D010101050003818D0030818902818100A6C89F29799A2E0BAB52D29F9A07E1022135F381151A CF20BF9F064D4BF7DA25597F07FD411C  
DA8DFD7785AE569F33AFDFD7B3799D9D467A27955B621A031114B85A C6D12C362B65E199D8C561D8A79F65451DDC8329243E11FC9E4F0D673AFC3C6A377CF6360B  
2A765C949D02BAD4CCFA9C06BAD2642B2589E14E5B361CCE7D0203010001

**CRL Distribution Points** *C=ES,O=Seg-social,OU=SGI,CN=CRL1*

**Authority Key Identifier** *71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*

**Subject Key Identifier** *71:74:77:E8:3C:22:A7:52:86:52:08:5D:C0:65:64:BC:F3:34:D9:F8*

**Basic Constraints** *IsCA: true*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F8:00:14:4F:1B:0F:26:83:42:3F:3D:03:3A:4E:5B:B8:A4:67:59:9C:BB:06:36:2C:4C:19:C1:A9:D8:  
C2:51:B9*

**X509SubjectName**

**Subject OU:** *SGI*

**Subject O:** *Seg-social*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time***2018-05-03T00:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-  
us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-  
es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**18.1.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:2.16.724.1.4.2.1.3

**18.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**18.1.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified certificates issued by GISS

**Name** [es] Certificados reconocidos emitido por GISS

**Service digital identities****X509SubjectName**

**Subject OU:** SGI

**Subject O:** Seg-social

**Subject C:** ES

**X509SKI**

**X509 SK I** cXR36Dwip1KGUghdwGVkvPM02fg=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

**18.1.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
----------------------------	------	------------

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:2.16.724.1.4.2.1.3
-------------------	------------	----------------------------

**18.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

**18.1.4 - History instance n.2 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[en]	Qualified certificates issued by GISS
-------------	------	---------------------------------------

<b>Name</b>	[es]	Certificados reconocidos emitido por GISS
-------------	------	---

**Service digital identities****X509SubjectName**

<b>Subject OU:</b>	SGI
--------------------	-----

<b>Subject O:</b>	Seg-social
-------------------	------------

<b>Subject C:</b>	ES
-------------------	----

**X509SKI**

<b>X509 SK I</b>	cXR36Dwip1KGUghdwGVkvPM02fg=
------------------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>
-----------------------	---

<b>Status Starting Time</b>	2010-04-20T00:00:00Z
-----------------------------	----------------------

**18.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
-----------------------------------	------	--

[es] está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

Criteria list assert=atLeastOne

Policy Identifier:

Identifier [ OIDsURN ] urn:oid:2.16.724.1.4.2.1.3

18.2 - Service (withdrawn): Qualified certificates issued by SUBCA GISS01

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [ en ] Qualified certificates issued by SUBCA GISS01

Name [ es ] Certificados reconocidos emitido por SUBCA GISS01

Service digital identities

Certificate fields details

Version: 3

Serial Number: 1466067264

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIHkDCCBggAwIBAgIEV2JpODANBgkqhkiG9w0BAQsFADCBjEELMAAGAIUEBMBKCRVMDzANBgNV
BAcMBRIRZDRDEAMCMAUExCcmwVETTFjRiRBEjFVSOIwRHEjTEU0VHVVYjRlEjFNP
Q0BIDE3MDUGAIUECcmwVSRU5DSUeRUpSU5GTlNOVGRJQ0RlEjUjEzEzU0VHVVYjRlEjFNP
Q0BIDE3MDUGAIUEBMBKCRVMDzANBgNVYwA1YDQODDASQ0UjEjFDR0ITU3YyMBAKDTE2MDYx
NjAsMTENbG90DTM2MDY1YmEwMjEwYkZlbnVBAU0YU0Y0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0ODQ0
MTA-BzNVBAgMKFRFUD0SRVJ0S0BRHU5UkFMIERHIE-BIFNFR1VSSURBCBTTONJQUwaNzAIBzNV
BAcMLkFUV0Q0BIEIEJERKSTUFUSUNBERFIE-BIFNFR1VSSURBCBTTONJQUwaDzANBgNV
BAcMBRIRZDRDEAMCMAUExCcmwVSRU5DSUeRUpSU5GTlNOVGRJQ0RlEjUjEzEzU0VHVVYjRlEjFNP
MAOGCqGSIb3DQEBAQUAA4ICDwAwggKAOlCAQCmoxDF0P6zDRz9FzAk-U9UwFAVZ-0DzG
LZC9vZH0dDg-OtXOn+7EJGqCJZFGBC0ua0AB7AcAAVp2GC6U8IaG3YhuJsmBNDHY
zsePb2C8oyKzSots0B0w60VPYzAKLylPqhwJlmBP99-cpld31wDhDyDzCzVFMKPFmz
Lk2h4MqCYDbealqwer4ANFY5ioZkZxHuzCvtrvale9ZCHntApqgRKSklHzTK4HLZ
VBOAgvY7ohv98lplRRVssrJWNBYSGlmcRc57bTSOmrSTL37acv1KLAPlH7-OnT0ZvzplNur
bqHfHkKlmoZx-viaUuziKOD-bcSvuz2ocQWCGPZVSIkzKCM12-lw7yUllhgD7Fk
w15zS7Pcad6colvWk17U7bWcx-wqEG3PAC4dWRKBj9JOWOspMSuuWpPc5d4SvWYc-4S
bEDQeADRe3r0bMgVigbplL-HrFZVbPbqbcSecsrLIqIEC4d3BMu86053Jp5llm
pb1roV5XyCPpsjF4kIKqKcALLkAtqWq0Za6D0-a8Kv8eTz2wRVz-w9ZsZACXyG
I5G66YK8c49ym6m6nce50wT9mxF9hH20wIDAQAo4ICyCCAswDqYDVR0PAQHBAQADAgEG
MAAGAIUdeEBw-OFMAMBAIDwgc8GAIUldIASBzC-BzDCBQYIYUAAQCAGewgQwKwYkwyYBBQIH
AgEWEH0dHAEly93d3cnc2VnLXNvY2hhbC5icy9BQ0JUI1MwYkCCGSAQ0FbWkMlZm9udmY1S1
cyW0AYkwyYBBQIHMAKGN0dHAEly93d3cnc2VnLXNvY2hhbC5icy9BQ0JUI1MwYkCCGSAQ0FbWkMlZm9udmY1S1
W9BQ0JUI1NvY2hhbC5icy9BQ0JUI1MwYkCCGSAQ0FbWkMlZm9udmY1S1
LndhY3Icy9kcmwVSRU5DSUeRUpSU5GTlNOVGRJQ0RlEjUjEzEzU0VHVVYjRlEjFNP
LHEtEtw-LwYDQODDCHURVNPVSSURBIVRORVIBICBERSBMSQSBTRUJkUkEQU0Q0U09DSUFMMTCw
NOYDQODDCHURVNPVSSURBIVRORVIBICBERSBMSQSBTRUJkUkEQU0Q0U09DSUFMMTCw
EA YDQODDCHURVNPVSSURBIVRORVIBICBERSBMSQSBTRUJkUkEQU0Q0U09DSUFMMTCw
HwYDVR0BjBggwFoA45JKFY0HlVLElY1500c75k0wHQYDR00BbEYF1K1f1k8HGFgYVc
lhaatbTMAOGCqGSIb3DQEBCwUAIAAHCACQIy11-caPGAs1TU1W0mWokZdMxAn2ORhpyYhm-K
SABV9XzBY4fEcln4473M9Kc4kMa0464G9e-FO1b-9p07M0HkVr-lEBVA-w7TKPR01
8nUwKbdrP7BwORcmwslURApLL3d0C2F4WAOdp006bYQ-ahwcyW6ivVasQZ-cQsQeYkA
9XcTDpy08Auy2RhmBRWF5HKY-0T5PzohOzO4cDK1z4nNngdlsFYW4EIT5E2wP7D9P
Q0ZSW14fU0m946WBRKzckMa0464G9e-FO1b-9p07M0HkVr-lEBVA-w7TKPR01
8nUwKbdrP7BwORcmwslURApLL3d0C2F4WAOdp006bYQ-ahwcyW6ivVasQZ-cQsQeYkA
G9PcOD9EHOPE-d0Nms-PSPBxCIJMWrgM7nKAY9msA8H+gdlb-AA009L8z-n0ZH-B
XBVdntCv1s1WagBGE7BwORcmwslURApLL3d0C2F4WAOdp006bYQ-ahwcyW6ivVasQZ-cQsQeYkA
G4afvNzXohBYxySQ3Dd0c3q6uAyhdXWlukODRr52chSccrVW6684UOmHgAC6C6C
5pcouujkTcaY+vPNETVMjuONSF8bBzWz=
-----END CERTIFICATE-----
```

Signature algorithm: SHA256withRSA

Issuer CN: RAIZ ACGISSv2

**Issuer SERIAL NUMBER:** Q2827003A

**Issuer OU:** GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL

**Issuer O:** TESORERIA GENERAL DE LA SEGURIDAD SOCIAL

**Issuer L:** MADRID

**Issuer C:** ES

**Subject CN:** SUBCA GISS01

**Subject SERIAL NUMBER:** Q2827003A

**Subject OU:** GISS01

**Subject OU:** GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL

**Subject O:** TESORERIA GENERAL DE LA SEGURIDAD SOCIAL

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Thu Jun 16 11:51:17 CEST 2016

**Valid to:** Mon Jun 16 12:21:17 CEST 2031

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A6:A3:10:CS:DC:E3:C9:EA:D6:43:47:3C:7D:17:32:2E:2B:E5:3D:53:07:C0:57:65:7E:D0:3C:C6:95:90:BD:66:F6:47:7F:49:C3:83:E3:C4:E9:FE:7E:B1:09:1A:D6:89:5F:61:46:04:2D:09:49:A1:F4:00:1F:3B:BC:07:80:94:0B:CF:27:61:82:E8:45:3C:20:09:C6:B1:88:6E:26:C9:81:34:31:D8:CE:C7:8F:85:FD:82:08:8C:97:4B:7A:2D:8E:77:CE:07:4B:E2:74:65:4E:55:99:CA:44:BC:9B:3E:37:21:C0:72:2B:88:13:FD:D3:E7:A3:A5:47:48:DF:3C:03:BB:C8:C3:60:2C:DS:1S:62:A6:3C:59:B3:2CAD:A7:E2:83:2A:71:80:E3:85:E6:AS:AB:07:AB:C7:80:2B:56:D1:58:8B:98:A8:64:69:36:72:F1:D4:CC:24:93:BE:BC:1A:21:EF:59:0A:21:E7:B4:0A:7F:8A:A7:51:E4:A2:C7:CD:3B:4A:ED:72:D9:56:5F:4E:02:0E:95:63:CA:21:BF:DF:35:A6:5F:D1:45:5B:1A:F4:95:8D:6D:8E:6D:18:89:91:09:EE:7B:85:34:8E:AC:C4:79:4C:BD:FE:EA:7A:F2:C2:C0:3C:7E:3A:74:F4:DB:2C:E9:2C:DB:AB:6E:AA:2D:1D:B9:2D:04:A2:33:A1:B3:99:BF:FE:ED:6B:55:2E:CE:29:64:38:3F:A1:0A:C4:A7:BB:3D:A8:71:05:82:E8:13:D9:55:22:4B:DD:A9:19:08:CD:7F:DB:E9:70:EF:1C:94:88:76:ED:0F:B1:64:C6:24:F9:CE:C4:BB:3D:CB:9D:E9:CA:14:BF:02:AS:ED:4E:DB:C0:2C:7E:C2:A1:06:DC:F0:02:E2:58:96:7D:12:81:8F:2F:49:39:64:2CA7:F3:3C:BA:EA:16:B4:F7:9F:DD:DE:2D:49:55:B2:0B:EE:12:84:40:D0:AD:E0:03:46:D7:B7:AC:E6:CC:A9:58:E0:6E:99:4B:F9:F2:1F:C4:56:55:95:B3:DB:6E:A9:5B:71:27:9C:AE:4B:11:23:F2:2A:7C:40:88:E2:20:F7:FC:13:2E:F3:AD:39:DC:96:29:E5:F9:66:A5:BD:6B:A0:95:52:5F:20:B4:3E:CB:1F:8E:51:62:02:D8:B5:2A:A0:42:BA:42:DB:02:4A:EA:1A:56:6A:A5:39:A1:BA:0F:EC:7C:E8:AB:FC:12:BA:DF:CF:DD:AE:C1:15:73:F9:6F:5C:66:CC:C0:09:75:46:8F:9B:46:EB:A6:0A:F2:BF:F8:F7:29:AD:87:A9:9E:6B:93:B0:75:3F:66:C4:59:7D:84:79:F6:D3:02:03:01:00:01

**Basic Constraints** IsCA: true

**Certificate Policies**  
Policy OID: 2.16.724.1.4.2.2.1  
CPS pointer: <http://www.seg-social.es/ACGISS>  
CPS text: [Certificado de la CA Subordinada GISS01 de ACGISSv2. Consulte las condiciones de uso en <http://www.seg-social.es/ACGISS>]

**Authority Info Access**  
<http://ocsp.seg-social.gob.es/>  
[http://www.seg-social.es/ACGISS/Certs/RAIZ\\_ACGISS\\_V2](http://www.seg-social.es/ACGISS/Certs/RAIZ_ACGISS_V2)

**CRL Distribution Points**  
<http://crl.seg-social.gob.es/arl.crl>  
C=ES,L=MADRID,O=TESORERIA GENERAL DE LA SEGURIDAD SOCIAL,OU=GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL,SERIALNUMBER=Q2827003A,CN=RAIZ ACGISSv2,CN=CRL1

**Authority Key Identifier** E3:78:D3:90:56:28:1E:D2:EF:2C:14:E4:62:5E:62:D3:47:3B:E6:4D

**Subject Key Identifier** 8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A9:20:D6:61:E8:D9:0D:A3:07:AB:B1:1C:AC:5E:00:FF:93:02:26:AE:B0:FE:B6:A8:81:49:C6:55:95:5B:03:E1*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2021-10-26T01:00:00Z*

#### 18.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 18.2.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

#### 18.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDA sURN ]* *urn:oid:2.16.724.1.4.2.2.1.1.2*

**Description**

#### 18.2.4 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified certificates issued by SUBCA GISS01*

**Name** *[ es ]* *Certificados reconocidos emitido por SUBCA GISS01*

### Service digital identities

#### X509SubjectName

**Subject CN:** *SUBCA GISS01*

**Subject SERIAL NUMBER:** *Q2827003A*

**Subject OU:** *GISS01*

**Subject OU:** *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

**Subject O:** *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

**Subject L:** *MADRID*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-05-03T00:00:00Z*

#### 18.2.4.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 18.2.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

#### 18.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**



**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.1.4.2.2.1.1.2

**Description****18.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates issued by SUBCA GISS01*

**Name** [ es ] *Certificados reconocidos emitido por SUBCA GISS01*

**Service digital identities****X509SubjectName**

**Subject CN:** *SUBCA GISS01*

**Subject SERIAL NUMBER:** *Q2827003A*

**Subject OU:** *GISS01*

**Subject OU:** *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

**Subject O:** *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**18.2.5.4 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [ en ] *undefined.*

[ es ] *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.1.4.2.2.1.1.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.1.4.2.2.1.1.1

**18.2.5.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**18.2.6 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified certificates issued by SUBCA GISS01*

**Name** [ es ] *Certificados reconocidos emitido por SUBCA GISS01*

**Service digital identities****X509SubjectName**

**Subject CN:** *SUBCA GISS01*

**Subject SERIAL NUMBER:** *Q2827003A*

**Subject OU:** *GISS01*

**Subject OU:** *GERENCIA DE INFORMATICA DE LA SEGURIDAD SOCIAL*

**Subject O:** *TESORERIA GENERAL DE LA SEGURIDAD SOCIAL*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *jUrV/XKSPwcaEV/NgKrWGhp/9tM=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2016-06-23T22:00:00Z

**18.2.6.6 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:2.16.724.1.4.2.2.1.1.2

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:2.16.724.1.4.2.2.1.1.1

**18.3 - Service (withdrawn): Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

**Service Name**

**Name** [en] Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

**Name** [es] Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 1466133214



**Certificate Policies**

Policy OID: 2.16.724.1.4.2.2.1.3.1

CPS pointer: <http://www.seg-social.es/ACGISS>CPS text: [Certificado de sellado de tiempo. Consulte las condiciones de uso en <http://www.seg-social.es/ACGISS> ]**Issuer Alternative Name**

rfc822Name=acgiss.soporte.giss@seg-social.es

**CRL Distribution Points**[http://crl.seg-social.gob.es/ac\\_sub.crl](http://crl.seg-social.gob.es/ac_sub.crl)**Authority Key Identifier**

8D:4A:D5:FD:72:92:3F:07:1A:11:5F:CD:80:AA:D6:1A:1A:7F:F6:D3

**Subject Key Identifier**

AA:26:8A:14:04:12:83:80:5A:6F:72:54:CE:53:AE:71:3B:1B:BC:5F

**Basic Constraints**

IsCA: false

**Key Usage:**

digitalSignature - nonRepudiation

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

EB:A2:BD:4B:A5:BD:CA:E7:73:A4:BA:EF:9E:59:74:83:AA:97:20:C2:5D:7C:AF:C7:4A:22:C4:DA:9A:76:02:09

**X509SubjectName****Subject SERIAL NUMBER:**

S2819001E+2.5.4.97

**Subject OU:**

SERVICIOS DE CONFIANZA

**Subject O:**

SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL

**Subject C:**

ES

**X509SKI****X509 SK I**

qiaKFAQSg4Bab3JUzlOucTsbvF8=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2021-10-26T01:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**URI**

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**18.3.1 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

**Name** [*en*] *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

**Name** [*es*] *Qualified timestamps issued by TSA AUTORIDAD DE SELLADO DE TIEMPO*

**Service digital identities****X509SubjectName**

**Subject SERIAL NUMBER:** *S2819001E+2.5.4.97*

**Subject OU:** *SERVICIOS DE CONFIANZA*

**Subject O:** *SECRETARIA DE ESTADO DE LA SEGURIDAD SOCIAL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *qiaKFAQSg4Bab3JUzlOucTsbvF8=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2018-05-03T00:00:00Z*

**19 - TSP: Ministerio de Empleo y Seguridad Social****TSP Name**

**Name** [ en ] *Ministerio de Empleo y Seguridad Social*

**Name** [ es ] *Ministerio de Empleo y Seguridad Social*

**TSP Trade Name**

**Name** [ en ] *Ministerio de Empleo y Seguridad Social*

**Name** [ es ] *Ministerio de Empleo y Seguridad Social*

**Name** [ en ] *Ministerio de Trabajo e Inmigracion*

**Name** [ es ] *Ministerio de Trabajo e Inmigracion*

**Name** [ en ] *VATES-S2819001E*

**Name** [ en ] *MINISTERIO DE TRABAJO E INMIGRACION*

**Name** [ en ] *MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL*

**PostalAddress**

**Street Address** [ en ] *Paseo de la Castellana, 63*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28071*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Paseo de la Castellana, 63*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28071*

**Country Name** [ es ] *ES*

**ElectronicAddress**





**Issuer L:** MADRID

**Issuer O:** MINISTERIO DE TRABAJO E INMIGRACION

**Issuer OU:** SUBDIRECCION GENERAL DE PROCESO DE DATOS

**Issuer OU:** PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN

**Issuer SERIAL NUMBER:** S2819001E

**Issuer CN:** AC1 RAIZ MTIN

**Subject C:** ES

**Subject L:** MADRID

**Subject O:** MINISTERIO DE TRABAJO E INMIGRACION

**Subject OU:** SUBDIRECCION GENERAL DE PROCESO DE DATOS

**Subject OU:** PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN

**Subject SERIAL NUMBER:** S2819001E

**Subject CN:** AC1 RAIZ MTIN

**Valid from:** Thu Nov 05 17:17:45 CET 2009

**Valid to:** Sun Nov 03 17:17:45 CET 2019

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100DC.CD.CD.B1.BF.DE.25.F5.FF.IC.33.73.99.3C.1B.A1.6D.F5.A0.C4.7D.9B.38.66.8D.09.DF.03.6C.57.35.B4.13.41.FE.E3.5F.E6.22.04.58.18.89.4E.69.33.04.3F.95.C7.D9.AE.FF.33.3A.A3.32.40.32.93.57.FE.81.AF.25.43.3C.1D.FB.7B.57.0B.62.08.67.67.62.B4.E3.E5.58.28.80.E6.AA.86.C2.40.E7.4F.10.61.29.69.26.AB.4D.7C.A1.AB.5.B.61.31.81.06.6A.64.94.4D.27.F8.4B.1E.D1.D5.43.E2.D7.B1.6D.F6.F6.FE.B4.70.55.F6.08.99.B7.74.01.E0.F3.9E.B5.7C.E4.04.88.08.50.59.78.1F.1A.94.DB.EF.C8.C9.89.D3.37.B8.F3.3D.86.D1.19.CB.83.5A.10.07.08.4F.99.74.02.07.F0.32.51.C8.FB.E6.D0.3C.26.76.7D.72.7E.AC.76.37.C1.8A.75.20.5C.40.DC.84.3F.D0.49.7C.4D.67.AE.39.EF.E4.CE.80.E1.CA.9D.E6.2D.AB.2E.E6.12.95.DA.F9.FB.DF.E3.E2.8C.3D.87.FB.45.6E.4A.AB.F.6.78.92.27.14.A1.5D.6B.4F.70.7B.57.73.EF.F9.3D.A8.0E.75.9F.EF.11.80.19.84.B0.64.40.EE.D8.A9.86.FA.A5.D7.45.F4.11.6F.F7.86.C8.34.5B.88.68.CE.BA.DD.CD.9B.DD.88.EE.01.36.E8.AC.6A.E8.12.0B.80.E0.7B.90.1E.85.0B.49.89.01.F6.FF.82.DE.58.65.22.83.48.D6.07.D0.1C.66.FC.66.28.3A.C4.C3.E5.F8.99.65.27.52.58.F3.6B.F1.6F.02.44.84.75.D0.A4.E3.68.53.61.72.EF.F6.2F.A9.B3.AC.F5.F4.F6.D0.5C.DC.69.4C.CC.79.D2.A4.1B.C8.73.06.34.74.B4.F1.6A.CA.29.28.C7.34.84.5B.23.D8.BA.00.8C.CC.09.C1.C7.6F.5D.04.AB.B7.4F.26.77.A9.35.CF.20.D6.B3.FF.31.69.D0.34.FB.25.EC.68.96.0A.A2.DD.83.1F.CA.3C.8F.74.36.28.54.EF.F5.18.7B.C.2.84.31.D1.FB.82.04.AE.04.82.D6.F5.02.29.71.E1.92.71.74.8E.DB.AA.71.1D.C4.3B.C6.62.26.6C.86.3C.23.55.EB.29.D1.1F.AB.CA.1E.63.E7.B3.73.B4.A7.B8.2A.3A.F6.1F.FB.87.65.88.FC.F3.9F.FE.BF.EB.D5.1D.B6.A.8.03.E9.63.83.19.8C.E0.18.ED.17.D8.1C.0D.3D.9C.8A.58.7F.02.03.01.00.01

**Basic Constraints** IsCA: true

**Subject Key Identifier** 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83

**Authority Info Access** <http://ca.mtin.es/mtin/ocsp>

**CRL Distribution Points** <http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz>  
<http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz>

**Certificate Policies** Policy OID: 1.3.6.1.4.1.27781.2.4.1  
CPS pointer: <http://ca.mtin.es/mtin/DPCyPoliticass>  
CPS text: [Certificado raíz. Consulte las condiciones de uso en <http://ca.mtin.es/mtin/DPCyPoliticass>]

**Authority Key Identifier** 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83

**Issuer Alternative Name** admin\_ca@mtin.es



**Subject OU:** SUBDIRECCION GENERAL DE PROCESO DE DATOS

**Subject OU:** PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN

**Subject SERIAL NUMBER:** S2819001E

**Subject CN:** AC1 RAIZ MTIN

**Valid from:** Thu Nov 05 17:17:45 CET 2009

**Valid to:** Sun Nov 03 17:17:45 CET 2019

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100DCCD0B1BFDE25F5FF1C3373993C1B A16D F5A0C47D9B38668D09DF036C5735B41341  
FE E35F E622045818B94E6933043F95C7D94E FF3334A7324032037FE31AF25435C1D FD7B570B620867676294E3E5582580E6AA866C240E74F1061294926AB4D7CA1AB5  
B613181066A64944D27F84B1E1D1D543E2D7B16DF6F6FFB47055F60899B77401EDF39EB57CE40488085059781F1A94DBFFC8C989D337B8F3D86D119CB835A1007084F  
99740207F03251C8FB E6D03C26767D727EAC7637C18A78205C40DC843FD0497C4D67AE39EF E4CE80E1CA9D E62DAB2E E61295DA F9FBDF E3E28C3D87FB456E44ABF  
678922714A15D56B4E707B5773EF F95DAB0F759FEF11801984B0640EEDE A986FAA5D745F4116FF186C8345B8848CEBA DD CD9BDD88E30136E8AC6A E8120B80E07B90  
1E850B498901F6FF82DF5865228348D607D01C66FC66283AC4C3E5F89965275258F36B F16F02448475D0A4E368536172EF F62FA9B3ACF5F4F6D05CD694CC79D2A4  
1B C873063474B4F16ACA2928C734845B23D8BA008CC09C1C76F5D04AB B74F2677A935CF20D6B3FF3169D034FB25EC68960AA2DD831FCA3C8F74362554E F5187B C  
22431D1FB8204AE0482D6F5022971E39271748E DBAA71DDC43BC662266C863C2355EB29D11FABCA1E63E7B373B4A7B82A3AF61FB876588FCF39FEFBFB51DB6A  
803E96583198CE018ED17D81C0D3D9CA587E0203010001

**Authority Info Access** <http://ca.mtin.es/mtin/ocsp>

**Subject Alternative Name** [admin\\_ca@mtin.es](mailto:admin_ca@mtin.es)

**Issuer Alternative Name** [admin\\_ca@mtin.es](mailto:admin_ca@mtin.es)

**Basic Constraints** *IsCA: true*

**CRL Distribution Points**  
<http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz>  
<http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.27781.2.4.1  
CPS pointer: <http://ca.mtin.es/mtin/DPCyPolitic>  
CPS text: [Certificado raiz. Consulte las condiciones de uso en <http://ca.mtin.es/mtin/DPCyPolitic>]

**Subject Key Identifier** 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83

**Authority Key Identifier** 33:43:18:B3:C4:4B:1D:CB:1F:F9:F0:4E:FC:DF:4A:E4:15:60:C8:83

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 5B:1D:9D:24:DE:0A:FE:A8:B3:5B:A0:4A:1C:3E:25:D0:81:2C:DF:7C:46:25:DE:0A:89:AF:9F:E4:BB:D1:BB:15

**X509SubjectName**

**Subject C:** ES

**Subject L:** MADRID

**Subject O:** MINISTERIO DE TRABAJO E INMIGRACION

**Subject OU:** *SUBDIRECCION GENERAL DE PROCESO DE DATOS*

**Subject OU:** *PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*

**Subject SERIAL NUMBER:** *S2819001E*

**Subject CN:** *AC1 RAIZ MTIN*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2018-05-07T00:00:00Z*

#### **Scheme Service Definition URI**

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

#### **19.1.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

##### **Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

#### **19.1.2 - Extension (critical): additionalServiceInformation**

##### **AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### **19.1.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** [es] *Certificados Reconocidos emitidos por la AC1 RAIZ MTIN*

**Name** [en] *Qualified Certificates issued by AC1 RAIZ MTIN*

### Service digital identities

#### X509SubjectName

**Subject C:** *ES*

**Subject L:** *MADRID*

**Subject O:** *MINISTERIO DE TRABAJO E INMIGRACION*

**Subject OU:** *SUBDIRECCION GENERAL DE PROCESO DE DATOS*

**Subject OU:** *PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN*

**Subject SERIAL NUMBER:** *S2819001E*

**Subject CN:** *AC1 RAIZ MTIN*

#### X509SKI

**X509 SK I** *M0MYs8RLHcsf+fBO/N9K5BVgyIM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 19.1.3.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.2*

##### **Policy Identifier:**

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.27781.2.4.3.2.3*

#### 19.1.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**19.1.4 - History instance n.2 - Status: undersupervision****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [ es ] *Certificados Reconocidos emitidos por la AC1 RAIZ MTIN***Name** [ en ] *Qualified Certificates issued by AC1 RAIZ MTIN***Service digital identities****X509SubjectName****Subject C:** ES**Subject L:** MADRID**Subject O:** MINISTERIO DE TRABAJO E INMIGRACION**Subject OU:** SUBDIRECCION GENERAL DE PROCESO DE DATOS**Subject OU:** PRESTADOR DE SERVICIOS DE CERTIFICACION MTIN**Subject SERIAL NUMBER:** S2819001E**Subject CN:** AC1 RAIZ MTIN**X509SKI****X509 SK I** M0MYs8RLHcsf+fBO/N9K5BVgyIM=**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>**Status Starting Time** 2010-12-21T00:00:00Z**19.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[ en ]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[ es ]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne**



**Issuer SERIAL NUMBER:** S2819001E

**Issuer OU:** PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Issuer OU:** S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Issuer O:** MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Issuer L:** MADRID

**Issuer C:** ES

**Subject CN:** SUBCA1 MEYSS

**Subject 2.5.4.97:** VATES-S2819001E

**Subject SERIAL NUMBER:** S2819001E

**Subject OU:** PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Subject OU:** S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Subject O:** MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Fri Dec 02 12:26:29 CET 2016

**Valid to:** Tue Dec 02 12:56:29 CET 2036

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D130CF7E14831857E9FA178D36A08FD4179BF6E50EA733D472BA523FCBA6E100647FF  
A9B2A5139633E262072DC7E142C7C8D8EF866523EE1F4F051B0259F3259B1D49F311643ED78E7FCBC4390F07A1057B771185370936D358C6226828C479E03E046C29E  
963D075A1B30F05FEDFF7A19CCDC2E82AC33D04812251F6DA325D9D6BD23438B8D637D8F8DDA8B726FAF651CB158B4D5E6C99DB98FD8C0521AC52A6B83066554A6  
176907E9C3E1A4AFD3784B895CA0A4B47098B4D5CE11502F62607BD8F91E0D74164739CE897527DA4B8F39C52C5D0B57C7CF46A081EFC2A162A0071D038180  
EAS807A0E8BE81ED6689948D037D4A31C9F680EF4846BE053B5D993FA1057B7507DC489E3976AA4601350C194923727E472E6B64DFAD82D878F033C6C82E4369FC  
AC8CAF7B954CB67AF32F169473B8C11A57B3DE8C66D2EFAE90BCD1D539DC2A4E5CF15385963F8681571E2D7FCB954EBE7A1584D1A396FC436CFCF437A9E3866A5  
AD97CEBE051D8E32A14D4EA46DDCFA9F332502D4FB3817D47831AB0A732CE32F1582A5BEA4090DD9D9A23E103AE95C4906F49BDB0E5D05E3750D0F5193D06791  
54A30CFD5CBA4CF664E8C7CB561800889AD9CC2A12F63AB49CEA87E1648F9DF6F7B1F9918F92D4D7686132683FA4A37C447001B272535A227ACEA59EB977001A8  
87A351CA84D1DE358400A7B77AB9222F4F869F030D750203010001

**Basic Constraints** IsCA: true

**Authority Info Access**  
<http://ca.empleo.gob.es/meyss/ocsp>  
<http://ca.empleo.gob.es/meyss/certificados>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.27781.2.5.1.1  
CPS pointer: <http://ca.empleo.gob.es/meyss/DPCyPoliticass>  
CPS text: [Certificado de AC Subordinada SUBCA1 MEYSS. Consulte las condiciones de uso en <http://ca.empleo.gob.es/meyss/DPCyPoliticass>]



**CRL Distribution Points**<http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz><http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz>

*C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1*

**Authority Key Identifier**

7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71

**Subject Key Identifier**

9E:8B:1D:B3:FA:07:2B:81:D7:EA:59:E8:B9:69:F7:9D:B5:48:02:E2

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

24:E0:BA:DA:DA:29:05:5C:66:22:CA:23:74:A2:28:A4:71:A4:D2:4C:2D:54:71:88:E3:8F:07:1A:9D:14:60:88

**X509SubjectName****Subject CN:**

SUBCA1 MEYSS

**Subject 2.5.4.97:**

VATES-S2819001E

**Subject SERIAL NUMBER:**

S2819001E

**Subject OU:**

PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Subject OU:**

S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Subject O:**

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Subject L:**

MADRID

**Subject C:**

ES

**X509SKI****X509 SK I**

nosds/oHK4HX6lnouWn3nbVIAuI=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-03-28T00:00:00Z

**19.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 19.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 19.2.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [ en ] SUBCA1 MEYSS

Name [ es ] SUBCA1 MEYSS

#### Service digital identities

##### X509SubjectName

Subject CN: SUBCA1 MEYSS

Subject 2.5.4.97: VATES-S2819001E

Subject SERIAL NUMBER: S2819001E

Subject OU: PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

Subject OU: S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Subject O: MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

##### X509SKI

X509 SK I <nosds/oHK4HX6lnouWn3nbVIAuI=>

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-05-07T00:00:00Z

**19.2.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**19.2.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**19.2.4 - History instance n.2 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

Name	[ en ]	SUBCA1 MEYSS
------	--------	--------------

Name	[ es ]	SUBCA1 MEYSS
------	--------	--------------

**Service digital identities****X509SubjectName**

Subject CN:	SUBCA1 MEYSS
-------------	--------------

Subject 2.5.4.97:	VATES-S2819001E
-------------------	-----------------

Subject SERIAL NUMBER:	S2819001E
------------------------	-----------

Subject OU:	PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS
-------------	---

Subject OU:	S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
-------------	--

Subject O:	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
------------	---

Subject L:	MADRID
------------	--------

Subject C:	ES
------------	----

**X509SKI**

X509 SK I	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">nosds/oHK4HX6lnouWn3nbVIAuI=</a>
-----------	--

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---



**Issuer 2.5.4.97:** VATES-S2819001E

**Issuer SERIAL NUMBER:** S2819001E

**Issuer OU:** PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Issuer OU:** S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Issuer O:** MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Issuer L:** MADRID

**Issuer C:** ES

**Subject CN:** SUBCA2 MEYSS

**Subject 2.5.4.97:** VATES-S2819001E

**Subject SERIAL NUMBER:** S2819001E

**Subject OU:** PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Subject OU:** S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Subject O:** MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Fri Dec 02 12:52:49 CET 2016

**Valid to:** Tue Dec 02 13:22:49 CET 2036

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A626656A15BD46DC EEAA D01A0CEE D92120DA B628189E842067607D5E773E CF4E8E9B  
282AE170412CA77D12C0FAA771A515B1665A53B80A9489E4C07C36CB88F378011A51F4F220AF E5C7E28B0B12EEAE7CBB071B704167B5F6FBDA B5277494465048C0  
55AC43AD8E24628A9042CS06D4EF5317320F12F66695944241E52C449DD1754701FEE1C609731BF0D4E52C00CDAB8CSCD2D9F10651156233A8184E65D61919EC E3CB  
2FD5F6055B3990C4DC0E5F048C5C86DF5B3FAAC06711E3D30690DD559448E695CE29ACFD05B310F954F741DE44755ACB11AC3C476B7907275C404E CD0E B20F97125  
E491D79C2A029AAE251E24D40E52A717C560C88C33382E91698274AB2E40B4CE7615095094A919511608489A942A9567CD129582D86D3CABA1DE2240E2C030C5B6E2  
16826FD580D756BD67E91B0DA46007180E360621522945A9AD07E B2208F4748BA1CF0B955B67E1895895AD558BA236E4ECF73092B927485F303600F3AD8E1A81B4EA E4  
EB9958583C92241B390AEB8781D7479E4B21F11284878CN77A28A8366FA923D2FF209A93BCF5A3D540040A302B1727599919F61E6BEA0D37AD17F243F05017D51E2  
86E8A94A94D34CA9C11934F3F2476B46AC9D8AA1581E FF CB B11D25EF86A1BC4DE5D9FC218D8BDA4C586830854876A57D9FCA72D9F381D432D607E21D179C3E  
10E7A620C182EA62A7E2934B74064457D114E90203010001

**Basic Constraints** IsCA: true

**Authority Info Access**  
<http://ca.empleo.gob.es/meyss/ocsp>  
<http://ca.empleo.gob.es/meyss/certificados>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.27781.2.5.1.2  
CPS pointer: <http://ca.empleo.gob.es/meyss/DPCyPolíticas>  
CPS text: [Certificado de AC Subordinada SUBCA2 MEYSS. Consulte las condiciones de uso en <http://ca.empleo.gob.es/meyss/DPCyPolíticas>]

**CRL Distribution Points**<http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz><http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz>

*C=ES,L=MADRID,O=MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL,OU=S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES,OU=PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS,SERIALNUMBER=S2819001E,2.5.4.97=VATES-S2819001E,CN=AC RAIZ MEYSS,CN=CRL1*

**Authority Key Identifier**

7F:B7:2D:F2:2E:B6:0F:AC:05:38:A7:63:2F:D6:3F:4F:0E:1A:F5:71

**Subject Key Identifier**

72:2D:90:3D:45:86:98:6C:9D:E3:89:F6:E0:E4:3D:77:CC:FD:96:02

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

18:70:4F:60:CC:F3:59:4C:89:9A:DA:8B:E4:D4:D3:D3:7D:AA:8F:38:A5:FC:B0:61:FA:D8:D6:B1:A9:F5:6E:0B

**X509SubjectName****Subject CN:**

SUBCA2 MEYSS

**Subject 2.5.4.97:**

VATES-S2819001E

**Subject SERIAL NUMBER:**

S2819001E

**Subject OU:**

PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

**Subject OU:**

S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

**Subject O:**

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

**Subject L:**

MADRID

**Subject C:**

ES

**X509SKI****X509 SK I**

ci2QPUWGmGyd44n24OQ9d8z9lgI=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-03-28T00:00:00Z

**19.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 19.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 19.3.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [ en ] SUBCA2 MEYSS

Name [ es ] SUBCA2 MEYSS

#### Service digital identities

##### X509SubjectName

Subject CN: SUBCA2 MEYSS

Subject 2.5.4.97: VATES-S2819001E

Subject SERIAL NUMBER: S2819001E

Subject OU: PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS

Subject OU: S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Subject O: MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Subject L: MADRID

Subject C: ES

##### X509SKI

X509 SK I [ci2QPUWGmGyd44n24OQ9d8z9lgI=](http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted)

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2018-05-07T00:00:00Z

**19.3.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**19.3.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**19.3.4 - History instance n.2 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

Name	[ en ]	SUBCA2 MEYSS
------	--------	--------------

Name	[ es ]	SUBCA2 MEYSS
------	--------	--------------

**Service digital identities****X509SubjectName**

Subject CN:	SUBCA2 MEYSS
-------------	--------------

Subject 2.5.4.97:	VATES-S2819001E
-------------------	-----------------

Subject SERIAL NUMBER:	S2819001E
------------------------	-----------

Subject OU:	PRESTADOR DE SERVICIOS DE CONFIANZA MEYSS
-------------	---

Subject OU:	S.G. DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
-------------	--

Subject O:	MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
------------	---

Subject L:	MADRID
------------	--------

Subject C:	ES
------------	----

**X509SKI**

X509 SK I	ci2QPUWGmGyd44n24OQ9d8z9lgI=
-----------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---



Status Starting Time

2017-04-11T00:00:00Z

**19.3.4.3 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

URI

[ en ]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**20 - TSP: Consejo General de Colegios Oficiales de Médicos****TSP Name**

<b>Name</b>	[ en ]	<i>Consejo General de Colegios Oficiales de Médicos</i>
<b>Name</b>	[ es ]	<i>Consejo General de Colegios Oficiales de Médicos de España (CGCOM)</i>

**TSP Trade Name**

<b>Name</b>	[ en ]	<i>Entidad de Certificación de la Organización Médica Colegial (EC-OMC)</i>
<b>Name</b>	[ es ]	<i>Entidad de Certificación de la Organización Médica Colegial (EC-OMC)</i>
<b>Name</b>	[ en ]	<i>Organizacion Medica Colegial</i>
<b>Name</b>	[ es ]	<i>Organizacion Medica Colegial</i>
<b>Name</b>	[ en ]	<i>VATES-Q2866017C</i>
<b>Name</b>	[ en ]	<i>ORGANIZACION MEDICA COLEGIAL</i>
<b>Name</b>	[ en ]	<i>CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS</i>

**PostalAddress**

<b>Street Address</b>	[ es ]	<i>Plaza de las Cortes, 11</i>
<b>Locality</b>	[ es ]	<i>Madrid</i>
<b>State Or Province</b>	[ es ]	<i>Madrid</i>
<b>Postal Code</b>	[ es ]	<i>28014</i>
<b>Country Name</b>	[ es ]	<i>ES</i>

**PostalAddress**

<b>Street Address</b>	[ en ]	<i>Plaza de las Cortes, 11</i>
<b>Locality</b>	[ en ]	<i>Madrid</i>
<b>State Or Province</b>	[ en ]	<i>Madrid</i>
<b>Postal Code</b>	[ en ]	<i>28014</i>
<b>Country Name</b>	[ en ]	<i>ES</i>

**ElectronicAddress**



**Issuer O:** *VeriSign, Inc.*

**Issuer C:** *US*

**Subject CN:** *OMC*

**Subject OU:** *Class 2 Managed PKI Individual Subscriber CA*

**Subject OU:** *Entidad de Certificacion*

**Subject OU:** *VeriSign Trust Network*

**Subject O:** *Organizacion Medica Colegial*

**Subject C:** *ES*

**Valid from:** *Fri Jan 26 01:00:00 CET 2007*

**Valid to:** *Thu Jan 26 00:59:59 CET 2017*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C87C2B1A62694919FEFE7621D5D63E3B037696DFEEF0BFCS14807F14F75B21481A6F32  
39246CD7F6906A04941A757AD1C42D0C36E4690B382D70B681B58827424C625712B67F15F30727B70D3C51089A4DF28D390DE35FE1B6182684F332848A5A79718F4  
2780BF4222A396283AA2A1F1B1CD2E0987ECF7BF4856152580E16B7DC557037B4B267968E4D1549E96AE DA1C98639D8D109CE9FA D83E03DB3E786CCE025F12387  
414AF C1277CA81808757E36754E73739934FC447D1B23E299DE1950DD B082921B5514E5A520DC98FB C4F835834554EE65484D5F7A7850770E6FBF89611845D071A24F  
4A08247FF56E92BF B19C48E021A2AA742683400B0D BA AF0203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Certificate Policies**  
*Policy OID: 2.16.840.1.113733.1.7.23.2*  
*CPS pointer: <https://www.verisign.com/rpa>*

**CRL Distribution Points** *<http://crl.verisign.com/pca2-g2.crl>*

**Subject Alternative Name** *CN=PrivateLabel4-2048-4*

**Subject Key Identifier** *D3:58:FC:F2:2F:B6:F5:BC:D0:DC:27:19:3E:AA:3C:69:29:88:99:76*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A4:8A:6D:DD:5D:D5:5C:AF:68:CC:AA:E0:A5:98:97:9C:AE:35:BF:D3:AC:6E:20:B5:11:FA:A7:8  
7:4F:BF:B6:92*

**Certificate fields details**

**Version:** *3*

**Serial Number:** *35019734869110279053858484427741191449*



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *6B:15:6A:E6:9A:C3:76:29:C4:4B:A2:66:57:AE:ED:3B:7D:FE:E9:5F:F3:61:51:6D:97:55:A9:55:6B:CE:4F:52*

**X509SubjectName**

**Subject CN:** *OMC*

**Subject OU:** *Class 2 Managed PKI Individual Subscriber CA*

**Subject OU:** *Entidad de Certificacion*

**Subject OU:** *VeriSign Trust Network*

**Subject O:** *Organizacion Medica Colegial*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2018-07-16T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**20.1.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.5*

**20.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**20.1.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by AC EC-OMC*

**Name** [ es ] *Certificados Reconocidos emitidos por AC EC-OMC*

**Service digital identities****X509SubjectName**

**Subject CN:** *OMC*

**Subject OU:** *Class 2 Managed PKI Individual Subscriber CA*

**Subject OU:** *Entidad de Certificacion*

**Subject OU:** *VeriSign Trust Network*

**Subject O:** *Organizacion Medica Colegial*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *01j88i+29bzQ3CcZPqo8aSmImXY=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**20.1.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [ en ] *undefined.*

[ es ] *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.5

### 20.1.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 20.1.4 - History instance n.2 - Status: supervisionincessation

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### **Service Name**

**Name** [ en ] *Qualified Certificates issued by AC EC-OMC*

**Name** [ es ] *Certificados Reconocidos emitidos por AC EC-OMC*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *OMC*

**Subject OU:** *Class 2 Managed PKI Individual Subscriber CA*

**Subject OU:** *Entidad de Certificacion*

**Subject OU:** *VeriSign Trust Network*

**Subject O:** *Organizacion Medica Colegial*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *01j88i+29bzQ3CcZPqo8aSmImXY=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

**Status Starting Time** *2016-03-31T22:00:00Z*



**20.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.26852.1.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.26852.1.1.5

**20.1.5 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified Certificates issued by AC EC-OMC

**Name** [es] Certificados Reconocidos emitidos por AC EC-OMC

**Service digital identities****X509SubjectName**

**Subject CN:** OMC

**Subject OU:** Class 2 Managed PKI Individual Subscriber CA

**Subject OU:** Entidad de Certificacion

**Subject OU:** VeriSign Trust Network

**Subject O:** Organizacion Medica Colegial

**Subject C:** ES

**X509SKI**

**X509 SK I** 01j88i+29bzQ3CcZPqo8aSmImXY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2011-01-27T00:00:00Z

#### 20.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.26852.1.1.3

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.26852.1.1.5

#### 20.2 - Service (withdrawn): Qualified Certificates issued by AC OMC (new CA)

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [en] Qualified Certificates issued by AC OMC (new CA)

**Name** [es] Certificados Reconocidos emitidos por AC OMC (Nueva AC)

#### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 484251359877222014



**Extended Key Usage** *id\_kp\_clientAuth - id\_kp\_OCSPSigning*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: https://policy.camerfirma.com*

**CRL Distribution Points** *http://crl.camerfirma.com/ac\_camerfirma-2009.crl*  
*http://crl1.camerfirma.com/ac\_camerfirma-2009.crl*

**Subject Alternative Name** *certificacion@cgcom.es*  
*CN=CONSEJO GENERAL DE COLEGIOS DE MÃDICOS DE ESPAÑA, SERIALNUMBER=Q2866017C, STREET=PLAZA DE LAS CORTES 11, OID.2.5.4.17=28014, L=MADRID, ST=MADRID, C=ES*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *C1:76:11:DB:7B:31:13:61:E2:0D:7B:82:31:AA:DF:47:8B:CB:7F:FA:0B:E5:85:C0:6D:E2:30:92:23:C2:EF:8A*

**X509SubjectName**

**Subject CN:** *OMC*

**Subject OU:** *ENTIDAD DE CERTIFICACION*

**Subject O:** *ORGANIZACION MEDICA COLEGIAL*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time***2021-01-26T01:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**20.2.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.5

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3.2

**20.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**20.2.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**20.2.4 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by AC OMC (new CA)*

**Name** [ es ] *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

**Service digital identities****X509SubjectName**

**Subject CN:** OMC

**Subject OU:** ENTIDAD DE CERTIFICACION

**Subject O:** ORGANIZACION MEDICA COLEGIAL

**Subject C:** ES

**X509SKI**

**X509 SK I** *52QVZL6nNb73Ok7PLT4HC7dePys=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-07-16T00:00:00Z*

**20.2.4.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.5*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

**20.2.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**20.2.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**20.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ] Qualified Certificates issued by AC OMC (new CA)*

**Name** [es] *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

### Service digital identities

#### X509SubjectName

**Subject CN:** *OMC*

**Subject OU:** *ENTIDAD DE CERTIFICACION*

**Subject O:** *ORGANIZACION MEDICA COLEGIAL*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *52QVZL6nNb73Ok7PLT4HC7dePys=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

#### 20.2.5.4 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] *undefined.*

[es] *undefined.*

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.5*

##### Policy Identifier:

**Identifier** [OIDAsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.3.2*

#### 20.2.5.5 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**20.2.6 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by AC OMC (new CA)*

**Name** *[ es ]* *Certificados Reconocidos emitidos por AC OMC (Nueva AC)*

**Service digital identities****X509SubjectName**

**Subject CN:** *OMC*

**Subject OU:** *ENTIDAD DE CERTIFICACION*

**Subject O:** *ORGANIZACION MEDICA COLEGIAL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *52QVZL6nNb73Ok7PLT4HC7dePys=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2016-03-31T22:00:00Z*

**20.2.6.6 - Extension (not critical): Qualifiers [QCForLegalPerson]**

**Qualifier type description** *[ en ]* *it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.*

*[ es ]* *está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.26852.1.1.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.26852.1.1.5*





**Issuer C:** ES

**Subject CN:** CGCOM QUALIFIED 2020

**Subject O:** CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

**Subject OU:** ENTIDAD DE CERTIFICACION

**Subject 2.5.4.97:** VATES-Q2866017C

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Valid from:** Mon Mar 02 11:41:18 CET 2020

**Valid to:** Wed Mar 02 11:41:18 CET 2033

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:A4:EE:FB:A9:0A:E7:0B:51:CD:12:AD:4B:4A:EB:10:43:2C:E1:37:F4:F9:3D:33:28:67:9E:7B:BF:03:66:01:82:BA:31:87:4F:03:DE:4A:AF:E7:4B:7E:F1:20:12:27:72:BB:DB:83:AB:B3:18:D9:04:C2:C5:A7:3C:07:AD:76:38:66:0B:99:7B:8D:10:27:BD:9A:CC:E5:EA:30:02:FD:93:29:86:41:12:62:65:42:FA:06:60:AA:BA:13:77:4B:04:2B:CD:AF:2F:C6:52:94:09:F3:70:B3:2A:85:F0:C2:28:BB:93:6B:SD:15:84:44:FB:9F:98:70:EB:86:1D:24:7C:B6:B4:72:72:1E:59:9D:D6:80:26:59:68:0C:01:5A:AF:09:C3:D1:B7:B8:77:21:51:FA:72:D0:C3:42:8B:20:18:05:48:12:E0:3D:AFA9:C7:C4:2F:B6:97:9C:EA:01:CD:56:26:2E:21:0F:D5:CB:09:88:97:EC:84:4F:50:FE:3E:DB:02:E0:E6:30:B5:74:9F:BB:6A:6F:70:FB:FE:B0:92:E5:02:23:EC:BC:D9:D6:7D:14:D3:DE:65:5E:27:2B:3B:2E:11:CF:2D:CD:15:EB:AA:0C:44:ED:F0:D7:F6:C5:BA:FB:33:AE:EC:B3:ED:44:D2:17:80:34:16:F4:01:DE:6D:0A:A1:0C:0B:08:86:9B:5E:30:D0:DB:9C:8E:92:63:28:A5:00:1F:B1:5B:D4:55:4D:AE:DF:39:FB:84:A4:FB:E7:78:FE:F0:87:C7:8E:6F:CD:6E:CD:42:9B:7E:7D:B3:4F:24:BB:6E:9E:67:86:AB:EB:21:CC:BF:D7:62:5B:C1:7B:2B:D0:67:80:D1:4B:1B:A6:22:52:75:D4:58:F6:63:1F:4F:FE:C7:40:6C:62:4D:8E:31:A9:3A:8B:EB:A7:CE:34:31:5C:CA:8E:CF:06:9BA6:25:5D:2B:21:A3:3E:01:BS:E4:5F:3D:F1:8F:E9:4E:00:4E:3C:59:5E:5C:70:66:85:2A:25:5E:A6:C5:E3:50:C5:08:D7:78:26:CC:18:F1:53:02:45:8F:2B:66:86:F1:6D:7E:15:23:92:97:86:F9:3F:F3:32:37:0E:B9:2B:1B:72:16:46:A6:DA:55:48:4D:19:1F:4E:CF:AF:DA:A7:6A:93:06:EA:DS:63:59:03:19:12:79:0C:C9:2F:1F:DD:3A:9E:B6:5B:48:F3:C9:91:F0:99:29:FF:40:49:74:3C:67:27:65:6C:62:9A:8F:A8:70:32:ED:32:E0:2A:15:CA:3C:BC:CA:34:01:BB:E6:15:59:A7:BF:DC:35:26:2D:BF:6D:12:8B:D0:BD:B4:C4:0A:10:CF:02:03:01:00:01

**Authority Key Identifier** D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0

**Subject Key Identifier** 32:41:64:94:D4:2D:41:3A:CD:EB:2B:72:09:EB:AB:8D:88:3A:D1:CF

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.vincasign.net>  
 CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

**Subject Alternative Name** info@vincasign.net

**CRL Distribution Points**  
<http://crl3.vincasign.net/casub.crl>  
<http://crl4.vincasign.net/casub.crl>

**Authority Info Access** <http://www.vincasign.net/publickeys/caqualified.cer>

**Basic Constraints** IsCA: true - Path length: 1

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 6E:8A:B9:A7:28:5D:70:EF:22:FC:7D:23:75:83:8D:65:3B:64:87:48:81:7A:80:63:4B:0C:1A:F1:04:3C:D3:66

X509SubjectName

Subject CN: CGCOM QUALIFIED 2020

Subject O: CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Subject OU: ENTIDAD DE CERTIFICACION

Subject 2.5.4.97: VATES-Q2866017C

Subject L: MADRID

Subject ST: MADRID

Subject C: ES

**X509SKI**

X509 SK I *MkFkINQtQTrN6ytyCeurjYg60c8=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description [en] *undefined.*  
[es] *undefined.*

Status Starting Time *2020-09-07T01:00:00Z*

**20.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**20.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**20.3.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] *undefined.*  
[es] *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] *urn:oid:1.3.6.1.4.1.26852.1.1.1.4*



**Issuer C:** ES  
**Issuer ST:** BARCELONA  
**Issuer L:** HOSPITALET DE LLOBREGAT  
**Issuer O:** VINTEGRIS SLU  
**Issuer 2.5.4.97:** VATES-B62913926  
**Issuer CN:** CA Vintegris ROOT TrustServices  
**Subject C:** ES  
**Subject ST:** MADRID  
**Subject L:** MADRID  
**Subject O:** CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS  
**Subject 2.5.4.97:** VATES-Q2866017C  
**Subject OU:** ENTIDAD DE CERTIFICACION  
**Subject CN:** CGCOM QUALIFIED 2023  
**Valid from:** Wed May 24 12:25:19 CEST 2023  
**Valid to:** Sat May 21 12:25:18 CEST 2033  
**Public Key:**

```

30820222300D06092A864886F70D01010105000382020F003082020A0282020100BB3CFC58C51C1C8E6E43B89F5D34EA1A2549367F9583071EEF278C3B94D09A6BB7C
B1FB81727F2EEF8B70236AE0A2C2FC12F3D1D9E1FF8633A9E083FC A26D4F886F7C42A1A97538867A3DC927A83BDFAD1A1DDC6D67B914546882D8E120C715E
DD924DAF7A41BA16C24F30C9513D5B080274AE462A396702C30CB08CDEFDFCC56DD8011B67F6CB6B74712330D46A2E8D1B06634EE5F50E955451D91986E
D1B0E4F115EA566454C398458D368D57B47B17B56645A8C6607752DD0E829170D467ACD1F7EF9028ARAB94D28FA9A9B657E3A15856FCF679033263D64B
D3ED3A3E62157848C703E7FD2457786601109B8B7D4B7E6B144A30F05E225E32569422084238C10E8F3BE6F443BE2CA77C0BD0B58BFAE22426854A8026805
A96EBA0A3D8B493B4B985A79EDABBEBCAC11E569FCECA49DEP9D77434DFE8E3D36248C9E21F1FBCC743057F2EEA3A928CAD6068DC4D5DE363838E0D931929
B7341897C523687177390A11C259819AF07067DFB8ADBA19EEA21A99E3AA1C6BAG7DF1558F37AFE16162F7C2D3A71E89573DC25DC301AA5C9548C278E
C6448171AB912F8E6FA3ECC5FDA73D22EAAE51CC5DA110662B45C96048D4CC3D2B120B4FABD979E7F20911C8F866F0D29413A9F2774FBC82E3F4D2A99076EA
C9343707825D4AEE8B8F33FDCE02E7F259D06AA30218E1A405C94DE066151240D87D89E7C668B6F0203010001

```

**Basic Constraints** IsCA: true - Path length: 1  
**Authority Key Identifier** FB:70:16:61:37:9E:DB:E7:32:97:40:3B:44:76:A2:7C:14:E3:B1:24  
**Authority Info Access** <http://www.vincasign.net/publickeys/cavintegris.cer>  
**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.vincasign.net>  
**CRL Distribution Points** <http://crl1.vincasign.net/cavintegris.crl>  
<http://crl2.vincasign.net/cavintegris.crl>  
**Subject Key Identifier** 34:44:02:DE:15:70:B6:FF:4D:FA:47:E3:5A:8D:9B:60:51:80:FC:AB  
**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 87:03:3F:EE:AB:43:12:15:50:5C:DD:79:AE:AF:56:93:36:7D:8B:84:CF:85:34:00:35:A6:A8:B6:92:62:8A:C9

#### X509SubjectName

**Subject C:** ES

**Subject ST:** MADRID

**Subject L:** MADRID

**Subject O:** CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

**Subject 2.5.4.97:** VATES-Q2866017C

**Subject OU:** ENTIDAD DE CERTIFICACION

**Subject CN:** CGCOM QUALIFIED 2023

#### X509SKI

**X509 SK I** NEQC3hVwtv9N+kfjWo2bYFGA/Ks=

#### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2023-12-11T01:00:00Z

#### 20.4.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 20.4.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 20.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.1.4**Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.6**Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.12**Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.26852.1.1.10.2**Description**

## 21 - TSP: BANCO DE ESPAÑA

### TSP Name

**Name** [ en ] *BANCO DE ESPAÑA*

**Name** [ es ] *BANCO DE ESPAÑA*

### TSP Trade Name

**Name** [ en ] *BANCO DE ESPAÑA*

**Name** [ es ] *BANCO DE ESPAÑA*

**Name** [ en ] *EUROPEAN SYSTEM OF CENTRAL BANKS*

**Name** [ es ] *EUROPEAN SYSTEM OF CENTRAL BANKS*

**Name** [ en ] *VATES-V28000024*

### PostalAddress

**Street Address** [ en ] *C/Alcalá, 48*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28014*

**Country Name** [ en ] *ES*

### PostalAddress

**Street Address** [ es ] *C/Alcalá, 48*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28014*

**Country Name** [ es ] *ES*

### ElectronicAddress

**URI** [ en ] *http://www.bde.es*

**URI** [ en ] *mailto:escb-pki@pki.escb.eu*





**Issuer O:** BANCO DE ESPAÑA

**Issuer C:** ES

**Subject CN:** BANCO DE ESPAÑA-AC CORPORATIVA

**Subject O:** BANCO DE ESPAÑA

**Subject C:** ES

**Valid from:** Thu Jul 29 09:03:28 CEST 2004

**Valid to:** Mon Jul 29 09:03:28 CEST 2019

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100BBBC9B010DBD034D21722534E4CA30E7D0CF90FAF5440E52192C17E6DD135057CF5E012A3472659BA77585DA1DD696CF9F3023FC6E237094751C83F258AB1DF0BE28B3F79226F81E13FD1509A446A6E198327E9EC39968568BD0A0C0FD729AA0D7402D0E3B160B4A41642CFA95BF4391627E61A00C54EB4276D14B4E505CE09B76C47E4290D79AEFF4E1C32987485FD92CEB7C8127A6D884A70F0F3EB9227FF858C461C3F87D1C0B742B2FD5A63F3EBEDB558C1205EA359C8F3A76C7B6B32C1826A49AF3DC16A5FAA29101A4621110AB2AB6A921FA0D79674350E694AAE16221DB56CB20776A74D07E21C6E523877E1AEA04828DBE093E911DB780F1570203010001

**Basic Constraints**                    *IsCA: true - Path length: 0*

**Subject Key Identifier**                *C2:45:2B:F4:F9:92:EE:33:59:98:E1:82:75:6B:8C:BC:D0:B6:E5:C1*

**Authority Key Identifier**              *57:5E:6F:71:9E:36:73:9C:56:1C:3A:D5:08:F8:F2:2E:3D:08:64:EC*

**Certificate Policies**                 *Policy OID: 1.3.6.1.4.1.19484.2.2.1*  
*CPS pointer: <http://pki.bde.es/politicas>*  
*CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. @2004 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]*

**Authority Info Access**                *<http://pkiva.bde.es>*

**CRL Distribution Points**              *ldap://CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=SNTPKI01,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*  
*ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ,CN=Internas,CN=PKI,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint*  
*<http://pki.bde.es/crls/ACraiz.crl>*

**Key Usage:**                            *keyCertSign - cRLSign*

**Thumbprint algorithm:**                *SHA-256*

**Thumbprint:**                          *FF:2C:7C:52:66:D4:84:DB:63:87:C9:9A:0F:EB:F0:60:38:91:76:C4:9D:27:28:79:44:85:85:F1:9F:EC:13:0F*

**X509SubjectName**

**Subject CN:** BANCO DE ESPAÑA-AC CORPORATIVA

**Subject O:** BANCO DE ESPAÑA

**Subject C:** ES

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2017-07-01T22:00:00Z

#### 21.1.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 21.1.2 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### **Service Name**

**Name** [es] *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

**Name** [en] *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA*

**Subject O:** *BANCO DE ESPAÑA*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

#### 21.1.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**21.1.3 - History instance n.2 - Status: supervisionincessation**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ es ]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

**Name** *[ en ]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

**Service digital identities****X509SubjectName**

**Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA*

**Subject O:** *BANCO DE ESPAÑA*

**Subject C:** *ES*

**X509SKI**

**X509 SKI** *wkUr9PmS7jNZmOGCdWuMvNC25cE=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

**Status Starting Time** *2015-11-01T00:00:00Z*

**21.1.4 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ es ]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA*

**Name** *[ en ]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA*

**Service digital identities****X509SubjectName**

**Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA*

**Subject O:** *BANCO DE ESPAÑA*

**Subject C:** *ES*

**X509SKI**



**Subject O:** EUROPEAN SYSTEM OF CENTRAL BANKS

**Subject C:** EU

**Valid from:** Fri Jul 22 12:46:35 CEST 2011

**Valid to:** Wed Jul 22 12:46:35 CEST 2026

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100D26FCB8642B34127CE25DA85A619E603F9A3DF3B2F1E67C2EE4F856098F1D5D294A2  
B0682098D0A2D85DD8494C5EEC76926F18B71A412E5E1830F88A7B9A9C1F073F8A5B2AF781977384064816AC3CD5E57E4EF983C6A94E176D1A45C1239E923C6E  
E565ADDC8F38C10DE753D1BE226A8FB8B8E3E9AC2F828941B24974E9F14789CA7390FC298B72627C35E55A3C29949F301373658BB581A32F7B12B6CAC60DC275  
C5C066121AC9A91F6F5CD4F14727E1DC6CD7988111CB7825F6275BA4C75B CA0A7D70D84788C454C69310D1F518E2529983047E60DC2F12ECDE4F19967C13C10189  
8F804277CE3B2AACCE75118BB4253F95E61531A77D7B4FD4648D1188D4E2BA0F3C5A25A336F208E71079F37A C144D1056F85FD8998A00B684E603FB45EF133D84  
F6E11EAB0DE8A970AE90A987D2F2DE5186682E5284FA482838E876199BE6AA06A7F61E03BE4ABB93BA69E7D76670FA CE1249094BB983D46D01FCB590EB63AA4  
BE8048B096F9498A122C54711395FEA3C57A66F740A7B1741C7A7F1AC577B1B94A1D8698C6E4F4A591E07DE675E889195EDD4E94A5E4DEB78C227CC9B6444751D783  
10F1D2CCB9850743BE9EC8BE496932FF149C715173E60D88AD1BEE1174B167C96BDF60351ED5B1C51F268B6BFD2ECA1DB1FE843EAF9BA7DADD5F59EA6ADB109  
D4156CE050D140E6924F44644403021764BBDC6FB90203010001

**Basic Constraints** IsCA: true

**Subject Key Identifier** E4:59:DE:44:24:B6:A4:3C:83:43:37:28:B0:C8:A4:AE:26:2D:3D:03

**Authority Key Identifier** D5:85:1D:69:63:97:28:C9:59:E6:D1:67:07:CD:54:BC:DC:02:7E:EA

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://pki.escb.eu/policies>

**Authority Info Access** <http://pki.escb.eu/certs/rootCA.crt>

**CRL Distribution Points**  
<http://pki.escb.eu/crls/rootCA.crl>  
ldap://ldap-pki.escb.eu/CN=ESCB-PKI%20Root%20CA,OU=PKI,OU=ESCB-  
PKI,O=ESCB,C=EU?certificateRevocationList?base?objectclass=cRLDistributionPoint  
<http://iam-crl.escb.eu/escb/rootCA.crl>  
<http://escbpci/crls/rootCA.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 4B:18:76:44:BF:79:4F:83:D0:00:99:9D:79:27:43:3F:75:F3:CF:B1:64:3A:6D:0F:8A:25:94:35:BE:86  
:1B:7A

**Certificate fields details**

**Version:** 3

**Serial Number:** 135646708379632619634537957133020884269



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *13:35:26:DC:99:E9:CC:36:62:F8:F5:FA:20:06:30:05:BA:90:E6:63:2B:F3:4F:18:A8:4B:A3:9B:5F:AA:57:00*

**X509SubjectName**

**Subject CN:** *ESCB-PKI ONLINE CA*

**Subject O:** *EUROPEAN SYSTEM OF CENTRAL BANKS*

**Subject C:** *EU*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time** *2017-07-01T22:00:00Z*

**21.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**21.2.2 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en]* *Qualified Certificates issued by ESCB-PKI ONLINE CA*

**Name** *[es]* *ESCB-PKI ONLINE CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *ESCB-PKI ONLINE CA*

**Subject O:** *EUROPEAN SYSTEM OF CENTRAL BANKS*

**Subject C:** *EU*

**X509SKI**



**X509 SK I***5FneRCS2pDyDQzcosMikriYtPQM=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2016-06-30T22:00:00Z***21.2.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***21.2.3 - History instance n.2 - Status: undersupervision****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service Name****Name***[ en ]**Qualified Certificates issued by ESCB-PKI ONLINE CA***Name***[ es ]**ESCB-PKI ONLINE CA***Service digital identities****X509SubjectName****Subject CN:***ESCB-PKI ONLINE CA***Subject O:***EUROPEAN SYSTEM OF CENTRAL BANKS***Subject C:***EU***X509SKI****X509 SK I***5FneRCS2pDyDQzcosMikriYtPQM=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision***Status Starting Time***2015-02-24T23:00:00Z***21.3 - Service (withdrawn): Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA****V2****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/CA/QC***Service type description***[ en ]**A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name [en] Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Name [es] Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2

Service digital identities

Certificate fields details

Version: 3

Serial Number: 33025408625715663557967398552839070848

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHjCCBggAwIBAgIQGN2W+abhszVRE3hKckglDANBgkqhkiG9w0BAQsFADBOMQswCQYDVQOQ...
-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA

Issuer CN: BANCO DE ESPAÑA-AC RAIZ V2

Issuer O: BANCO DE ESPAÑA

Issuer C: ES

Subject CN: BANCO DE ESPAÑA-AC CORPORATIVA V2

Subject O: BANCO DE ESPAÑA

Subject C: ES

Valid from: Mon May 04 18:00:00 CEST 2015

Valid to: Sat May 04 18:00:00 CEST 2030

Public Key: 30:82:02:22:30:0D:06:09:2A:86:48:86:7F:0D:01:01:01:05:00:03:82:02:0F:00:80:82:02:0A:02:82:02:01:00:C6:D7:28:F8:74:25:3E:F8:1E:D3:9C:AB:B8:99:3D:8B:D7:FA:C7:E1:00:10:78:39:6A:85:EC:82:47:AC:3:E6:1E:23:53:7E:18:B1:1B:31:AD:83:09:3C:3C:EB:FE:AB:42:DC:97:8B:72:7D:64:77:B4:3F:D4:1A:F1:F7:B2:E4:27:5B:D8:40:15:8D:32:BA:ED:A0:B1:A4:62:84:5F:28:BB:04:0C:ED:4A:DB:D9:78:7F:43:2E:08:66:66:B7:AD:67:3E:1D:60:64:72:80:8A:AE:ED:55:29:93:EX:96:83:45:87:18:11:62:7F:48:A7:FF:0D:CC:84:79:1C:67:7F:2D:D1:46:67:F2:E8:97:7B:32:9D:83:B7:B4:80:CE:40:BA:BD:DS:AE:F3:4E:39:BD:23:CA:C9:8B:74:82:2E:D2:7A:3A:34:EA:FA:B2:68:A7:8F:45:1F:6S:2S:D8:8C:0F:00:26:C8:84:21:AA:08:AC:C8:71:42:95:0D:35:F3:4F:2E:4C:0E:4A:60:93:FA:56:30:6C:0A:3C:52:C8:F9:20:6A:92:F0:EA:AS:A7:78:4D:0C:E2:2E:BA:4C:8B:96:54:AD:DF:61:BF:C7:68:99:83:99:9D:F3:BC:01:DA:C8:B1:49:70:A1:16:05:3C:05:DA:5B:25:BA:7A:1F:04:D6:ED:BA:44:9E:CB:F8:26:A3:64:5B:3A:42:C3:E6:F0:84:EC:AF:04:3B:80:26:D4:99:EE:79:11:E6:CD:2B:C0:55:85:87:85:D0:AS:61:29:31:98:8E:61:7F:18:3C:2A:85:DC:91:79:A9:09:79:22:71:5C:52:B9:4E:38:3C:CE:4C:2E:F0:42:BB:99:26:19:84:BA:AS:34:9D:31:1F:90:65:E8:87:BF:0F:65:60:D1:BD:DA:CD:1D:CF:BS:22:85:7B:31:45:A5:AF:65:0B:5:AC:43:FB:49:B7:25:2D:ED:9A:5F:79:16:16:28:63:06:8C:5C:93:B4:69:ED:A4:F7:36:07:9C:E4:2C:53:90:8E:8B:9B:F7:AS:52:6F:20:67:BF:7D:2D:8A:16:76:7A:67:21:D6:B4:70:BC:BF:31:AF:B1:6C:20:0E:22:CC:EE:6F:83:A5:DE:1A:9C:7E:DS:22:46:A6:BF:CS:D7:0A:B7:D2:C9:30:B9:49:C1:F2:74:0F:DF:7B:90:1C:CC:9A:DB:10:DB:43:FA:69:B9:B6:F7:77:52:4F:07:68:26:0C:37:D3:7B:CF:21:03:B0:AC:AS:1B:92:2B:6C:27:F6:05:9A:C:A:53:81:53:14:53:2C:7B:F1:A9:E4:40:8A:3A:4E:49:A1:32:42:C:00:10:6F:02:03:01:00:01

<b>Basic Constraints</b>	<i>IsCA: true - Path length: 0</i>
<b>Subject Key Identifier</b>	<i>31:ED:F3:61:80:C8:49:DC:D6:CC:3D:0C:E6:28:E2:5C:60:53:DD:58</i>
<b>Certificate Policies</b>	<i>Policy OID: 1.3.6.1.4.1.19484.2.2.1</i> <i>CPS pointer: http://pki.bde.es/politicas</i> <i>CPS text: [Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. @2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)]</i>
<b>Authority Key Identifier</b>	<i>4B:CC:E3:6B:D3:6C:39:34:4F:4D:C3:DE:60:C2:06:19:90:6D:6E:BF</i>
<b>CRL Distribution Points</b>	<i>ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20RAIZ%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint</i> <i>http://pki.bde.es/crls/ACraizv2.crl</i> <i>http://pki.redbde.es/crls/ACraizv2.crl</i>
<b>Key Usage:</b>	<i>keyCertSign - cRLSign</i>
<b>Thumbprint algorithm:</b>	<i>SHA-256</i>
<b>Thumbprint:</b>	<i>64:4B:79:C4:7D:87:C2:9B:31:6A:5C:D7:99:4C:F1:CF:CA:3E:1F:C0:78:55:21:87:56:5F:22:ED:83:25:03:95</i>
<b>Service Status</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</i>
<b>Service status description</b>	<i>[en] undefined.</i> <i>[es] undefined.</i>
<b>Status Starting Time</b>	<i>2017-07-01T22:00:00Z</i>

**21.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	-------------	--

**21.3.2 - History instance n.1 - Status: granted**

<b>Service Type Identifier</b>	<i>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</i>
<b>Service Name</b>	
<b>Name</b>	<i>[en] Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2</i>
<b>Name</b>	<i>[es] Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2</i>

**Service digital identities**

**X509SubjectName**

**Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA V2*

**Subject O:** *BANCO DE ESPAÑA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**21.3.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**21.3.3 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

**Name** *[ es ]* *Certificados Reconocidos emitidos por la AC BANCO DE ESPAÑA-AC CORPORATIVA V2*

**Service digital identities****X509SubjectName**

**Subject CN:** *BANCO DE ESPAÑA-AC CORPORATIVA V2*

**Subject O:** *BANCO DE ESPAÑA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Me3zYYDISdzWzD0M5ijiXGBT3Vg=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time**

*2015-07-12T22:00:00Z*

**22 - TSP: Servicio de Salud de Castilla-La Mancha (SESCAM)****TSP Name**

**Name** [ en ] *Servicio de Salud de Castilla-La Mancha (SESCAM)*

**Name** [ es ] *Servicio de Salud de Castilla-La Mancha (SESCAM)*

**TSP Trade Name**

**Name** [ en ] *Servicio de Salud de Castilla-La Mancha (SESCAM)*

**Name** [ es ] *Servicio de Salud de Castilla-La Mancha (SESCAM)*

**Name** [ en ] *JCCM*

**Name** [ es ] *JCCM*

**Name** [ en ] *SESCAM (NIF Q-4500146H)*

**Name** [ es ] *SESCAM (NIF Q-4500146H)*

**Name** [ en ] *VATES-Q4500146H*

**PostalAddress**

**Street Address** [ en ] *Avenida Río Guadiana*

**Locality** [ en ] *Toledo*

**State Or Province** [ en ] *Toledo*

**Postal Code** [ en ] *45007*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Avenida Río Guadiana*

**Locality** [ es ] *Toledo*

**State Or Province** [ es ] *Toledo*

**Postal Code** [ es ] *45007*

**Country Name** [ es ] *ES*

**ElectronicAddress**



**Subject CN:** *SESCAM CA Entidades Finales*

**Subject O:** *SESCAM (NIF Q-4500146H)*

**Subject O:** *JCCM*

**Subject C:** *ES*

**Valid from:** *Tue Nov 30 11:49:29 CET 2010*

**Valid to:** *Fri Nov 30 11:49:29 CET 2035*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D23E9F5B97A11459CD86D3F2BFD90BE5F70438CEB515FC5911D3BA7C1D55B5D6ACA4CC4A48B261286A2AF7C105D3A813C9A8CE5D7E83E5C314E18B9FF2AFA804520A979FE7B29FA182C12FA4BF5963E835797D7C8A27A50FD5A810A75C5F1F787DAF424F45FD08D1088C6FE68CB0CA8A07FD3F1B0AFEAESA42935EE628347FEDEF756F705BE265B6FCF5692A1766EB615425CF0A0B26E5754A4DFEB71BF8A2F39BB79CBBEF1F1834AD870AA4679C171FC041B090B22C52BE6A80D2C5BF63EC216184F3C2163A18A514BEC5A19620665C6E6DF0BF6F50E6BFCC7F5A849F04CF203E3105CA3DD08A98C6CAC2C853B8F8826FD74A31238321817A1A5F75DB7B3870203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *B5:C3:BB:5E:44:E9:E4:2E:34:04:E4:37:E3:1D:EA:51:FA:D2:07:FD*

**Authority Key Identifier** *E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://sescam.jccm.es/pki/dpc/dpcv2.html>*

**CRL Distribution Points** *[http://sescam.jccm.es/pki/crls/sescam\\_root\\_ca.crl](http://sescam.jccm.es/pki/crls/sescam_root_ca.crl)*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *7B:14:45:2A:70:9D:F3:C6:8C:8E:EB:75:2F:88:78:C0:F5:21:C7:18:8C:23:81:11:DE:1D:DF:82:91:C4:17:2B*

## X509SubjectName

**Subject CN:** *SESCAM CA Entidades Finales*

**Subject O:** *SESCAM (NIF Q-4500146H)*

**Subject O:** *JCCM*

**Subject C:** *ES*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2017-07-01T22:00:00Z*

**Scheme Service Definition URI**



URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 22.1.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [en] undefined.  
[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

##### Policy Identifier:

Identifier [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

### 22.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 22.1.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales

Name [es] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales

#### Service digital identities

##### X509SubjectName

Subject CN: SESCAM CA Entidades Finales

Subject O: SESCAM (NIF Q-4500146H)

Subject O: JCCM

Subject C: ES

**X509SKI**

**X509 SK I** *tcO7XkTp5C40BOQ34x3qUfrSB/0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**22.1.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2*

**22.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**22.1.4 - History instance n.2 - Status: supervisionincessation**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ] Qualified Certificates issued by CA SESCAM CA Entidades Finales*

**Name** *[ es ] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales*

**Service digital identities****X509SubjectName**

**Subject CN:** *SESCAM CA Entidades Finales*

**Subject O:** *SESCAM (NIF Q-4500146H)*

Subject O: JCCM

Subject C: ES

X509SKI

X509 SK I tcO7XkTp5C40BOQ34x3qUfrSB/0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

Status Starting Time 2012-06-08T00:00:00Z

#### 22.1.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1

##### Policy Identifier:

Identifier [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2

#### 22.1.5 - History instance n.3 - Status: undersupervision

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales

Name [es] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales

#### Service digital identities

#### X509SubjectName

Subject CN: SESCAM CA Entidades Finales

Subject O: SESCAM (NIF Q-4500146H)

Subject O: JCCM

Subject C: ES

X509SKI

X509 SK I tcO7XkTp5C40BOQ34x3qUfrSB/0=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2011-09-16T00:00:00Z

#### 22.1.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier [ OIDAURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1

##### Policy Identifier:

Identifier [ OIDAURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2

#### 22.2 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

Name [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

Name [es] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012

#### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 5621409961360079976468545019885437822

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIIGhCCB6G6AwIBAgIQBdQk6MRhcP52jUACzDfIANBqkqkiG9w0BAQUAFADBWM0swCOYDVQOQ
EwJFzENMAsGA1UECgwESkNDTTEMB0GA1UECgwWUVV0QFNFESIRBRLTQIMDaxNDZlKlEXMBLUG
A1UEAw0UV0TQFNF5b3Q00wEhlcBMlTWMJEMTEYODFwWheNMcwMEI3MTEYODFwWjBhMkQsw
COYDVQOGEwJFzEPMAUGA1UECwwGU0V0QFNFMO0wCwYDVQOQDARK00NNRlRwEAYDVQOQGEwIRNDUw
MDE0NzEzDAIBBgNVBAMMGjNFU0BTSBDBQSBhaRzZGZkZXMGtmtlYVwlcCA0S1wDQVJkZVJlbnN
AQEBRQADAgEAFDCAOCgZgBAKml15k0kPQOVh0ncJMSN8qcs3NDkRyWwSCmlWpFLdMVF670
9gc21NnhBdDfmpkUS4K1cWDF0Ynl13m1LBKwcl1-mLxFeFUHnfy7P5cUkLXA-JU104Z01
JjmoF6l_eVzUMDAnBRBscRDWrlh0gXY06EL2XWdH7BOHTTcfcqJWJaw2XvWHINQJZQaMX
M1LNQFecYAVFoujhwGQMMH4H4pTsk3PH089YvWKZDBKdIdc-1c1c59P9ywj2E53daK
pr39V8E0xovJHhR3r3WSBenc93NjHZXMcHhaW9RtJlUkqNdlM8CAwEAAsCAI0w
ggI5MBGAIUdEwEBwQIMAYARCAQAwDgYDR0PAQHBAQDAgEGBG0GA1UdDgQWBBSAkpSobH
QMSFRvscQWAKYVNDABgNVHSMEDDAWgB1rdsGlmRvK09PcDn0vBPljy1TCCAveCAIUdASCA
AU4wggFKMIBRgYEVROgADCCATwNAyKwYBBQUHAgEwKGBG0GA1UdEwYXZLNjY0UamNjBS5cy9w
a2kvZlhlL2RwY3YyLm006WwweYOGCUsGAOUFBwICMHeadkvecyBzJl0WzPzY2Fh3MgZw1pdGik
l3Mg1m1p0Bc3THHbY01awNbhHvnbBwWlWwRvwyBv3lgZWwglUOVQMNHbkmEgQUz
IHNIYm5yZGluYWRhcyBkZSBSY290YyBvYyWl6GRlBcBTRVNDQ0Uw0YQKwYBBOUHAglwscRvQ2Vy
dGlnaWwNidGvZGlz3VlZCB1mRlcB0aGlzIHBybG9eSBhcnRlgaXNzdWVkiG5IHROZSBTRVND
QU0glm1p0Bc3THHbY01awNbhHvnbBwWlWwRvwyBv3lgZWwglUOVQMNHbkmEgQUz
AQUFBwEBBCEwJAKBgggrBgEFBQ0BAyYyYHRoCDevL3Nlcnh5S3Y2NlMvZl3ZmEIGA1UdHwQ7
MDkwN6A1dD0GMW00A6L1y9ZXXNjY0UamNjBS5cy9wa2kvY3YyLm006WwweYOGCUsGAOUFBw
cmwDQVJkZVJlbnNAsGA1UEAglEQU00MDE0NzEzDAIBBgNVBAMMGjNFU0BTSBDBQSBhaRzZGZk
XkZkZXMGtmtlYVwlcCA0S1wDQVJkZVJlbnNAsGA1UEAglEQU00MDE0NzEzDAIBBgNVBAMMGj
Xx=TglNscKcp=Q8gzc35R4RkrF62BkWrka2TL6Qk0W0SB3+M59rB4RlcmicpKv4mms
7Eg1NMFQHKRtWjHHPH336BCr86adNzYTYyqSwb3P0sHHMxdDLJ4KnbVTVmcbzROnUxYL8r
lEAS57eHINAkKs59smkoD5=mlLqSxHtpz2CV0l0ngDKSLpWmVMSVvOK0hbF0xMfEq
dPR4psS8r4jN2RRW0kaldpsvmsNc0Jd5rGXlJN6AvYNb0m1CQmms=ZHG1hbNDACzNK2
//PzD0486AKzN2nYk5o1ZQ0pdSoUYDUSI4cCqErfP0QZvhh70Hue61lLFRwgTWSdJ
Zs5F1gbswEELPR4FD9QK4drcfllc=7e=smidz2funt7NzDMMS0lQevTmlGlsYAdZx
LcGggc=JSpW0MBA66zCgJhKN23WEyveMcM2nPF3Y4vEQ87qKwSf84D0vY9GAHqYPA0M
Y0m=wY6vdVurYn=dsSynEN5wzqUWVpjuVQ0k4E6Sh10bnEdlqQncr1fh1f06vZLceBSZ
wDEjRkG4Y2KcOHUFDlly32a

```

-----END CERTIFICATE-----

**Signature algorithm:** SHA1withRSA

**Issuer CN:** SESCOAM Root CA

**Issuer O:** SESCOAM(NIF Q-4500146H)

**Issuer O:** JCCM

**Issuer C:** ES

**Subject CN:** SESCOAM CA Entidades Finales

**Subject SERIAL NUMBER:** Q4500146H

**Subject O:** JCCM

**Subject OU:** SESCOAM

**Subject C:** ES

**Valid from:** Mon Feb 27 12:28:20 CET 2012

**Valid to:** Fri Feb 27 12:28:20 CET 2037

**Public Key:**

3082:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:00:05:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A8:66:D5:22:64:A2:53:DF:41:50:68:96:70:89:31:23:7C:A9:C7:B7:34:3C:51:C9:F9:56:48:26:EE:21:6A:8F:2D:D3:15:17:AE:CE:F6:AA:F6:D4:D9:E1:06:20:C4:A2:5A:6A:91:44:BB:29:38:9E:58:31:4E:62:79:75:DE:79:93:2C:19:16:70:B2:E:98:BC:45:78:55:07:FE:77:EB:8B:79:94:0B:5C:0F:89:53:37:CE:11:9D:08:26:3B:67:5A:21:74:23:F8:15:CD:43:03:02:70:51:05:A0:91:0D:6A:C8:8B:A2:20:5D:8D:3A:10:BD:97:59:D1:FB:04:EB:47:4E:57:89:7A:A2:6A:58:96:80:D9:7B:E7:58:77:CD:40:9D:99:41:A3:17:6C:84:E4:35:01:5A:71:CS:40:58:9B:E7:8E:A8:70:19:03:0C:30:9E:11:E2:94:F1:96:4D:DF:3C:73:BC:F5:8B:D6:2B:B0:FC:F3:12:9D:69:47:3E:AC:8B:F9:6C:FC:D1:CB:08:D9:1F:9D:FF:76:20:0A:A6:BA:77:F5:5F:04:D1:B5:EC:8:9B:63:1C:76:91:DE:25:92:05:C9:DE:36:FF:77:56:31:ED:66:25:CC:72:B1:E1:9D:6F:51:86:22:6E:51:A2:AA:35:D1:09:31:DF:02:05:01:00:01

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** B3:92:9C:69:4A:88:47:40:C4:85:46:DB:DE:19:68:80:29:8B:55:48

**Authority Key Identifier** E8:13:AF:C6:26:64:55:91:B6:FD:7C:5C:63:0E:C7:6F:7C:FD:72:4D

**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS pointer: <http://sescam.jccm.es/pki/dpc/dpcv2.html>

CPS text: [Los certificados emitidos bajo esta política son emitidos por el SESCAM para ACs subordinadas de la AC raíz del SESCAM]

CPS text: [Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA]

**Authority Info Access**<http://sescam.jccm.es/va>**CRL Distribution Points**[http://sescam.jccm.es/pki/crls/sescam\\_root\\_ca.crl](http://sescam.jccm.es/pki/crls/sescam_root_ca.crl)**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

6F:C2:32:D6:10:27:6E:1B:95:B2:84:8A:E0:B2:60:36:23:C7:80:86:98:C8:97:56:42:AD:40:D2:8F:4B:D2:84

**X509SubjectName****Subject CN:**

SESCAM CA Entidades Finales

**Subject SERIAL NUMBER:**

Q4500146H

**Subject O:**

JCCM

**Subject OU:**

SESCAM

**Subject C:**

ES

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2017-07-01T22:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**URI**

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**22.2.1 - Extension (critical): Qualifiers [NotQualified]****Qualifier type description**

[en]

undefined.

[es]

undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2

**22.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**22.2.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*

**Name** [ es ] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

**Service digital identities****X509SubjectName**

**Subject CN:** *SESCAM CA Entidades Finales*

**Subject SERIAL NUMBER:** *Q4500146H*

**Subject O:** *JCCM*

**Subject OU:** *SESCAM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *s5KcaUqIR0DEhUbb3hlogCmLVUg=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**22.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

**22.2.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**22.2.4 - History instance n.2 - Status: supervisionincessation**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012*

**Name** [es] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012*

**Service digital identities****X509SubjectName**

**Subject CN:** *SESCAM CA Entidades Finales*

**Subject SERIAL NUMBER:** *Q4500146H*

**Subject O:** *JCCM*

**Subject OU:** *SESCAM*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *s5KcaUqIR0DEhUbb3hlogCmLVUg=*



**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation>

**Status Starting Time** 2016-06-26T22:00:00Z

#### 22.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.1

##### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:2.16.724.4.8.10.60.10.3.2.2

#### 22.2.5 - History instance n.3 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] Qualified Certificates issued by CA SESCAM CA Entidades Finales - 2012

**Name** [es] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales - 2012

#### Service digital identities

##### X509SubjectName

**Subject CN:** SESCAM CA Entidades Finales

**Subject SERIAL NUMBER:** Q4500146H

**Subject O:** JCCM

**Subject OU:** SESCAM

**Subject C:** ES

##### X509SKI

X509 SK I

s5KcaUqIR0DEhUbb3hlogCmLVUg=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2012-06-08T00:00:00Z

**22.2.5.4 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2

**22.3 - Service (withdrawn): Qualified Certificates issued by CA SESCAM CA Entidades Finales v2**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

**Name** [ en ] Qualified Certificates issued by CA SESCAM CA Entidades Finales v2

**Name** [ es ] Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2

**Service digital identities**

Certificate fields details

**Version:** 3

**Serial Number:** 147066880981946919780166724887946939210



**Authority Info Access** *http://sescam.jccm.es/va*

**CRL Distribution Points** *http://sescam.jccm.es/pki/crls/sescam\_root\_ca\_v2.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *CE:9F:E1:F8:BC:D8:9C:47:69:57:C7:82:17:F4:C4:6F:F5:02:2E:B9:06:63:12:36:2F:61:01:6F:62:9E:79:C4*

**X509SubjectName**

**Subject CN:** *SESCAM CA Entidades Finales v2*

**Subject SERIAL NUMBER:** *Q4500146H*

**Subject O:** *JCCM*

**Subject OU:** *SESCAM*

**Subject C:** *ES*

**Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time***2017-07-01T22:00:00Z***Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**22.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2*

**22.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**22.3.3 - History instance n.1 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [en] *Qualified Certificates issued by CA SESCAM CA Entidades Finales v2*

Name [es] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2*

**Service digital identities****X509SubjectName**

Subject CN: *SESCAM CA Entidades Finales v2*

Subject SERIAL NUMBER: *Q4500146H*

Subject O: *JCCM*

Subject OU: *SESCAM*

Subject C: *ES*

**X509SKI**

X509 SK I *ieoqRDcPTF7MtM4a7omkbeilxa0=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

**22.3.3.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description [en] *undefined.*

[es] *undefined.*

Criteria list assert=**atLeastOne**

Policy Identifier:

**Identifier** [ OIDsURN ] *urn:oid:2.16.724.4.8.10.60.10.3.2.1*

**Policy Identifier:**

**Identifier** [ OIDsURN ] *urn:oid:2.16.724.4.8.10.60.10.3.2.2*

### 22.3.3.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 22.3.4 - History instance n.2 - Status: undersupervision

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** [ en ] *Qualified Certificates issued by CA SESCAM CA Entidades Finales v2*

**Name** [ es ] *Certificados reconocidos emitidos por CA SESCAM CA Entidades Finales v2*

#### Service digital identities

##### **X509SubjectName**

**Subject CN:** *SESCAM CA Entidades Finales v2*

**Subject SERIAL NUMBER:** *Q4500146H*

**Subject O:** *JCCM*

**Subject OU:** *SESCAM*

**Subject C:** *ES*

##### **X509SKI**

**X509 SK I** *ieoqRDcPTF7MtM4a7omkbeilxa0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2016-06-26T22:00:00Z*

### 22.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:2.16.724.4.8.10.60.10.3.2.2

**23 - TSP: SIGNE S.A.****TSP Name**

**Name** [ en ] *SIGNE S.A.*

**Name** [ es ] *SIGNE S.A.*

**TSP Trade Name**

**Name** [ en ] *SIGNE Autoridad de Certificación*

**Name** [ es ] *SIGNE Autoridad de Certificación*

**Name** [ en ] *VATES-A11029279*

**PostalAddress**

**Street Address** [ es ] *Avenida de la Industria, 18*

**Locality** [ es ] *Tres Cantos*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28760*

**Country Name** [ es ] *ES*

**PostalAddress**

**Street Address** [ en ] *Avenida de la Industria, 18*

**Locality** [ en ] *Tres Cantos*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28760*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:signe-ac@signe.com*

**URI** [ en ] *http://www.signe.es/signe-ac*

**TSP Information URI**

**URI** [ en ] *http://www.signe.es/en*







**Signature algorithm:** SHA256withRSA

**Issuer CN:** Autoridad de Certificacion Firmaprofesional CIF A62634068

**Issuer C:** ES

**Subject CN:** SIGNE Autoridad de Certificacion

**Subject SERIAL NUMBER:** A11029279

**Subject O:** SIGNE S.A.

**Subject L:** Avenida de la Industria 18. Tres Cantos 28760-Madrid

**Subject C:** ES

**Valid from:** Thu Jul 09 13:15:08 CEST 2020

**Valid to:** Tue Dec 31 05:02:55 CET 2030

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100CD97AD27C9B81076D3A1685BE23F23D1DB5B8553A22B3E22A964399858E7316ABB64B16074C62C5B08DDA570CD8B7A5D893FBA849800F96EC8BA78C1D3A61C35BE00419AB9E39D4D1DCCE0B8407A48F98AA8C7A7A1D1A83D609126923D25DCBCEB53BEAE23AA0FF8389960E072F6FB17E83021128B178DB8EBB5F0FFB62671DC2AAE47226C999F40651404A6C4E3CCB2821AE47A10D77E7F801785D823AAB0C757B2F61D0315C3D77C19A8C0649992184D8493C45EFCF0B2B71EC087D6ADE722B23E6F33B6B5F513BF70B45FD03A91EED0EA67AFD6167D2037A95B60CF6BB426D26767B20CD74970505FF42E97F09C1859B17F92A8F202EAE85F6E94FE7050203010001

**Authority Info Access**  
<http://crl.firmaprofesional.com/caroot.crt>  
<http://ocsp.firmaprofesional.com>

**Subject Key Identifier**  
90:AD:1A:31:FD:47:45:6D:32:44:43:18:85:97:64:C7:38:AE:6D:A8

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS text: [Certificado de Autoridad de Certificación. Consulte las condiciones de uso en <http://www.firmaprofesional.com/cps>]  
CPS pointer: <http://www.firmaprofesional.com/cps>

**CRL Distribution Points**  
<http://crl.firmaprofesional.com/fpoot.crl>

**Extended Key Usage**  
id\_kp\_clientAuth

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** C4:2C:E0:22:D0:A3:45:7B:6B:D6:97:87:11:CE:7B:C7:43:85:C4:B3:4E:11:EB:C8:BA:EE:8B:1D:1B:83:27:99

X509SubjectName

**Subject CN:** *SIGNE Autoridad de Certificacion*

**Subject SERIAL NUMBER:** *A11029279*

**Subject O:** *SIGNE S.A.*

**Subject L:** *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

**Subject C:** *ES*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2021-04-21T00:00:00Z*

### 23.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.3.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.3.2*

### 23.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

### 23.1.3 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

### 23.1.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** *[en] undefined.*

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.2.3**Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.10.3**Policy Identifier:****Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.5.3**Description****23.1.5 - History instance n.1 - Status: granted****Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name** [ es ] *Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación***Name** [ en ] *Qualified certificates issued by SIGNE- Certification Authority***Service digital identities****X509SubjectName****Subject CN:** *SIGNE Autoridad de Certificacion***Subject SERIAL NUMBER:** *A11029279***Subject O:** *SIGNE S.A.***Subject L:** *Avenida de la Industria 18. Tres Cantos 28760-Madrid***Subject C:** *ES***X509SKI****X509 SK I** *kK0aMf1HRW0yREMYhZdkxziubag=***Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Status Starting Time** *2019-10-28T01:00:00Z*

**23.1.5.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.3.2

**23.1.5.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**23.1.5.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**23.1.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

**Description**

**23.1.6 - History instance n.2 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ es ]* *Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación*

**Name** *[ en ]* *Qualified certificates issued by SIGNE- Certification Authority*

**Service digital identities****X509SubjectName**

**Subject CN:** *SIGNE Autoridad de Certificacion*

**Subject SERIAL NUMBER:** *A11029279*

**Subject O:** *SIGNE S.A.*

**Subject L:** *Avenida de la Industria 18. Tres Cantos 28760-Madrid*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *kK0aMf1HRW0yREMYhZdkxziubag=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-01-16T01:00:00Z*

**23.1.6.5 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.36035.1.3.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.36035.1.3.2*

**23.1.6.6 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

23.1.6.7 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

23.1.6.8 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [ en ] undefined.

[ es ] undefined.

## Criteria list assert=atLeastOne

## Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.2.3

## Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.10.3

## Policy Identifier:

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.36035.1.5.3

## Description

23.1.7 - History instance n.3 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

Name [ es ] Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación

Name [ en ] Qualified certificates issued by SIGNE- Certification Authority

Service digital identities

## X509SubjectName

Subject CN: SIGNE Autoridad de Certificacion



Subject SERIAL NUMBER: A11029279

Subject O: SIGNE S.A.

Subject L: Avenida de la Industria 18. Tres Cantos 28760-Madrid

Subject C: ES

**X509SKI**

X509 SK I kK0aMf1HRW0yREMYhZdkxziubag=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2016-06-30T22:00:00Z

**23.1.7.9 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.36035.1.3.1
------------	------------	---------------------------------

**Policy Identifier:**

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.36035.1.3.2
------------	------------	---------------------------------

**Policy Identifier:**

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.36035.1.10.1
------------	------------	----------------------------------

**Policy Identifier:**

Identifier	[OIDAsURN]	urn:oid:1.3.6.1.4.1.36035.1.10.2
------------	------------	----------------------------------

**23.1.7.10 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	------	---

**23.1.8 - History instance n.4 - Status: undersupervision**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>	
<b>Service Name</b>		
<b>Name</b>	[ es ]	Certificados reconocidos emitidos por SIGNE-Autoridad de Certificación
<b>Name</b>	[ en ]	Qualified certificates issued by SIGNE- Certification Authority

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	SIGNE Autoridad de Certificación
<b>Subject SERIAL NUMBER:</b>	A11029279
<b>Subject O:</b>	SIGNE S.A.
<b>Subject L:</b>	Avenida de la Industria 18. Tres Cantos 28760-Madrid
<b>Subject C:</b>	ES

**X509SKI**

<b>X509 SK I</b>	kK0aMf1HRW0yREMYhZdkxziubag=
------------------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision</a>
-----------------------	---

<b>Status Starting Time</b>	2011-10-07T00:00:00Z
-----------------------------	----------------------

**23.1.8.11 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[ en ]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[ es ]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.36035.1.3.1
-------------------	-------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.36035.1.3.2
-------------------	-------------	---------------------------------

**Policy Identifier:**



**Subject 2.5.4.97:** VATES-A11029279

**Subject O:** SIGNE S.A.

**Subject C:** ES

**Valid from:** Thu Jul 30 11:26:04 CEST 2020

**Valid to:** Tue Dec 31 05:02:55 CET 2030

**Public Key:**

```
3082 02 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 02 0F 00 39 82 02 0A 02 82 02 01 00 CF FF 2F 19 A4 4F 80 93 D4 B1 99 78 E5 94 4D 44 E6 52 11 A3 5B 1C E3 1B 83 F4 61 33 A7 28 FC 5E CA 32 4
A F8 AF 50 4D B2 E2 68 E2 F3 2A 5E 78 9F C9 52 8D 43 9D 09 16 37 D3 2E 92 76 C6 A0 1B FB A2 CE 89 C9 6A 19 84 22 FC 4A B9 8E 13 7B E3 BA 0F 82 73 07 7B 7C 24 B6 E9 09 AB 4C 8B 00 23 B5 87 0D C1 7
B 94 8E 15 5C 47 CA 94 B9 93 23 9D 8B A9 2A F1 23 D8 C 62 7A 99 79 17 30 CF 74 E0 8F 0B 6D DA C5 25 45 DD 4D 49 B3 43 3F SD 4B DD B8 34 0C 4D 39 31 C6 78 F4 41 00 E2 2E 44 16 9F 0C E4 97 4D 77 17
CF 0A B1 87 BF E1 32 65 D2 8D F3 86 39 A9 9E 19 7E 7C 8A A3 B2 33 B5 75 60 E7 93 AB 7B 23 52 08 C8 B5 65 48 FB C9 7D B5 B9 8A CA 24 D1 38 80 61 F6 89 1A C1 1A E5 40 E1 D7 A9 4B E5 B4 56 FE A0
39 D6 4C 94 62 6F 5F 92 D1 24 63 63 63 37 D4 83 A A 93 7D E7 E2 FD 67 66 80 DA 51 14 70 64 D6 13 16 2B 83 A4 67 49 DF E7 90 A8 62 BA 12 A0 B9 91 7A E7 6B F1 72 4A C8 45 FB 2C 9B D1 9C B8 68 A6 4F 20
18 E6 0E 28 FB C2 CE 6E 84 ED 2C 48 A5 F0 C4 A8 89 F2 7D 56 AE 0A EC 4F B4 5B 1E 68 5D 9E DF 7C 68 F4 91 4C 08 D1 55 56 2F 00 00 02 62 D2 90 2E 05 96 B3 6C 1C FD A6 44 69 E7 C6 34 0E 98 20 AC B8 B
A E4 A9 93 D8 A3 B3 2D 03 49 75 A9 8D 43 E0 54 3C 84 BE DD 97 C0 C1 60 16 2F 01 9B 79 3D 1F 05 D1 56 AE 9A 80 C1 A9 8E 48 48 25 B3 85 C8 8C 96 95 DF 1B D9 FD 0A FD A3 92 43 DD 64 57 08 E6 03 A5 E
2 B5 BB 8A 52 4C 4D 0E A8 B7 5D 1C 9E 6D 54 ED 07 8E 9D BB 8D 5D 9F 77 1F 2F 98 BC F2 19 1E 71 A9 41 0C A4 53 A9 67 80 FB 7C 6C 43 B3 24 AE 25 E9 6E C2 46 78 F6 D9 7A 3A 3D 36 CA 4C 52 2A C9 7B
A1 CB C7 22 B7 28 DD 63 EC 68 5C 0D 3F 0C AE 2D ED A9 C4 0C D7 02 03 01 00 01
```

**Authority Info Access** <http://crl.firmaprofesional.com/caroot.crt>

<http://ocsp.firmaprofesional.com>

**Subject Key Identifier** 22:3A:82:E6:A8:3F:A9:E3:EA:23:A0:AB:F6:8D:04:4B:48:7B:68:CC

**Basic Constraints** IsCA: true - Path length: 0

**Authority Key Identifier** 65:CD:EB:AB:35:1E:00:3E:7E:D5:74:C0:1C:B4:73:47:0E:1A:64:2F

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <http://www.firmaprofesional.com/cps>

**CRL Distribution Points** <http://crl.firmaprofesional.com/froot.crl>

**Extended Key Usage** id\_kp\_clientAuth

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** B8:DF:38:4F:1F:CD:6E:CB:3F:4D:7D:D6:38:0E:54:D3:54:C6:12:56:56:0A:59:9D:80:45:32:47:D9:3A:F5:EA

## X509SubjectName

**Subject CN:** SIGNE Autoridad de Certificacion - 2020

**Subject OU:** Autoridad de Certificacion

**Subject 2.5.4.97:** VATES-A11029279

**Subject O:** SIGNE S.A.

**Subject C:** ES

## X509SKI

X509 SK I

IjqC5qg/qePqI6Cr9o0ES0h7aMw=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.  
[es] undefined.

**Status Starting Time**

2023-10-24T00:00:00Z

**23.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**23.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**23.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.21.3

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.3.3

**Description****23.2.4 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

**Name** [ en ] *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

**Service digital identities****X509SubjectName**

**Subject CN:** *SIGNE Autoridad de Certificacion - 2020*

**Subject OU:** *Autoridad de Certificacion*

**Subject 2.5.4.97:** *VATES-A11029279*

**Subject O:** *SIGNE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *IjqC5qg/qePqI6Cr9o0ES0h7aMw=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2022-10-20T00:00:00Z*

**23.2.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**23.2.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**23.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.10.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.5.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.36035.1.21.3

**Description****23.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados reconocidos emitidos por SIGNE Autoridad de Certificación - 2020*

**Name** [en] *Qualified Certificates issued by SIGNE Autoridad de Certificación - 2020*

**Service digital identities****X509SubjectName**

**Subject CN:** *SIGNE Autoridad de Certificacion - 2020*

**Subject OU:** *Autoridad de Certificacion*

**Subject 2.5.4.97:** *VATES-A11029279*

**Subject O:** *SIGNE S.A.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *IjqC5qg/qePqI6Cr9o0ES0h7aMw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2020-10-05T00:00:00Z*

**23.2.5.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**23.2.5.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**23.2.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*  
*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.36035.1.2.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.36035.1.10.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.36035.1.5.3*

**Description**



**24 - TSP: SISTEMAS INFORMATICOS ABIERTOS S.A.U.****TSP Name**

**Name** [ en ] *SISTEMAS INFORMATICOS ABIERTOS S.A.U.*

**Name** [ es ] *SISTEMAS INFORMATICOS ABIERTOS S.A.U.*

**TSP Trade Name**

**Name** [ en ] *SIA*

**Name** [ es ] *SIA*

**Name** [ en ] *VATES-A82733262*

**Name** [ en ] *SISTEMAS INFORMATICOS ABIERTOS S.A.*

**Name** [ es ] *SISTEMAS INFORMATICOS ABIERTOS S.A.*

**Name** [ en ] *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Name** [ es ] *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**PostalAddress**

**Street Address** [ en ] *Avda. de Bruselas N.º 35*

**Locality** [ en ] *Alcobendas*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28108*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Avda. de Bruselas N.º 35*

**Locality** [ es ] *Alcobendas*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28108*

**Country Name** [ es ] *ES*

**ElectronicAddress**



**Issuer O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Issuer C:** ES

**Subject CN:** SIA SUB01

**Subject SERIAL NUMBER:** A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**Valid from:** Thu Jan 29 10:56:43 CET 2015

**Valid to:** Tue Jan 29 11:26:43 CET 2030

**Public Key:**

```
30820222300D06092A864886F70D01010105000382020F003082020A028202010096B7EC41AA6C6ADE920AD4FF04C073A575FF6FDD5DAFBC78323B769F8281F785B32F621C619FBF2AA1C183138CD2CF8A4E1631E05955A029E6B7A41634DF34CF2E49C9540BB0BDBDC3C213C3D7B5619D6712BC16833448995FB5BC9789FF3B39E54A52C65D74AB42FCA2FCDF7A26D4F716089E0E0D0414B3DE157BBB19E0F27FC2E07990B3FE08B2F020C41F965CB1D1B186E33222B9103BA18E2F7B5B798530204723B8D338FE52A05611980696CA88BD71CF88314F84ACE7D1186F3B33FB9EB0E08E1B81F99E75A053F9C76827CE38C9C6F30A07C9CDC3E0B15B9FE5D126E475921F23FDCD19564073CE6EC1F6734F8E8F82B3E8F56194F88D5A015DB31D1588D3D1B1AC360FE3C6A863EB1C1E1D9A89C7B5D1846C3936231FD8B8A6459DFAA3433A319448C7681DE4D7423ADCA8E98285F8D53C830C87C9E4672B384DAC8D2E99F944FB190FEC98C13292B07570AF2C615464378AB0F58FC02EE72C871622A37A5F1B4532036EAC5E7A5512220F7CE12FFDA85693B806F8BFAF176A5110C892A29F5B2D89F917006FFFA33AC8D22615E24A2E7E2D11A01B861E778163E85DD76EFB4461265C653C5D33819E378273D43127AF3003625406280DA9962A85E01AB2E586CAF94CF80A635163B30C3AADAA698D89F7DDEA095903EDE2A8E6C6C37590F79E94EFA08A53B5E0B0486C472D6BE6937547CECC69F9B0203010001
```

**Basic Constraints** IsCA: true - Path length: 0

**Authority Info Access** [https://psc.sia.es/ac\\_raiz.crt](https://psc.sia.es/ac_raiz.crt)

<https://psc.sia.es/ocsp>

**Certificate Policies** Policy OID: 2.5.29.32.0

CPS pointer: <https://psc.sia.es>

CPS text: [Certificado de AC subordinada. Consulte las condiciones de uso en <https://psc.sia.es>]

**CRL Distribution Points** <https://psc.sia.es/arl.crl>

C=ES,O=SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA,SERIALNUMBER=A82733262,CN=SIA ROOT,CN=CRL1

**Authority Key Identifier** 2E:E0:8D:C9:54:AE:A2:1B:73:C9:A6:A3:47:AB:99:63:C2:EE:D4:F0

**Subject Key Identifier** DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 68:69:00:54:B9:17:C0:E4:A9:60:92:C4:B3:59:F7:41:80:98:B6:4E:F1:49:A7:0B:78:5A:38:9C:45:51:5D:10

**X509SubjectName**

**Subject CN:** SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA

Subject O: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C: ES

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2022-12-22T00:00:00Z

#### 24.1.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 24.1.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 24.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

##### Criteria list assert=atLeastOne

###### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

###### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

###### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

###### Policy Identifier:

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.18
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.20
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.13
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.20.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.13.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.39131.10.1.13.2
<b>Description</b>		

#### 24.1.4 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

#### **Service Name**

**Name** [ en ] *Qualified Certificates issued by CA SIA SUB01*

**Name** [ es ] *Certificados Reconocidos emitidos por CA SIA SUB01*

#### Service digital identities

#### **X509SubjectName**

**Subject CN:** *SIA SUB01*

**Subject SERIAL NUMBER:** *A82733262*

**Subject OU:** *QUALIFIED CA*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

#### **X509SKI**

**X509 SK I***2mDRJzDSJoXNfkji9ul5H1owVaw=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2022-01-11T02:00:00Z***24.1.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***24.1.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI***[ en ]**http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals***24.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]****Qualifier type description***[ en ]**undefined.**[ es ]**undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier***[ OIDsURN ]**urn:oid:1.3.6.1.4.1.39131.10.1.15***Policy Identifier:****Identifier***[ OIDsURN ]**urn:oid:1.3.6.1.4.1.39131.10.1.16***Policy Identifier:****Identifier***[ OIDsURN ]**urn:oid:1.3.6.1.4.1.39131.10.1.17***Policy Identifier:****Identifier***[ OIDsURN ]**urn:oid:1.3.6.1.4.1.39131.10.1.18***Policy Identifier:****Identifier***[ OIDsURN ]**urn:oid:1.3.6.1.4.1.39131.10.1.20***Policy Identifier:**

**Identifier** [ OIDA sURN ] urn:oid:1.3.6.1.4.1.39131.10.1.13

**Description**

**24.1.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] Qualified Certificates issued by CA SIA SUB01

**Name** [ es ] Certificados Reconocidos emitidos por CA SIA SUB01

**Service digital identities**

**X509SubjectName**

**Subject CN:** SIA SUB01

**Subject SERIAL NUMBER:** A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**X509SKI**

**X509 SK I** 2mDRJzDSJoXNfkji9ul5H1owVaw=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2020-01-16T01:00:00Z

**24.1.5.4 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**24.1.5.5 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**24.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.18

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.20

**Description****24.1.6 - History instance n.3 - Status: granted**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [en] Qualified Certificates issued by CA SIA SUB01

Name [es] Certificados Reconocidos emitidos por CA SIA SUB01

**Service digital identities****X509SubjectName**

Subject CN: SIA SUB01

Subject SERIAL NUMBER: A82733262

Subject OU: QUALIFIED CA



**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**X509SKI**

**X509 SK I** 2mDRJzDSJoXNfkji9ul5H1owVaw=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2019-10-28T01:00:00Z

**24.1.6.7 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**24.1.6.8 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**24.1.6.9 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [ en ] undefined.

[ es ] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.39131.10.1.15

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.39131.10.1.16

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.39131.10.1.17

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.39131.10.1.18

**Description****24.1.7 - History instance n.4 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by CA SIA SUB01*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA SIA SUB01*

**Service digital identities****X509SubjectName**

**Subject CN:** *SIA SUB01*

**Subject SERIAL NUMBER:** *A82733262*

**Subject OU:** *QUALIFIED CA*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *2mDRJzDSJoXNfkji9ul5H1owVaw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2019-08-02T00:00:00Z*

**24.1.7.10 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**24.1.7.11 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**24.1.7.12 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.15

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.16

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.17

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.39131.10.1.18

**Description****24.1.8 - History instance n.5 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] Qualified Certificates issued by CA SIA SUB01

**Name** [es] Certificados Reconocidos emitidos por CA SIA SUB01

**Service digital identities****X509SubjectName**

**Subject CN:** SIA SUB01

**Subject SERIAL NUMBER:** A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**X509SKI**

**X509 SKI** *2mDRJzDSJoXNfkji9ul5H1owVaw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-02-15T01:00:00Z*

**24.1.8.13 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**24.1.8.14 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**24.1.8.15 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*  
*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.39131.10.1.7*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.39131.10.1.15*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.39131.10.1.16*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.39131.10.1.17*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.39131.10.1.18*

**Description****24.1.9 - History instance n.6 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA SIA SUB01*

**Name** [ es ] *Certificados Reconocidos emitidos por CA SIA SUB01*

**Service digital identities****X509SubjectName**

**Subject CN:** *SIA SUB01*

**Subject SERIAL NUMBER:** *A82733262*

**Subject OU:** *QUALIFIED CA*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *2mDRJzDSJoXNfkji9ul5H1owVaw=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**24.1.9.16 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**24.1.10 - History instance n.7 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by CA SIA SUB01*

**Name** *[ es ]* *Certificados Reconocidos emitidos por CA SIA SUB01*

### Service digital identities

#### X509SubjectName

**Subject CN:** *SIA SUB01*

**Subject SERIAL NUMBER:** *A82733262*

**Subject OU:** *QUALIFIED CA*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *2mDRJzDSJoXNfkji9ul5H1owVaw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2015-07-06T00:00:00Z*

## 24.2 - Service (withdrawn): Qualified timestamps issued by TSAQC

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[ en ]* *A time-stamping generation service creating and signing qualified time-stamps tokens.*  
*[ es ]* *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

#### Service Name

**Name** *[ en ]* *Qualified timestamps issued by TSAQC*

**Name** *[ es ]* *Sellos de tiempo cualificados emitidos por TSAQC*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *1481140816*

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```

MIHADCCBOgAwIBAgEWEhUdANBgkqhkiG9w0BAQoFADCCBjEMLAAKAU1UEBMCRVMxODA2BGNV
BaoTLINJUIRETFUEIRK9STUFIUSINPUBBOKIFURIPUyBTTONRURBRCBBT908U1BMRUwEwYD
VOQLERVUFMSZIRUQgOQESAgQBNVBAIUTCLEMzEzMEJESMBAGAU1UEAMUUBIBFNWQjAs
MBx4DTE3MThwMTExNDI0bWVMTyBwMTI0bWVMTyBwMTI0bWVMTyBwMTI0bWVMTyBwMTI0bW
EY9tSVNURU1BUyB1TKZPLIBVEIDTImgOUJRVIU7TImgU99DSUVEUQgOUQSPTRINOTEVMBMGAIUE
CMMUUVBIEGSIUVEIENBMRewfYDVQIRhw9wOVRFUyIBODJEM2M0YjVjZjAAMBgNVBAMTBTBVRTQVFD
MIBIBANBgkqhkiG9w0BAQEFAAOCAQAMIBCCcKCAQAEImSNqSphXB34A4W34S3SCZIEh3stfp
yq1BpNVbJslE.CocCINdVpO98SCXII1caRRIMHcnSFTOqNhg3oEwvH95-J9ONKkv+a8tk4
cKvYzZzK195WUoZEVIMgmhukUjgsdFrl4bW0MaO6HlpQ7YIagzXKLdYVSYLN
zY0RCAMGesN9eQIVKGwGAT0mNAQR0zduZHWo6tldLmIAK1ESd0W69-v0EwoXBVvVQp
nRlaZ1sL2KU1bvd0wa6WgdZ+065gNFAW6M5pxxmOF3ZYT Ehh9lJh0z2Z26BUhhqV7Yr
UYENQDAOAB04cC.CAmwDeYDVRPAQBABQDABMBYGA1UJQEBwOMMAoGCCsGAQUFBwMI
MFAGAU1dHwRMEwRafDoEGChZhdHBBz0h5NjLnNpYS5lcw9bY19sdWVwMSJemvGHmh0HIA6
LY9wC2uc2ilLmVdL2FjX3N1YjAALmNvbDBBZBggBGFEBQcBAORUMETwYkwyBBQUHIAAGGF2b0
dHBR0h5NjLnNpYS5lcw9bY19sdWVwMSJemvGHmh0HIA6LY9wC2uc2ilLmVdL2FjX3N1YjAALm
c3VMDUuY3M0MlhwBgNVHSALgegwglwgdGCSysGAOQBrFBCeFOMIHMB4GCCsGAOUFBwIBFhJo
dHRwczovLjBzYy5zaWwEuzXMGwzOCCcGAOUFBwICMIGXDIUQV2VudGlnaWwNbzG8zGULgc2Vvdmlj
aW9kZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZl
IHRpZWlwa9eQ29hZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZlZGZl
O8wEhNjLnNpYS5lcw9bY19sdWVwMSJemvGHmh0HIA6LY9wC2uc2ilLmVdL2FjX3N1YjAALm
RgEDAgPMBUCCcGAOUFBwCCMAKGBwQAt+JAQJwYGBACORgFMB0wGaY2ihR0EIMdI59wC2Mu
c2hlLnVdL2VwEwJhYATBGEYASGAQYwCQYHBCORgEgAIAIBNVHSMEGDAWgBfYnEnMnIbc1+
SOL26XktBWBVANBgkqhkiG9w0BAQoFAAOCAgEAc4dWVYLUYUWchPXRDIIBFchlRwcySBedEo
m9mkl-FAFkzKfocvShdsIUcr33M6YmwwA0BwFm3m9hS5Hf-Sap-X3XKXKXgmh0kOCBjm
GMskSmZ0rPIm5ShoKpCa9bX09RMCUYI+9dqDr3yMcdAsy1dkV3NLTVDfBf+ms80bsj
vB82U3b+qZ9T7GB0mZNSyaf84wqOwCsbCuzypAIIHolZ7Muren7BHwSu+ymVrPsgtWfU0
8IuLg75CIBfakId9u0F44grRMLZTRPEXYyITP88lIsewHkMEGVWV5zIovZwaIKz3
5UWoufWdEFH09pNcCeYpV7HlEFkbrKlu6EAY7hblZ6ZCJ4s0bvZagwvkaM4XRawT
pctGBdAAcWtTbVlZc3AKPFY7Q7NqGDa7QcdDAsAZH3gUoiMRkwzZm93AZJvQeAt+u
w08hME8RUEUj0KwW=52384ERocVY40cczXpPawYKfZ7HBIUwP0ssMPgzJdk
hr-jhnpz3qtUsYVYkzrPBNCs2ebXMVJGZSIPvWntIBQESHDpshDMS1YNgzp4w-nDURAGH
x8GISH0Nmao-XUgfnOZR1dseJh6hzZTfwbA=
    
```

-----END CERTIFICATE-----

**Signature algorithm:** SHA256withRSA

**Issuer CN:** SIA SUB01

**Issuer SERIAL NUMBER:** A82733262

**Issuer OU:** QUALIFIED CA

**Issuer O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Issuer C:** ES

**Subject CN:** TSAQC

**Subject 2.5.4.97:** VATES-A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**Valid from:** Fri Dec 01 12:42:49 CET 2017

**Valid to:** Tue Dec 01 13:12:49 CET 2020

**Public Key:**  
30820122300D06092A8648867F0D01010105000382010F003082010A0282010100D6648DA9B4A98570776F8016DF84A15D20992446F79ECD69CAAB350693556D48EC2C4  
 FC27E809F36B0E75DC4E7FC4828C8235C776914653077274854C8A8D86AD8E12FC07F79F89F5034A2AFF9A2F4B872D9178DEC09B6DF37EB78A1FDE564359F6115  
 94C6E09B4B44E90CA071D15E3CE2E2D86D0CB907F396949B6136A091F35E4214753579BC8D0C05634442022377AC37D710215286C200132F9CD01F4096C165D89  
 91EFA3FE887DD2EEB922402B577945DD3A57DFB2D04C285F16D5AD54299D125A8B6D6C8C8D8A51BC9D5BFC1AE98682D759F90EA0CA34016E8CE69C7199017765  
 84F211D1FF65FC98748B6759DBA054861D6A57B62B53210D950203010001

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
[https://psc.sia.es/ac\\_sub01.crl](https://psc.sia.es/ac_sub01.crl)  
[http://psc.sia.es/ac\\_sub01.crl](http://psc.sia.es/ac_sub01.crl)

**Authority Info Access**  
<https://psc.sia.es/ocsp>  
[https://psc.sia.es/ac\\_sub01.crl](https://psc.sia.es/ac_sub01.crl)





**Subject 2.5.4.97:** VATES-A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**Valid from:** Fri Sep 04 13:54:01 CEST 2020

**Valid to:** Mon Sep 04 14:24:01 CEST 2023

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D6648DA9B4A98570776F8016DF84A15D20992446F79ECD69CAAB350693556D48EC2C4  
F4272809E36B0E757DC4E7F4482C8235C778914653077274854CEA3D86AD8E12FC07F79F89F5034A2AFF9A1F24B1F872D9178D1EC0986DF37E7878A1FDE564359F6115  
94C6E09B4BA4E94CA071D15E3CB2E2D856DDCB907F896943B6136A09F35E4214753579BCBC8DCD56344420223377AC37D710215286C20013D2F9CD01F4096CE65DB9  
91EFA3FE887DD2EEB922402B577945DD3A57DFB2D04C285F16D5AD54299D125A8B6D6C8C8DB3A51BC9D3BFC1AE9682D759F90EA0C40345016E8CE69C7199017765  
84FF1211DFF65FC98748B6759DBA054861D6A57B62B53210D950203010001

**Extended Key Usage** *id\_kp\_timeStamping*

**Authority Info Access**  
<https://psc.sia.es/ocsp>  
[https://psc.sia.es/ac\\_sub01.crt](https://psc.sia.es/ac_sub01.crt)

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.39131.10.1.14  
CPS pointer: <https://psc.sia.es>  
CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo.  
Condiciones de uso y vías de contacto en: <https://psc.sia.es>]

Policy OID: 0.4.0.194112.1.1

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
<http://psc.sia.es/crlc10.crl>  
<https://psc.sia.es/crlc10.crl>

**Authority Key Identifier**  
DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 55:A4:10:9A:4E:AA:63:B6:46:1F:DB:B1:1E:1C:0B:AD:A6:E1:8C:DA:DB:45:4F:E5:63:A7:D3:6F:18:BF:57:1C

**X509SubjectName**

**Subject CN:** TSAQC

**Subject 2.5.4.97:** VATES-A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *nrZ7bmnQvpA1gs5HCLWNwxsusSE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-12-21T00:00:00Z*

### 24.2.1 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

## Service Name

**Name** *[en] Qualified timestamps issued by TSAQC*

**Name** *[es] Sellos de tiempo cualificados emitidos por TSAQC*

## Service digital identities

### X509SubjectName

**Subject CN:** *TSAQC*

**Subject 2.5.4.97:** *VATES-A82733262*

**Subject OU:** *QUALIFIED CA*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *nrZ7bmnQvpA1gs5HCLWNwxsusSE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-02-15T01:00:00Z*

### 24.3 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada "SIAVAL"



**Subject C:** ES

**Valid from:** Wed Nov 20 10:31:12 CET 2019

**Valid to:** Sun Nov 20 11:01:12 CET 2022

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100A6ED2B5AEAE05F54A4D23ABBF73F791FE25C2B577DEFC A949AC160B6BC351F7F33  
D13E3E8D34FC5AAEBC2E1EDD07EA483A2F3399E2E308E4510C D1A60B8184711A CFB47399B7BC45CC9E CE819372E61B8C4E426DD457B408238866CE6D59EE4  
DAFECCE58F8B2C7B0BAB06BBDE1F39DF5B6E9C59E87783A1E891EE6EC188FB BB1933D94A AF27D4BF26EE53D24349DC848A07856D5DA2EA96E2BB76639A54B3  
70A10B860FD154FEC8A5C EC024DF92FA9244B176464E06B5FDF41EA7FB049AD C381E396BC56903F38367F75D8031DB3DA09BE EE B1C540D91100E9036E25F31503AB  
BC0F00D4D58E36641C6712339A9B6AFF44FB2E1C2134A0F8BBD2A744B0205010001

**Subject Alternative Name** *OID.1.3.6.1.4.1.39131.10.2.7=A82733262, OID.1.3.6.1.4.1.39131.10.2.6=SISTEMAS  
INFORMATICOS ABIERTOS S.A., OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE  
NIVEL MEDIO*

**Extended Key Usage** *id\_kp\_clientAuth*

**Authority Info Access** *https://psc.sia.es/ocsp  
https://psc.sia.es/ac\_sub01.crt*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.39131.10.1.12  
CPS pointer: https://psc.sia.es  
CPS text: [Certificado cualificado de Sello Electrónico de nivel medio. Condiciones de uso y vías de  
contacto en: https://psc.sia.es]  
Policy OID: 0.4.0.194112.1.1  
Policy OID: 2.16.724.1.3.5.6.2*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://psc.sia.es/crlc4.crl  
https://psc.sia.es/crlc4.crl*

**Authority Key Identifier** *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

**Subject Key Identifier** *C3:93:A3:67:10:16:FC:2A:81:8B:8B:E5:3F:FA:81:EC:13:E8:20:8A*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*

**Thumbprint algorithm:** SHA-256

**Thumbprint:** *B5:AA:55:A4:C5:50:58:F0:AE:92:63:96:18:EE:D9:F1:5D:63:F8:54:63:78:03:8A:9D:BD:92:9A:CB  
:4E:1B:52*

**X509SubjectName**

**Subject CN:** SIAVAL

**Subject OU:** SELLO ELECTRONICO

**Subject 2.5.4.97:** VATES-A82733262

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS S.A.*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *w5OjZxAW/CqBi4vIP/qB7BPoIlo=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-12-22T00:00:00Z*

### 24.3.1 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

## Service Name

**Name** *[es] Servicio cualificado de entrega electrónica certificada "SIAVAL"*

**Name** *[en] Qualified electronic registered delivery service "SIAVAL"*

## Service digital identities

### X509SubjectName

**Subject CN:** *SIAVAL*

**Subject OU:** *SELLO ELECTRONICO*

**Subject 2.5.4.97:** *VATES-A82733262*

**Subject O:** *SISTEMAS INFORMATICOS ABIERTOS S.A.*

**Subject C:** *ES*

## X509SKI

**X509 SK I** *w5OjZxAW/CqBi4vIP/qB7BPoIlo=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2019-12-10T01:00:00Z*



**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**Valid from:** Fri Jul 23 12:54:36 CEST 2021

**Valid to:** Sat Jul 19 12:54:36 CEST 2036

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C595DF85EB0A08FC EB56FCF28CB35F461F7824B0BA4256995C7F4C6BC5E929A4CE66  
B1C45BBA42021595A8B301149B4A8B42BE04F4FD8840BC1F85A90B46D91E1A2AED2D5507CFD34D5D56C9A7B4A91A8A68D391CF41593003140803727397225B3E02  
53794CDEFFA0AC7D88B58E9827EBF213A87B0AE93A2D6CF4129DFF4E7FBE4F3C3E9797BAE1EA918C0F6E04C8BB02518A4495E23C2217F66048A546C0583ABCDDA  
ADEE8952BC993598E85AFEE38C9E5FE28ACC636B045E77237E4FAB2AD6AD8975BC2FB71A3048732B57251E3014C0CAD40E176D58303016DB07C5697BF97F1577C1E5  
294F979DB6C242213FF2E8484ABE8F78C0295C1D31303803F8FE234847888C46A0374F8EC44471E501E4219143685BDFF068EBE2198ECS593CAF72D99D089E79D6BD82  
41236BF97A241549D2A4C6C871683F3CF5842168FC4D5F439779D0721134DD8486E2EC250701FA2C415470B0610464B72E6215E4E6010D7872C625946B3E094A1BE3  
743BDFAE91AD696B951C4BEEC1E1520715B3D73E5DD6CBAE74EDAD6C2C5713C6B5BFC5378A1770715409B896142CDF5600AA842FA18394508B915F91277D72D  
B7DAEC6D9DF6F26D4E3A79DF9325D359EB9298BB469E765536019DB0AB38DF213EC9CB6A92AABEFEEC39F1EE24C6F662962C523F3A004381BB79FCDE6D20D132  
D1E3C40E4FF1EB8B39741E1DBA89E0E0EFB1131CC680203010001

**Basic Constraints** IsCA: true

**Authority Key Identifier** 95:1D:51:F9:FF:61:4D:DC:63:A1:8F:2E:C4:95:C7:22:56:33:72:53

**Authority Info Access**  
[http://psc.sia.es/ac\\_raiz\\_2020.crt](http://psc.sia.es/ac_raiz_2020.crt)  
<http://psc.sia.es/ocsp>

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <http://psc.sia.es/>

**Extended Key Usage** id\_kp\_serverAuth

**CRL Distribution Points** <http://psc.sia.es/arl2020.crl>

**Subject Key Identifier** 5B:58:D8:89:DC:DA:B8:55:32:64:4D:9B:B5:6C:27:9A:07:50:B9:6C

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** B1:02:3E:84:41:80:A7:25:4F:7C:0F:1A:D6:C6:5C:2D:CC:D5:9D:EF:38:80:01:C4:38:0B:CA:73:D  
B:F4:F3:38

**X509SubjectName**

**Subject CN:** SIA SSL SUB01 CA

**Subject 2.5.4.97:** VATES-A82733262

**Subject OU:** QUALIFIED CA

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Subject C:** ES

**X509SKI**

**X509 SK I** W1jYidzauFUyZE2btWwnmgdQuWw=





**Issuer SERIAL NUMBER:** A82733262

**Issuer OU:** QUALIFIED CA

**Issuer O:** SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

**Issuer C:** ES

**Subject CN:** SIAVAL

**Subject OU:** SELLO ELECTRONICO

**Subject 2.5.4.97:** VATES-A82733262

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS S.A.

**Subject C:** ES

**Valid from:** Mon Sep 26 12:37:02 CEST 2022

**Valid to:** Fri Sep 26 13:07:02 CEST 2025

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C733C6595192E49F66AFD13A67D6C646D8DD599BDD899E1089AE6C31B5192EA8921929D3052E4C1F012B299AC428C1A1F3F28EAD784204EB2A55D0278F7E6CC885D7F1E70E5FBDB8EADF11F1E2DC3D632EB090424B35E7465BDD93D716977A324E111F3D55FD2B1094AF0F3EDE635B8844AD20CA7E36B3E0A4BBBE58ABCB3849B875A3236C0EC659A4189AE4D041A79F858DC2236CD9500239D27D7A075D39AC90F77B632B739A380FB28CF005FEA8E6B15CF5AA3030032A38C96CF8A4FA055EA18416D66B07C189C4810139725F2DEA71F74B00CC20D9B3EA3D995558ABCBE34F1F623DADC:AE7E1090650533184FA5259B099FAD1C31827D8BE6AA040D92C20F0203010001

**Subject Alternative Name** *OID.1.3.6.1.4.1.39131.10.2.1=SELLO ELECTRONICO DE NIVEL MEDIO*

**Extended Key Usage** *id\_kp\_clientAuth*

**Authority Info Access**  
<https://psc.sia.es/ocsp>  
[https://psc.sia.es/ac\\_sub01.crt](https://psc.sia.es/ac_sub01.crt)

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.39131.10.1.12*  
*CPS pointer: <https://psc.sia.es>*  
*CPS text: [Certificado cualificado de Sello Electrónico de nivel medio. Condiciones de uso y vías de contacto en: <https://psc.sia.es/>]*  
*Policy OID: 0.4.0.194112.1.1*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
<http://psc.sia.es/crlc46.crl>  
<https://psc.sia.es/crlc46.crl>

**Authority Key Identifier** *DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC*

**Subject Key Identifier** *A0:19:31:0A:1A:7D:CA:E3:54:60:E5:22:F6:D2:1B:F9:45:60:1E:30*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment - keyAgreement*

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 68:17:1A:DD:9F:B5:E4:A8:DB:08:65:8D:17:8D:B1:1F:9A:17:C2:00:76:CF:7C:65:CE:B7:37:C5:6C:E0:BA:7F

**X509SubjectName**

**Subject CN:** SIAVAL

**Subject OU:** SELLO ELECTRONICO

**Subject 2.5.4.97:** VATES-A82733262

**Subject O:** SISTEMAS INFORMATICOS ABIERTOS S.A.

**Subject C:** ES

**X509SKI**

**X509 SK I** oBkxChp9yuNUYOUi9tlb+UVgHjA=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2022-12-22T00:00:00Z

**24.6 - Service (granted): Qualified timestamps issued by TSAQC 2022****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

**Service Name**

**Name** [en] Qualified timestamps issued by TSAQC 2022

**Name** [es] Sellos de tiempo cualificados emitidos por TSAQC 2022

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 614817116171548320148179293635051900945888052447

X509 Certificate

-----BEGIN CERTIFICATE-----

MiHMzCCBrugAwIBAgIUtaFXRSLR/7SpwKIAAAAFAhWBN8wDQYJKoZIhvcNAQELBQAwYzA1B2N0YU90OD06092A3684886F70D01010105000382018F003082018A0282018100ACFF8C5BEEBEFFBF78A240F69613B0A8701EF2AA68D94E3B0EC EA1922899F8AF218C206DE4B4B8753255344A3A5F3884518DA32506E04E1BCE7E489729233DCE0788E3787B88090921571768A66C66F32A29C2CCAE304C991E40DB178F8E12C1BA74143EAB8808687034271A1B4C64E95181B1CB303D3DA2F599637C5C224344D3838DC991850DF17B22C1C978678DBFB5700D6CE2B8A7D55745E04474CC5B42694B6CB4934584AD2911D994C0A5A7B709FB5C4AFC5B5A1D1C98DFD771B8FEACD1D6CEB2A04FE568EAFA0B0D624346169BA4CE66D675A1A00ACB9DB44133791B23E4277E83726EA30A12EA740F78C55C579CEA28A87634E5B744F69808180FC88EC3D4F843C2E8F22D004290F598C7918B99150C4E66C24E79457E7FC42094B335AA4FAC A567F14D565F1060808F54DA121E5FC7D89D7D215FC6C214617B86DE2632330E85C82BA7B0E86A2024EFBE C86565617CA2592D8D859534379C BD8771944970693AC23431F47CA44642A8757F7FAA2066AB64237E634751930203010001

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer CN:

SIA SUB01

Issuer SERIAL NUMBER:

A82733262

Issuer OU:

QUALIFIED CA

Issuer O:

SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Issuer C:

ES

Subject CN:

TSAQC 2022

Subject 2.5.4.97:

VATES-A82733262

Subject OU:

QUALIFIED CA

Subject O:

SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA

Subject C:

ES

Valid from:

Thu Nov 24 10:44:49 CET 2022

Valid to:

Tue Jan 29 11:26:43 CET 2030

Public Key:

308201A2300D06092A3684886F70D01010105000382018F003082018A0282018100ACFF8C5BEEBEFFBF78A240F69613B0A8701EF2AA68D94E3B0EC EA1922899F8AF218C206DE4B4B8753255344A3A5F3884518DA32506E04E1BCE7E489729233DCE0788E3787B88090921571768A66C66F32A29C2CCAE304C991E40DB178F8E12C1BA74143EAB8808687034271A1B4C64E95181B1CB303D3DA2F599637C5C224344D3838DC991850DF17B22C1C978678DBFB5700D6CE2B8A7D55745E04474CC5B42694B6CB4934584AD2911D994C0A5A7B709FB5C4AFC5B5A1D1C98DFD771B8FEACD1D6CEB2A04FE568EAFA0B0D624346169BA4CE66D675A1A00ACB9DB44133791B23E4277E83726EA30A12EA740F78C55C579CEA28A87634E5B744F69808180FC88EC3D4F843C2E8F22D004290F598C7918B99150C4E66C24E79457E7FC42094B335AA4FAC A567F14D565F1060808F54DA121E5FC7D89D7D215FC6C214617B86DE2632330E85C82BA7B0E86A2024EFBE C86565617CA2592D8D859534379C BD8771944970693AC23431F47CA44642A8757F7FAA2066AB64237E634751930203010001

Extended Key Usage

id\_kp\_timeStamping

Authority Info Access

https://psc.sia.es/ocsp

https://psc.sia.es/ac\_sub01.crt

**Certificate Policies***Policy OID: 1.3.6.1.4.1.39131.10.1.25**CPS pointer: <https://psc.sia.es>**CPS text: [Certificado de servicio de expedición de sellos electrónicos cualificados de tiempo. Condiciones de uso y vías de contacto en: <https://psc.sia.es>]**Policy OID: 0.4.0.2042.1.2***CRL Distribution Points***<http://psc.sia.es/crlc50.crl>**<https://psc.sia.es/crlc50.crl>***Authority Key Identifier***DA:60:D1:27:30:D2:26:85:CD:7E:48:E2:F6:E9:79:1F:5A:30:55:AC***Subject Key Identifier***A8:CD:60:77:23:67:9B:2C:13:FE:FD:08:B9:36:A5:83:EE:90:C9:A8***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***E8:F7:5A:D5:CE:08:97:D9:5A:FD:CA:AC:28:75:82:11:68:7E:A4:0D:3F:CE:D0:1C:80:6A:CA:08:5E:64:3D:1E***X509SubjectName****Subject CN:***TSAQC 2022***Subject 2.5.4.97:***VATES-A82733262***Subject OU:***QUALIFIED CA***Subject O:***SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA***Subject C:***ES***X509SKI****X509 SK I***qM1gdyNnmywT/v0luTalg+6Qyag=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2022-12-22T00:00:00Z*

**25 - TSP: COLORIURIS, S.L****TSP Name**

**Name** [ en ] *COLORIURIS, S.L*

**Name** [ es ] *COLORIURIS, S.L*

**TSP Trade Name**

**Name** [ en ] *Coloriuris, Prestador de Servicios de Confianza (CIPSC)*

**Name** [ es ] *Coloriuris, Prestador de Servicios de Confianza (CIPSC)*

**Name** [ en ] *VATES-B99091696*

**Name** [ en ] *Coloriuris S.L.*

**PostalAddress**

**Street Address** [ en ] *C/ Alfonso I nº 23, entresuelo centro*

**Locality** [ en ] *Zaragoza*

**State Or Province** [ en ] *Zaragoza*

**Postal Code** [ en ] *50003*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ Alfonso I nº 23, entresuelo centro*

**Locality** [ es ] *Zaragoza*

**State Or Province** [ es ] *Zaragoza*

**Postal Code** [ es ] *50003*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *https://cipsc.coloriuris.net/*

**URI** [ en ] *mailto:info@coloriuris.net*

**URI** [ es ] *mailto:info@coloriuris.net*



**Issuer L:** Zaragoza

**Issuer O:** Coloriuris S.L.

**Issuer OU:** Prestador de Servicios de Confianza

**Issuer SERIAL NUMBER:** B99091696

**Issuer CN:** CIPSC - Raíz de la Autoridad de Certificación

**Issuer E:** cipsc@coloriuris.net

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:** B99091696

**Subject CN:** CIPSC - Subautoridad de emisión de certificados de persona física

**Subject E:** cipsc@coloriuris.net

**Valid from:** Tue Jul 14 12:15:10 CEST 2015

**Valid to:** Mon Jul 14 12:15:10 CEST 2025

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100E33BD077B958C88054905D2EAB10DBDA836024BAD0363445B1A6BA5A2B D7C1B51F43  
2A13F0C051D30066EC09FDCC3DD45242A2690C8E7AD51B5DF04359C989C72A875B1BAF9A21F8010832ECCF813541AF727A80A0D A6C5A847B559BAE7C3533741ED7  
A393943FA36CD88164C0E99A57F32056E F970F3E4C8EA25D57330E3678C3B441E5E0AD947F5285D1FAC98EB648532E3E3C70210B8D84751CB D18F9F96AF5B08B1413  
E471861BA5205DFDA CCFB F4ADBF D8636B7B4208C46CA732B86299944FC41954F1A40893C0E439604BA4C9E763C92F931240E82DB4B59026785A4051734043A5968BE  
E70B1C3F87A57A7DA45890459021C990CF65884522F7930D550203010001

**Authority Info Access**  
<https://cipsc.coloriuris.net/certificados/ac/raiz.crt>  
<https://ocsp.coloriuris.net>

**Subject Key Identifier**  
02:E9:6A:2F:B2:05:D3:1B:63:FB:3C:C0:C5:92:6A:0B:FF:2D:83:29

**Basic Constraints**  
IsCA: true

**Authority Key Identifier**  
79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0  
CPS text: [SubAutoridad CIPSC para emisión de certificados de firma electrónica para persona física]  
CPS pointer: <https://cipsc.coloriuris.net/politicas/>

**CRL Distribution Points**<https://cipsc.coloriuris.net/crl/ac/ac.crl>

CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

D8:23:77:C5:2B:28:D8:A9:39:40:35:B2:8B:71:3A:62:1C:C0:49:DA:5E:BC:D1:7F:F9:A3:8C:5F:25:EA:1A:6D

**X509SubjectName****Subject C:**

ES

**Subject L:**

Zaragoza

**Subject O:**

Coloriuris S.L.

**Subject OU:**

Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:**

B99091696

**Subject CN:**

CIPSC - Subautoridad de emisión de certificados de persona física

**Subject E:**

cipsc@coloriuris.net

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2017-07-01T22:00:00Z

**25.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI**

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**25.1.2 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service Name****Name**

[en]

Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física



**Name** [ es ] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

### Service digital identities

#### X509SubjectName

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:** B99091696

**Subject CN:** CIPSC - Subautoridad de emisión de certificados de persona física

**Subject E:** cipsc@coloriuris.net

#### X509SKI

**X509 SK I** AulqL7IF0xtj+zzAxZJqC/8tgyk=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

#### 25.1.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 25.1.3 - History instance n.2 - Status: undersupervision

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [ en ] *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona física*

**Name** [ es ] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona física*

### Service digital identities

**X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:** B99091696

**Subject CN:** CIPSC - Subautoridad de emisión de certificados de persona física

**Subject E:** cipsc@coloriuris.net

**X509SKI**

**X509 SK I** AulqL7IF0xtj+zzAxZJqC/8tgyk=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2015-10-19T22:00:00Z

## 25.2 - Service (withdrawn): Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica

**Name** [es] Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 3581065887593727996



**Authority Info Access** <https://cipsc.coloriuris.net/certificados/ac/raiz.crt>  
<https://ocsp.coloriuris.net>

**Subject Key Identifier** 35:7F:37:8F:21:EE:4F:0A:68:00:7A:A7:A2:41:B1:E1:95:3A:D1:AE

**Basic Constraints** IsCA: true

**Authority Key Identifier** 79:21:E1:5C:A1:F1:96:7C:D7:A0:36:89:66:B4:A5:AB:E4:36:71:A6

**Certificate Policies** Policy OID: 1.3.6.1.4.1.37799.0.3.1.2.0  
 CPS text: [SubAutoridad CIPSC para emisión de certificados para sello electrónico de persona jurídica]  
 CPS pointer: <https://cipsc.coloriuris.net/politicas/>

**CRL Distribution Points** <https://cipsc.coloriuris.net/crl/ac/ac.crl>  
 CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz de la Autoridad de Certificación,SERIALNUMBER=B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 2B:03:88:BB:3A:37:32:FD:55:1B:21:BE:FE:2F:6D:6C:18:D0:FC:76:20:BD:31:EC:C3:4F:71:43:7F:DE:B2:E7

**X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:** B99091696

**Subject CN:** CIPSC - Subautoridad de emisión de certificados de persona jurídica

**Subject E:** cipsc@coloriuris.net

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2017-07-01T22:00:00Z

**25.2.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.1.2.1

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.1.2.2

### 25.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 25.2.3 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

**Name** [en] *Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

**Name** [es] *Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

#### Service digital identities

##### X509SubjectName

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject SERIAL NUMBER:** B99091696

**Subject CN:** CIPSC - Subautoridad de emisión de certificados de persona jurídica

**Subject E:** cipsc@coloriuris.net

**X509SKI**

**X509 SK I** *NX83jyHuTwpoAHqnokGx4ZU60a4=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**25.2.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.37799.20.1.2.1*

**Policy Identifier:**

**Identifier** *[ OIDsURN ] urn:oid:1.3.6.1.4.1.37799.20.1.2.2*

**25.2.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**25.2.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ] Qualified Certificates issued by - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

**Name** *[ es ] Certificados Reconocidos emitidos por CA - CIPSC - Subautoridad de emisión de certificados de persona jurídica*

**Service digital identities****X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Zaragoza*

**Subject O:** *Coloriuris S.L.*

**Subject OU:** *Prestador de Servicios de Confianza*

**Subject SERIAL NUMBER:** *B99091696*

**Subject CN:** *CIPSC - Subautoridad de emisión de certificados de persona jurídica*

**Subject E:** *cipsc@coloriuris.net*

**X509SKI**

**X509 SK I** *NX83jyHuTwpoAHqnokGx4ZU60a4=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2015-10-19T22:00:00Z*

#### 25.2.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	<i>[en]</i>	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	<i>[es]</i>	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

#### **Criteria list assert=atLeastOne**

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.1*

##### **Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.37799.20.1.2.2*

#### 25.3 - Service (withdrawn): Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

<b>Service type description</b>	<i>[en]</i>	<i>A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.</i>
	<i>[es]</i>	<i>Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.</i>

#### **Service Name**

**Name** *[ en ]* *Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*





**Subject E:** *cipsc@coloriuris.net*

**Valid from:** *Thu Sep 10 10:13:25 CEST 2015*

**Valid to:** *Wed Sep 10 10:13:25 CEST 2025*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D5DDCD663FEC79032CB9E73C4333DB00FA17A79CA31234D6043DA A64BC3197E E9D  
87A81C21083D0F39A767E8013E514B233A2BF8C52C7B36BDD75587F6D4E37EAD43A0F6339432A557337EA7CCBD269F58EA6A6CB805C9A04EF46B15FDCED3A93B4F  
5A11604E914807D28B92A3D4679249C21DCBB C364C582A06842EA FE0E9B5517BE C7D52D08270B C4BA970970A9293C85E9093E CD AE D508 CF4C 50F2 CF F1 E2 F4 37 4A 4  
09B3C2535DA7B45DD74D65406C884FCF0C77929F2B6AB C59C491C5D9830D648CC A00B C796CEFB1F7E B98B2B2F57CD A2E6FE DB3E3B8910E2FE70A15A916E4D6F4D  
8B28218C74981A6966A850E7C81E DA A226EF E30D239B D419E2062A DB0203010001

**Authority Info Access**  
*https://cipsc.coloriuris.net/certificados/ac/raiz-v3.crt*  
*https://ocsp.coloriuris.net*

**Subject Key Identifier**  
*7B:21:D2:FB:DA:8B:81:0D:06:3F:4F:8A:6B:7C:C9:A7:DE:5C:95:7B*

**Basic Constraints**  
*IsCA: true - Path length: 2*

**Authority Key Identifier**  
*56:0E:2D:3E:8C:F4:9F:C3:BF:7E:2B:E7:A7:BD:1B:53:14:01:28:EA*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: https://cipsc.coloriuris.net/politicas/*

**CRL Distribution Points**  
*https://cipsc.coloriuris.net/crl/ac/ac-v3.crl*  
*CRL issuer: 4: E=cipsc@coloriuris.net, CN=CIPSC - Raíz - Autoridad de  
Certificación, 2.5.4.97=VATES-B99091696, OU=Prestador de Servicios de Confianza, O=Coloriuris  
S.L., L=Zaragoza, C=ES*

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*55:01:5F:B9:D2:CD:21:76:57:32:A2:34:0E:53:E4:18:4F:0C:0D:57:F7:6E:3B:4F:08:03:B6:C1:56:F  
F:BB:1E*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Zaragoza*

**Subject O:** *Coloriuris S.L.*

**Subject OU:** *Prestador de Servicios de Confianza*

**Subject 2.5.4.97:** *VATES-B99091696*

**Subject CN:** *CIPSC - Emisión de certificados de persona jurídica*

**Subject E:** *cipsc@coloriuris.net*

**Service Status**  
*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

[es] undefined.

**Status Starting Time** 2017-07-01T22:00:00Z**25.3.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** [en] undefined.  
 [es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.2

**25.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**25.3.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica*

**Name** [es] *Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject OU:** Prestador de Servicios de Confianza

**Subject 2.5.4.97:** VATES-B99091696

**Subject CN:** *CIPSC - Emisión de certificados de persona jurídica*

**Subject E:** *cipsc@coloriuris.net*

**X509SKI**

**X509 SK I** *eyHS+9qLgQ0GP0+Ka3zJp95clXs=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2016-06-30T22:00:00Z*

**25.3.3.1 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	<i>[OIDAsURN]</i>	<i>urn:oid:1.3.6.1.4.1.37799.20.2.2.1</i>
-------------------	-------------------	---

**Policy Identifier:**

<b>Identifier</b>	<i>[OIDAsURN]</i>	<i>urn:oid:1.3.6.1.4.1.37799.20.2.2.2</i>
-------------------	-------------------	---

**25.3.3.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

<b>URI</b>	<i>[en]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	-------------	--

**25.3.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

<b>Name</b>	<i>[en]</i>	<i>Qualified Certificates issued by - CIPSC Emisión de certificados de persona jurídica</i>
-------------	-------------	---

<b>Name</b>	<i>[es]</i>	<i>Certificados Reconocidos emitidos por CA - CIPSC Emisión de certificados de persona jurídica</i>
-------------	-------------	---

**Service digital identities**

**X509SubjectName**

Subject C: ES

Subject L: Zaragoza

Subject O: Coloriuris S.L.

Subject OU: Prestador de Servicios de Confianza

Subject 2.5.4.97: VATES-B99091696

Subject CN: CIPSC - Emisión de certificados de persona jurídica

Subject E: cipsc@coloriuris.net

**X509SKI**

X509 SK I eyHS+9qLgQ0GP0+Ka3zJp95clXs=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time 2015-10-19T22:00:00Z

**25.3.4.3 - Extension (critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	<i>it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.</i>
	[es]	<i>está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.1

**Policy Identifier:**

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.37799.20.2.2.2

**25.4 - Service (withdrawn): Qualified timestamps issued by Coloriuris (TSACI)**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	<i>A time-stamping generation service creating and signing qualified time-stamps tokens.</i>
	[es]	<i>Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.</i>



**Subject CN:** CIPSC - v3 - Emisor de sellos de tiempo de 2048

**Valid from:** Tue Jul 04 18:27:29 CEST 2017

**Valid to:** Sun Jul 04 18:27:29 CEST 2027

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100ADF1213ADC3C412811979CE89BA749EFCFC9902399037EF66D6545F5D82CA7D130B5D131C3854321E2E2F7B617A6726F090F7F99F8688C4987CD2E5D8B2E4880D62AAFD5F22F6B7ACF11E5D893AC0945E1933D12C9E544B5AA2AC7D8E026C913B2CE4E86EB7CCDF1FD8B0FC5FE402DD307907AAE88049D803EA3194E53533DC32B7B65DCCED6717FECE1A487192904BAC05F75CC46E4544121BA891327F4B60A0651E6B2E64189EF175D6406D7D6C3D7C7F00F9F499BEF8F877BE2112CF5D15017F18341732FCDS57212764769FA23358EA6714DB0DC34277F242534886BE38AF96C4D05B30028133346005FED3D441824F34B6DF7E44F67404F4E28B9D70203010001

**Authority Info Access**  
<https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.crt>  
<https://ocsp.coloriuris.net>

**Subject Key Identifier**  
60:62:82:B7:28:58:B6:EF:BA:9C:7B:7F:BA:73:08:34:81:88:01:CB

**Authority Key Identifier**  
67:FF:D4:BC:47:58:FF:3C:0A:89:AF:9D:B0:2A:EF:FC:02:5C:2A:5A

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.37799.20.5.1  
 CPS text: [Certificado cualificado de emisión de sellos de tiempo electrónicos]  
 CPS pointer: <https://cipsc.coloriuris.net/politicas/>

**CRL Distribution Points**  
<http://cipsc.coloriuris.net/crl/tsa/tsa-v3.crl>  
 CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

**Extended Key Usage**  
id\_kp\_timeStamping

**Key Usage:**  
digitalSignature - nonRepudiation

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
D8:9C:1C:4E:94:77:B4:76:8B:1C:46:F7:E1:61:29:54:1C:CD:E1:99:51:A4:91:2A:F6:57:43:E7:BD:55:13:BE

**X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject 2.5.4.97:** VATES-B99091696

**Subject CN:** CIPSC - v3 - Emisor de sellos de tiempo de 2048

**X509SKI**

**X509 SK I** YGKCyhYtu+6nHt/unMINIGIAcs=

<b>Service Status</b>		<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn</a>
<b>Service status description</b>	[en]	undefined.
	[es]	undefined.
<b>Status Starting Time</b>		2023-10-24T00:00:00Z

#### 25.4.1 - History instance n.1 - Status: granted

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST">http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</a>
<b>Service Name</b>		
<b>Name</b>	[en]	Qualified timestamps issued by Coloriuris (TSACI)
<b>Name</b>	[es]	Sellos de tiempo cualificados emitidos por Coloriuris (TSACI)

#### Service digital identities

##### X509SubjectName

<b>Subject C:</b>	ES
<b>Subject L:</b>	Zaragoza
<b>Subject O:</b>	Coloriuris S.L.
<b>Subject 2.5.4.97:</b>	VATES-B99091696
<b>Subject CN:</b>	CIPSC - v3 - Emisor de sellos de tiempo de 2048

##### X509SKI

<b>X509 SK I</b>	YGK Ctyh Ytu+6nHt/unMINIGIAcs=
------------------	--------------------------------

<b>Service Status</b>		<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
<b>Status Starting Time</b>		2017-09-27T10:00:00Z

#### 25.5 - Service (granted): Qualified timestamps issued by Coloriuris (TSACI) v3.1

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST">http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</a>
<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.
<b>Service Name</b>		
<b>Name</b>	[en]	Qualified timestamps issued by Coloriuris (TSACI) v3.1





**Valid to:** Wed Apr 05 13:35:35 CEST 2028

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:CD:9A:9F:A6:4A:77:EB:40:13:3B:1C:68:AA:F2:8C:F7:A9:E9:3C:28:06:A6:8D:DB:98:19:48:E0:18:33:25:B2:E2:87:9C:DC:34:3B:50:EC:3E:99:BE:89:F1:69:7B:F1:5D:7C:C2:D8:FD:97:07:46:E9:F2:9A:A3:A6:00:30:A6:EB:7E:2B:3D:4E:26:B8:45:F1:31:BC:31:C8:55:83:4A:1D:08:F8:ED:D2:BE:B1:CK:3D:AE:CE:C4:FA:7E:3F:19:C2:A4:75:F4:1F:41:62:9D:4B:F8:CD:26:65:D6:A3:2F:54:12:9D:31:8B:58:48:70:5E:48:B3:06:98:1A:11:AD:22:1B:03:DB:CE:E9:F3:A5:A4:9A:F1:FB:47:39:B1:49:C4:ED:73:CD:46:8B:41:85:23:BA:5E:66:1D:2D:C8:1E:0A:D3:B3:80:19:4C:6D:A0:F7:B7:14:71:4E:95:7A:95:11:3C:0C:AF:65:45:E9:BS:A3:88:7B:F5:45:17:2A:7E:CD:AE:A8:49:21:07:F0:AE:58:67:AB:F6:6A:65:CE:4D:21:FF:D8:85:14:53:59:35:34:7B:53:B4:73:FF:6C:D3:C5:46:C2:33:5A:55:08:5A:4D:59:1C:E9:BE:EA:1D:D1:CD:D1:62:AE:4E:4D:89:89:1C:5F:E7:37:DE:FF:01:02:03:01:00:01

**Authority Key Identifier** 11:BC:35:3C:F5:EC:13:26:0E:60:43:B5:F8:86:A8:4E:1D:27:01:6A

**Authority Info Access**  
<https://cipsc.coloriuris.net/certificados/tsa/raiz-v3.1.crt>  
<https://ocspv3.coloriuris.net>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.37799.20.5.1  
 CPS pointer: <https://cipsc.coloriuris.net/politicas/>  
 CPS text: [Certificado de emisión de sellos electrónicos cualificados de tiempo]

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://cipsc.coloriuris.net/crl/tsa/tsa-v3.1.crl>  
 CRL issuer: 4: E=cipsc@coloriuris.net,CN=CIPSC - Raíz - Autoridad de Sellado de Tiempo v3.1,2.5.4.97=VATES-B99091696,OU=Prestador de Servicios de Confianza,O=Coloriuris S.L.,L=Zaragoza,C=ES

**Subject Key Identifier** 7E:5A:DB:1E:ED:2E:13:B5:89:50:AC:5E:C2:3D:54:AA:7B:23:82:AC

**Key Usage:** digitalSignature - nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 6C:17:A0:5F:0C:77:B9:6A:B0:39:A3:F8:50:58:73:1E:EB:02:F5:2F:B6:6D:87:D1:9B:93:D2:27:8D:82:64:99

**X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza

**Subject O:** Coloriuris S.L.

**Subject 2.5.4.97:** VATES-B99091696

**Subject CN:** CIPSC - v3.1 - Emisor de sellos electronicos cualificados de tiempo de 2048

**X509SKI**

**X509 SK I** flrbHu0uE7WJUKxewj1Uqnsjgqw=

**Service Status**  
<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time** 2018-05-24T00:00:00Z

**26 - TSP: UANATACA, S.A****TSP Name**

**Name** [ en ] UANATACA, S.A

**Name** [ es ] UANATACA, S.A

**TSP Trade Name**

**Name** [ en ] UANATACA

**Name** [ es ] UANATACA

**Name** [ en ] UANATACA S.A.

**Name** [ en ] VATES-A66721499

**Name** [ en ] Uanataca S.A.

**PostalAddress**

**Street Address** [ en ] Avda. Meridiana núm 350 Planta 3

**Locality** [ en ] Barcelona

**State Or Province** [ en ] Barcelona

**Postal Code** [ en ] 08027

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] Avda. Meridiana núm 350 Planta 3

**Locality** [ es ] Barcelona

**State Or Province** [ es ] Barcelona

**Postal Code** [ es ] 08027

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ en ] <mailto:info@uanataca.com>

**URI** [ en ] <http://www.uanataca.com>

## TSP Information URI

URI [en] <http://www.uanataca.com>

URI [es] <http://www.uanataca.com>

## 26.1 - Service (granted): Qualified Certificates issued by UANATACA CA1 2016

## Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

## Service Name

## Name

[en]

Qualified Certificates issued by UANATACA CA1 2016

## Name

[es]

Certificados Reconocidos emitidos por UANATACA CA1 2016

## Service digital identities

## Certificate fields details

## Version:

3

## Serial Number:

6611671282825056795

## X509 Certificate

-----BEGIN CERTIFICATE-----

```
MIIWjCCBKKgAwIBAgIw8FgAGhwUhsWDOY/KoZbhcNAQELBQAwbGhxCzAJBgNVBAYTAkVTMUMw
QgYDVQOHDEKYYXZlV3VvbmZuKUNZS29idXpZW50IGZlZHUlc3MeYXQgaS4EInVhbmF0YW50b2
bS9hZGRvZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90
MRswQYDVQQDDBIvVQU/SBVEFDQSBST09U/IDJwMTYyGDAWBgNVBGEEMDIZBVEVTLUE2NEcyMTQ3
0TAcFudnYAMTEAMDM1M2NzNDUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUy
QmFyY2Vsb25hZChzZUluY3VycmVudChzZGRyZXRyZXRyZXRyZXRyZXRyZXRyZXRyZXRyZXRyZXRy
cykxZjAU/BgNVBAAgMDVVBTRF1UQU/NBIFMuoQSAjTATHgNVBAsMDFR1UC1VQU/SBVEFDQTEaMBGGA
AUEAwRUVFOVBR0EgQdEldDwMTYyGDAWBgNVBGEEMDIZBVEVTLUE2NEcyMTQ30TAcFudnYAMTEAM
DM1M2NzNDUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUyOTUy
hvcNAQEBBQADgglPADCcAgoCggIBAN/2JPM78ximmGKZxG7CEHN90rwbFzDwBGaWBW4b
wko/Hh9qgEBy4uyl3kqg+mJly8DeymbkLx+9m9A/NR/W4QW9U/OvC168R5v3B/RKR
JLXh8r1VotAul/ENKw1Bq9wNl/Rek5H/TeXcajDVA7a/R90z2m/TLPOC00/1TuzzzZ9+rt
IZvQU/BCsAB2x5udn0awml/DatwLoas+2kGHI1p2FOuAg5HTjpsC8Di5x45+99oIf
+V341A/O0bc/CRGS2u/dI0bcXdurauV0Q6k7RwvK2NEyXCS3HML9VXYH49UhgRB+36uPNDJ
cOILB9-G/0XAVDNDuOZHG6/0y/0T/SeapScdy/WYLCsM/RJX2ANWYndZ+OKJ08at/dec/oc60G
A0763D+q4ZAVwv741Dsu9DNNz/Puz0kZ3Rfj00lo+uYpCy/Bh/RyWZ0D019J5xw1
ghHYZFcl/H9B0bVGebmcaZzy/whbTITSoaR/GHge3IZwskystb/DZw4E1dNWR4D6Kmp9mM0Pgm
5vnt/sg8Yg9wvow3LWYU/G9G7HLLy/uzscb7NwJGAg590w9mDvy/gbvaV9HnXVLLI
VBYJbD0cv7KsN/J8fct8B7gnXzAgMBAAGggGjMIICXZB-BggR/BgEFFBQCBABQ/MHAWNgYKwYB
BQUHMAAGKmb0HAA6L99Y3NwAM51YW/shdGfYSSj620wchVibGjLL3Bra59vY3NwLzABggR/BgEF
BQwAYYqHREKdwl29c3YLVhbmF0YW50b2bS9hZGRvZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90
BBQce+wY3/lcCDIKR/RBAwG/UNSTASBgNVHRMBAf8ECCDAGAQH/AgEAMB8GA1UdlwQYMBaAFFUs
8ybXrmooc+1Vx/BbJb3kZosMBwGA1UdeGQVMB0BEWluZm9AdWFrYXRyY2EuY29mHIMBGNVHSAE
gQwagFngB8BFLdLAw8w1wMwYKwYBBOJUAAGFwZD0d0A6L993dScuWFrYXRyY2EuY29mL3B1
Ym9pYy9wa2kZHBjLzB-BggR/BgEFFBQCBABY/DHBDZJ0aWZpY2F3byBkZSBySFBFbnRnZGFRIGRl
IENlcikpZmlhYW50b2bS9hZGRvZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90
Yw/shdGfYSSj620wchVibGjLL3Bra59mwyYXsX3VhbmF0YW50b2bS9hZGRvZG90ZG90ZG90ZG90
cmwL/VhbmF0YW50b2bS9hZGRvZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90
dHRwO8vY3Jm51YW/shdGfYSSj620wchVibGjLL3Bra59mwyYXsX3VhbmF0YW50b2bS9hZGRvZG90
BgNVQ0BAIEBAQCAQYwQYDVQDQ3IEAUEGZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90ZG90
cFhzZkp1u102cmqBzLkewJZvllHrAgcxsZplXO7PpWcUAX87KJUL7H0wVYDapLTCeG0s1
xykxZLH6kryG6fFqgk9mPQjB8smAGOPcmIRYR2b7GjN9JUVI/Zbbf7BhQgPw+Gw
46/rK7r/SFQdHh86sm1c8mXcvYsQJgrecK06X89pWwGouVv5s4JFEZ3ARCTDRH
Dzx/M9B70cyvhwVv6Mgxa0TPwM31B6/SFNrwee+X0eGncaxv6rLJld0dx+3KXODtblays
zHG99Msauch118QJ/BpWukdCsfWw4FAZAbdW4YRfWx2CIG1J3mWhTMS948BecOM0
6dsZFTXqk3AulTYZAWpwsZAEU/SuqfTnyapjRDKKESVsmfBAmgztY2s2H4+L+Q8
/SmehgaVho35uSuaM6068eY12wdebf-GL+O9KrcceU/RXAbU/PASf0mICNugWZCKM1K159y6
xtFA+mfGDej700kx19HZZh2k28zEgQc0QzPz1wslgUcVXps4N8o7GsrASRy7MZV1mm42s
SS9IgaKvaXw62WMFp6c7XhZUC0C1QyIKQyW09z9W
```

-----END CERTIFICATE-----

## Signature algorithm:

SHA256withRSA

## Issuer 2.5.4.97:

VATES-A66721499

## Issuer CN:

UANATACA ROOT 2016

## Issuer OU:

TSP-UANATACA

## Issuer O:

UANATACA S.A.

**Issuer L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Issuer C:** *ES*

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *UANATACA CA1 2016*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *UANATACA S.A.*

**Subject L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Subject C:** *ES*

**Valid from:** *Fri Mar 11 11:35:33 CET 2016*

**Valid to:** *Sun Mar 11 11:35:33 CET 2029*

**Public Key:**  
30820223300D06092A864886F70D01010105000382020F003082020A0282020100DFFD893CCFFC8B126D9E71A42D9F311BB0841CDF4E8ABC1B171CC3F046696056E  
1BC25A091F0F6F80405D6386BF7C8B9C8DF792087E98922BCBC0D0C260E4531FBFF66F406C8351FD6E105BD0B3AF09FD7AF11E6FDC17FC2242918C8B3BCC6F3356  
8E00B94236364593BC1ABF2F235445E2BC1F8FD37B1C6A82D0D503B68DCD1A23DB39932CF4340ADD0E4C8B8ABFF365BFAF7F5899FEF41451B0AC001DB1E6E767A7  
46B09A5FC3BAD14A1AB5EDBC7061E2D73A53D8E14EB808391D38EB8DEA82F0389FE7E21E7EAFDF6821F95DF84C020ED1A0A2091192DBFB93748D1B71776EAD  
AB95D3F43A2B8462BF0936344C97E524B77C2FD557607E3D521A9107EDAB8E34374971053404F786FEDD173150CD2303991C6880D327D44A880E49C745C9660994  
2B79F0264257A7600D59899D66F40A210F1A51D79E12873AD06034EFADE30FEAB8859015C30EC9E350ECBBD0C0D378CE23EEAF3D24671DDFF1F8CE008A3E8983DC  
B72FC16C78D1CAD599D03A08223F48E57C35825A8761914170B1FD04E85519E6E679A686672FE1C1B4DF4D2A1A44620781ED5670B3E932B34C83656E044DD356478  
0E72A6F6034CD0F1A6E6FEA752DA80F18829A30CA8C372D66086B51A5F464C7B4B8E3FEEB1971B23B3562063604B0470F6D983CA2FE0B5BC8EE572F47B8D5ED54B9  
2555F85825B0CE7AFE44A4C34927C15C87C05380DC730203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Authority Key Identifier**  
*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

**Issuer Alternative Name**  
*info@uanataca.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://www.uanataca.com/public/pki/dpc/>*  
*CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver <http://www.uanataca.com/public/pki/dpc/>]*

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*35:A9:92:84:A2:20:78:9B:A0:E0:62:EE:FF:1B:5F:2F:74:BE:43:75:44:69:97:7C:B3:18:C7:C8:6A:D  
4:8F:9F*

**X509SubjectName**

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2016

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Subject C:** ES

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time**

2019-10-28T01:00:00Z

**26.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**26.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.1.6

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.1.6.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.2.6.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.3.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.4.6.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.7.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.8.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.9.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.11.6

**Description****26.1.4 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by UANATACA CA1 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por UANATACA CA1 2016*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2016

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Subject C:** ES

**X509SKI**

**X509 SK I** LXHvsGN/9f3ggyJEf0QQMIFPTeU=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2019-06-24T00:00:00Z

**26.1.4.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.1.4.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**26.1.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [en] undefined.  
[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.1.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.1.6.2

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.2.6.2

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.3.6
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.4.6.2
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.7.6
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.8.6
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.9.6
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.11.6
<b>Description</b>		

**26.1.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by UANATACA CA1 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por UANATACA CA1 2016*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *UANATACA CA1 2016*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *UANATACA S.A.*

**Subject L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Subject C:** *ES*



**X509SKI****X509 SK I** *LXHvsGN/9f3ggyJEf0QQMIFPteU=***Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time** *2018-02-15T01:00:00Z***26.1.5.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures***26.1.5.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals***26.1.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]****Qualifier type description** *[ en ]* *undefined.*  
*[ es ]* *undefined.***Criteria list assert=atLeastOne****Policy Identifier:****Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47286.1.1.6***Policy Identifier:****Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47286.1.1.6.2***Policy Identifier:****Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47286.1.2.6.2***Policy Identifier:****Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47286.1.3.6***Policy Identifier:****Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47286.1.4.6.2*

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.7.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.8.6

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47286.1.9.6

**Description****26.1.6 - History instance n.3 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by UANATACA CA1 2016*

**Name** [ es ] *Certificados Reconocidos emitidos por UANATACA CA1 2016*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2016

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Subject C:** ES

**X509SKI**

**X509 SK I** LXHvsGN/9f3ggyJEf0QQMIFPTeU=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

**26.1.6.7 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47286.1.3.2

**26.1.6.8 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.1.7 - History instance n.4 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by UANATACA CA1 2016*

**Name** [es] *Certificados Reconocidos emitidos por UANATACA CA1 2016*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2016

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Subject C:** ES

**X509SKI**

X509 SK I

LXHvsGN/9f3ggyJEf0QQMIFPTeU=

Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

Status Starting Time

2016-06-14T22:00:00Z

**26.1.7.9 - Extension (critical): Qualifiers [QCForLegalPerson]**

Qualifier type description	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.3.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47286.1.3.2
------------	-------------	---------------------------------

**26.2 - Service (granted): Qualified Certificates issued by UANATACA CA2 2016**

Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name	[ en ]	Qualified Certificates issued by UANATACA CA2 2016
------	--------	--

Name	[ es ]	Certificados Cualificados emitidos por UANATACA CA2 2016
------	--------	--

**Service digital identities**

Certificate fields details

Version:	3
----------	---

Serial Number:	2317042835735686419
----------------	---------------------



**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** *55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

**Issuer Alternative Name** *info@uanataca.com*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: http://www.uanataca.com/public/pki/dpc/*  
*CPS text: [Certificado de la Entidad de Certificación subordinada de UANATACA. Ver http://www.uanataca.com/public/pki/dpc/]*

**CRL Distribution Points** *http://cr11.uanataca.com/public/pki/crl/arl\_uanataca.crl*  
*http://cr12.uanataca.com/public/pki/crl/arl\_uanataca.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *00:FF:2F:F2:EF:BA:98:C6:B0:23:AD:10:35:55:9A:60:6D:D9:FC:48:A3:9D:34:07:CC:07:A6:78:37:9A:79:09*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *UANATACA CA2 2016*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *UANATACA S.A.*

**Subject L:** *Barcelona (see current address at www.uanataca.com/address)*

**Subject C:** *ES*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2019-12-16T01:00:00Z*

**26.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**26.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**26.2.3 - History instance n.1 - Status: withdrawn**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

Name [ en ] *Qualified Certificates issued by UANATACA CA2 2016*

Name [ es ] *Certificados Reconocidos emitidos por UANATACA CA2 2016*

**Service digital identities****X509SubjectName**

Subject 2.5.4.97: *VATES-A66721499*

Subject CN: *UANATACA CA2 2016*

Subject OU: *TSP-UANATACA*

Subject O: *UANATACA S.A.*

Subject L: *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

Subject C: *ES*

**X509SKI**

X509 SK I *fVfnYHPOB0ap4qNo8OERsnSSc/0=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Status Starting Time *2018-02-15T01:00:00Z*

**26.2.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.2.4 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by UANATACA CA2 2016*

**Name** *[ es ]* *Certificados Reconocidos emitidos por UANATACA CA2 2016*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *UANATACA CA2 2016*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *UANATACA S.A.*

**Subject L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Subject C:** *ES*

**X509SKI**

**X509 SKI** *fVfnYHPOB0ap4qNo8OERsnSSc/0=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2016-06-30T22:00:00Z*

**26.2.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.2.5 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by UANATACA CA2 2016*



**Name** [es] *Certificados Reconocidos emitidos por UANATACA CA2 2016*

### Service digital identities

#### X509SubjectName

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *UANATACA CA2 2016*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *UANATACA S.A.*

**Subject L:** *Barcelona (see current address at www.uanataca.com/address)*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *fVfnYHPOB0ap4qNo8OERsnSSc/0=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision*

**Status Starting Time** *2016-06-14T22:00:00Z*

### 26.3 - Service (granted): Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA – TSU01

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** [en] *A time-stamping generation service creating and signing qualified time-stamps tokens.*  
[es] *Un servicio de generación de sellado de tiempo para crear y firmar tokens tiempo sellos cualificados.*

#### Service Name

**Name** [en] *Qualified timestamps issued by Sello cualificado de tiempo electrónico de UANATACA – TSU01*

**Name** [es] *Sellos de tiempo cualificados emitidos por Sello cualificado de tiempo electrónico de UANATACA – TSU01*

### Service digital identities

#### Certificate fields details

**Version:** *3*

**Serial Number:** *1067299580870664226*



**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*ED:FF:D4:0E:4D:9C:97:96:3E:A1:CB:26:51:0F:3F:28:A0:61:DB:59*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.1.5*  
*CPS pointer: <https://www.uanataca.com/public/cps/>*  
*CPS text: [Certificado de sello cualificado de tiempo electrónico.]*  
*Policy OID: 0.4.0.194112.1.3*

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Subject Alternative Name**  
*info@uanataca.com*

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*F7:E7:B3:C0:34:02:2E:9F:DD:3E:B2:BD:62:6A:B1:9F:E3:BF:56:D8:DB:20:D6:22:B3:13:17:6D:81:D2:9E:B5*

**X509SubjectName**

**Subject 2.5.4.97:**  
*VATES-A66721499*

**Subject CN:**  
*Sello cualificado de tiempo electrónico de UANATACA – TSU01*

**Subject OU:**  
*TSP-UANATACA*

**Subject O:**  
*UANATACA S.A.*

**Subject L:**  
*Barcelona*

**Subject C:**  
*ES*

**X509SKI**

**X509 SK I**  
*7f/UDk2c15Y+ocsmUQ8/KKBh21k=*

**Service Status**

**Service status description** *[en] undefined.*  
<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>



**Issuer C:** ES

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2021

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** Barcelona

**Subject C:** ES

**Valid from:** Thu Jun 03 12:52:31 CEST 2021

**Valid to:** Sat Jun 03 12:52:31 CEST 2034

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100BDE711A297D0BB6D885520E2171E8440BF26CF4D22ED E386547E825BE6D96670C54DA  
7FA3F817D127AADD0F076F3662A31C6E3C4F50B47756A2721A94A2BA1AE5E83C127B836B69C330BA89E7DEA482FC1BD985601DCB158881A857A781A84049D3E55  
54EC3D010264AA8037AFAA276EBC07F364B7C3AD71C4DE7411088FA6D2A1FD056A9373F4CS38CB51BD9E73C442017F0C680F5E94178298B717051CF759F0DC  
5BC6DA352A83519D85B6EE7BF3F6F10F7C2D55087274C42FE0E7B37173EA72DED03E5982E02EF5688B6056F70FC3ADF99A2FEFA7FD7EDBF0E3FB39025085D6  
DBE74E1A7DEEA99EDD2CC6A1483A54E790F684067233C1FA2116818CDE8C12A4B29A541353F9372CD6ACCC54A6BD6CFE1E9325B06E64DE364CB08B4CC08722  
79EA10FD65BA82E6B49CC1D5ACD0173EBA4EB9010BBE16B2D63DCA8F2B2B6555FC4427C87D5D1D5D18329A72A31D3680DF7DA455E4E120A017DE1161E946  
A621062D77C4D912555AD888B979902417AFCAEDAE4930DC22558D22B02AB39F49736E3A72D95D008DBC913FDF496668F031C79CAF310FA10486E2DDC8B46B336  
6B72B799A6549EF0A89D1A783C73A4A9BFB01987D28CA818A80D45176926B6A262310463C50B9C6C1A04F345811A4304E30E0A1CEE32901AFAFBE34DD8FD95D467  
54AC94F69BD883815BD0F1AE0AA9FA95FAF43B7FA99778FCS0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C

**Issuer Alternative Name**  
info@uanataca.com

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Certificado de la Autoridad de Certificación Subordinada de UANATACA. Ver <https://web.uanataca.com/>]

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Subject Alternative Name**  
info@uanataca.com

**Key Usage:**  
keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
9B:08:3D:C4:5B:1B:EC:21:1F:93:09:8F:91:5D:3D:5E:E2:D7:DF:A9:37:20:FE:D4:E2:86:B8:3C:1E  
:F4:46:9A

**X509SubjectName**

**Subject 2.5.4.97:** VATES-A66721499

**Subject CN:** UANATACA CA1 2021

**Subject OU:** TSP-UANATACA

**Subject O:** UANATACA S.A.

**Subject L:** Barcelona

**Subject C:** ES

**X509SKI**

**X509 SK I** gc+QWTS7arctGcUo8otbz8r8FWg=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2021-11-16T02:00:00Z

**26.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**26.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**26.5 - Service (granted): Qualified certificates issued by UANATACA CA2 2021****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified certificates issued by UANATACA CA2 2021

Name [ es ]

Certificados cualificados emitidos por UANATACA CA2 2021

Service digital identities

Certificate fields details

Version: 3
Serial Number: 2247335441897207227

X509 Certificate

-----BEGIN CERTIFICATE-----
MIINCCBB...
-----END CERTIFICATE-----

Signature algorithm: SHA256withRSA
Issuer 2.5.4.97: VATES-A66721499
Issuer CN: UANATACA ROOT 2016
Issuer OU: TSP-UANATACA
Issuer O: UANATACA S.A.
Issuer L: Barcelona (see current address at www.uanataca.com/address)
Issuer C: ES
Subject 2.5.4.97: VATES-A66721499
Subject CN: UANATACA CA2 2021
Subject OU: TSP-UANATACA
Subject O: UANATACA S.A.
Subject L: Barcelona
Subject C: ES
Valid from: Thu Jun 03 12:55:44 CEST 2021

**Valid to:** Sat Jun 03 12:55:44 CEST 2034

**Public Key:**  
3082022230D06092A864886F70D010105000382020F003082020A0282020100B55A0BDC70AA95CD72100726DF68FB95E393C9B042BAA4C29A66C9F9BD77BF78D7B  
51B669E4E378A65AFCE7E5B4050A7E93C8346C87A06D3FC69F3D18236AF9F71A54525D789995FCF9040A822DA27C2BDA93F6AD95ACDD78E3CDDB73C1920FC5  
B1E97C0C094B42933A894B8C09007D83A5F91A6A36C960C9D89C8DF901C7D9A12D05461456F3887B29604C5C8A011775B06F3CFD160332ACAE063C7E4D22CB779FC  
B890C254E886B9669DB353B1DA063C9BE2EC17ED632DB5AA5B368F02CA0C2E446D460EA386AC99D0E2B49F50926B978B7E93D75E900DB13F5656598C879990064  
B23FD98AD065FC40A2752A74F9CC54265A0FB53E92FDA283D9389781EAC809DF3FB6CF37C0471840991411AD904D1674011C21D1E0D388D21652B8BDA0C7CB  
639D7E5837191CDB40339F9C46234033EC4E08B9FA7D063D89C17AD1575762030C0303AA292BF34C5213ED0C7608B4FC7E22F2E7E76AFF89B5F8ED530FAE80EA7B  
86489DDC35420431C8EAE69171871E6CC833D0910553306B723DE3667567EB948310B90DF10B9404E81E2E61F3A679C054963F89937890C2D2B77CB78C1ACB644D423  
C90850DC0E470FBA1F8B7155682AE74B41A810A4689BEA4EA4B840BDD5D93B2F1CD62E64CD559140744238A877603CF0B6922252792E2BA24D616176821E7E68  
89ACADAE1E7D4C4C3D71FC9B54F17B88913C875A7CB0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
C5:E7:33:25:D8:EF:D4:8D:E7:53:87:CA:A2:5B:75:3A:8B:96:DD:4A

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C

**Issuer Alternative Name**  
info@uanataca.com

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Certificado de la Autoridad de Certificación Subordinada de UANATACA. Ver <https://web.uanataca.com/>]

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Subject Alternative Name**  
info@uanataca.com

**Key Usage:**  
keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
15:CE:AB:33:91:44:D4:8D:35:2E:EF:1C:22:7F:4D:2E:F4:FC:17:56:DE:AD:60:2C:22:BE:32:D5:21  
:00:E6:9A

**X509SubjectName**

**Subject 2.5.4.97:**  
VATES-A66721499

**Subject CN:**  
UANATACA CA2 2021

**Subject OU:**  
TSP-UANATACA

**Subject O:**  
UANATACA S.A.

**Subject L:**  
Barcelona

**Subject C:**  
ES

**X509SKI**

**X509 SK I**  
xeczJdvI13nU4fKolt1OouW3Uo=



**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2021-11-16T02:00:00Z

#### 26.5.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 26.5.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 26.6 - Service (granted): Qualified timestamps issued by Sello de tiempo electrónico de UANATACA – TSU02

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

#### **Service Name**

**Name** [en] Qualified timestamps issued by Sello de tiempo electrónico de UANATACA – TSU02

**Name** [es] Sellos de tiempo cualificados emitidos por Sello de tiempo electrónico de UANATACA – TSU02

#### Service digital identities

##### **Certificate fields details**

**Version:** 3

**Serial Number:** 1653782391149433752

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHBDCCBovgAwIBAgIFvNqLpbCEsgwDOYJKoZlhcNAQELBQAwYXZlbnVBAWVTRWwEADYVQ0HDAICyXjZwvxbmEaFAU... (Base64 encoded certificate data)

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer 2.5.4.97:

VATES-A66721499

Issuer CN:

UANATACA CA1 2021

Issuer OU:

TSP-UANATACA

Issuer O:

UANATACA S.A.

Issuer L:

Barcelona

Issuer C:

ES

Subject 2.5.4.97:

VATES-A66721499

Subject CN:

Sello de tiempo electrónico de UANATACA – TSU02

Subject OU:

TSP-UANATACA

Subject O:

Uanataca S.A.

Subject L:

Barcelona

Subject C:

ES

Valid from:

Tue Sep 21 19:48:02 CEST 2021

Valid to:

Fri Sep 21 19:48:02 CEST 2029

Public Key:

3082 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 E7 E7 F6 D5 DB 63 02 58 36 85 5D 91 5B 4C 60 80 19 75 A2 A7 B4 8F A8 01 77 FD 5C 68 52 26 41 ED 2C AA 6 A AF B6 22 01 CA 13 E3 43 DB 29 BF 76 D5 C4 12 5B A7 B1 BC 16 6A D2 91 09 97 9D 6C 62 4B 19 31 18 C9 60 0F 4F 20 5C 3A 09 43 7D 1A 40 BF 53 00 HD E6 FD 30 8D BF 9F 90 BB 7C E4 C2 78 34 A2 4D B9 1 8 7D E3 38 41 BE 30 A7 0D F4 A6 1A 7E 19 09 24 5E A8 63 43 01 E7 76 68 58 34 9E C3 AD 01 42 AB 33 89 75 37 49 5A 81 DF E4 4D A1 9E BA 99 CD 11 F6 BE 28 62 5A EA BC 44 15 74 95 D6 3A DE 21 26 9D 9 7 EF 35 4B DB 84 AC C7 4C D4 01 23 1E C8 55 44 D5 49 A7 76 3F 03 A7 6F 72 A7 C7 C4 91 B1 52 3B FA BA 23 BB 4F C8 91 4E 34 8F DB B3 E5 AD EA 55 20 20 51 C2 94 6D A5 06 5F 16 D5 C3 25 23 5A 82 52 60 78 13 88 00 B0 66 52 29 1F A4 AA CA 72 08 1B 97 44 B2 AB E4 5E 00 C0 44 DD 4D 02 03 01 00 01

Authority Info Access

http://ocsp1.uanataca.com/public/pki/ocsp/
http://ocsp2.uanataca.com/public/pki/ocsp/

Subject Key Identifier

2D:FF:66:C0:73:A2:58:C1:E0:66:7D:B4:2B:F0:79:B5:FD:5D:4B:A3

Basic Constraints

IsCA: false

**Authority Key Identifier** *81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

**Issuer Alternative Name** *info@uanataca.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.2.5*  
*CPS pointer: https://www.uanataca.com/public/cps/*  
*CPS text: [Certificado de sello de tiempo electrónico.]*  
*Policy OID: 0.4.0.2042.1.2*

**CRL Distribution Points**  
*http://cr1.uanataca.com/public/pki/crl/2021CA1sub.crl*  
*http://cr2.uanataca.com/public/pki/crl/2021CA1sub.crl*

**Extended Key Usage** *id\_kp\_timeStamping*

**Subject Alternative Name** *info@uanataca.com*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *AA:59:FB:3B:38:1C:94:7C:BE:22:5B:D8:8A:CE:7E:0C:19:C5:A4:48:E4:3B:BF:7D:30:EA:7D:CD:FB:7E:86:70*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-A66721499*

**Subject CN:** *Sello de tiempo electrónico de UANATACA – TSU02*

**Subject OU:** *TSP-UANATACA*

**Subject O:** *Uanataca S.A.*

**Subject L:** *Barcelona*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Lf9mwHOiWMHgZn20K/B5tf1dS6M=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-11-16T02:00:00Z*

**27 - TSP: VINTEGRIS S.L.U.****TSP Name**

**Name** [ en ] VINTEGRIS S.L.U.

**Name** [ es ] VINTEGRIS S.L.U.

**TSP Trade Name**

**Name** [ en ] vinCAsign

**Name** [ en ] VINTEGRIS SLU

**Name** [ en ] VATES-B62913926

**Name** [ en ] VINTEGRIS SL

**Name** [ en ] Vintegris SL

**Name** [ en ] VINTEGRIS

**PostalAddress**

**Street Address** [ en ] C. Pallars, 99 Planta 3 Oficina 33

**Locality** [ en ] Barcelona

**State Or Province** [ en ] Barcelona

**Postal Code** [ en ] 08018

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] C. Pallars, 99 Planta 3 Oficina 33

**Locality** [ es ] Barcelona

**State Or Province** [ es ] Barcelona

**Postal Code** [ es ] 08018

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ es ] <mailto:info@vintegris.com>



**Issuer SERIAL NUMBER:** B62913926

**Issuer OU:** EC-VINTEGRIS

**Issuer L:** Barcelona (see current address at <https://www.vincasign.net/contact>)

**Issuer O:** VINTEGRIS SL

**Issuer C:** ES

**Subject CN:** vinCAsign Global Authority

**Subject SERIAL NUMBER:** B62913926

**Subject OU:** EC-VINTEGRIS

**Subject L:** Barcelona (see current address at <https://www.vincasign.net/contact>)

**Subject O:** VINTEGRIS SL

**Subject C:** ES

**Valid from:** Thu Jan 28 15:02:06 CET 2016

**Valid to:** Fri Jan 28 15:02:06 CET 2022

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D29AFE3B9EC60A933F875F6D0C3D1A3F4F91EC3C3752F63E3CA18B90019BDBCF5D1C7B8ADA003F19A8283D1C03F1FD9BFDB3E69C9A2481DAB4D2E269D121F8A1160F450049B150F99BBD0E20D0A2D8679C6B27A1CF6ED6D666737AC9268E556FA187B42044547339D8F9785879B8C79AF2AE601B8B8E25448E459C23A0C82BAEB8C1A368AE6A581E3C364A542425A475BAE38B4189C034AE1657E9FF34C9B2A0571E68D380BBE744BD318C12B67A874505DAD212EDEF1137D70673CB080B6570D5C571B33CB916D509DFC647A005C523BED71BCD81A2CF69332AE7163DE3ECA9B62C168AE784CD1F5609CE7B4702E1E145DFA5A1BEAAE071CC62BDC952F0CD4DAAC830A209644A4B38510B80E765996FC19ACBD9A144030F31CD1E160F5C2C620CF4D1B6974B8D0E0CF9DD913C3CA8875225B2C8DC682B3556EB2704414E96C79F2FED9E6BE58DC1BBE55E3EAD062F4EFD3E1F26E630BD90EA03C15ADD6C64E8203AFA8676F6A49CFE31A74FC2B7574D420065B54EC0E2CBCBE8123484652E05C91EAFAD59F389156727055BF264174E9A9BF5B3C8E58D8048BD52CF05393F131E4F18130B9081C3B3C99F2C80E8491B002609AE1A3A52413671407E88E50A54C1751CB4CECA5416CD3CDB1D2D0BC8F203CE7065DC1E150C2E66006587903873E219A90BA220297D5C6E3B9424E9BC64742D38C566B69417022C585AA70830203010001

**Authority Key Identifier** A9:8A:AD:59:FD:ED:E8:E1:80:8B:48:B3:0E:D2:63:E6:44:E0:31:03

**Subject Key Identifier** 07:46:CB:4B:E5:D4:8E:61:73:44:7A:04:20:B2:E1:BA:8C:34:DE:CB

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.vincasign.net>  
 CPS text: [Certificado de la vinCAsign Global Authority de la Entidad de certificacion de Vintegris. Ver <https://policy.vincasign.net>]

**Subject Alternative Name** info@vincasign.net

**CRL Distribution Points**  
<http://crl1.vincasign.net/caroot.crl>  
<http://crl2.vincasign.net/caroot.crl>

**Authority Info Access**  
<http://ocsp1.vincasign.net>  
<http://ocsp2.vincasign.net>

**Basic Constraints** IsCA: true - Path length: 1

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *30:5E:88:A5:EB:B7:DA:E9:E6:6B:F8:A3:D2:1E:64:3C:C2:09:5C:18:FF:7A:F4:7D:FE:1B:AB:2B:88:1D:CB:F8*

**X509SubjectName**

**Subject CN:** *vinCAsign Global Authority*

**Subject SERIAL NUMBER:** *B62913926*

**Subject OU:** *EC-VINTEGRIS*

**Subject L:** *Barcelona (see current address at <https://www.vincasign.net/contact>)*

**Subject O:** *VINTEGRIS SL*

**Subject C:** *ES*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2017-12-20T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**URI** *[es]* *<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>*

**27.1.1 - Extension (critical): Qualifiers [NotQualified]**

**Qualifier type description** *[en]* *undefined.*

*[es]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.5.1*

**Policy Identifier:**

**Identifier** *[OIDAsURN]* *urn:oid:1.3.6.1.4.1.47155.1.5.2*

**27.1.2 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

27.1.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

## Service Name

Name [ en ] *Qualified Certificates issued by vinCAsign Global Authority*

Name [ es ] *Certificados Reconocidos emitidos por vinCAsign Global Authority*

Service digital identities

## X509SubjectName

Subject CN: *vinCAsign Global Authority*

Subject SERIAL NUMBER: *B62913926*

Subject OU: *EC-VINTEGRIS*

Subject L: *Barcelona (see current address at <https://www.vincasign.net/contact>)*

Subject O: *VINTEGRIS SL*

Subject C: *ES*

## X509SKI

X509 SK I *B0bLS+XUjmFzRHoEILLhuow03ss=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2016-06-30T22:00:00Z*

27.1.3.1 - Extension (critical): Qualifiers [NotQualified]

Qualifier type description [ en ] *undefined.*

[ es ] *undefined.*

## Criteria list assert=atLeastOne

## Policy Identifier:

Identifier [ OIDsURN ] *urn:oid:1.3.6.1.4.1.47155.1.5.1*



**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47155.1.5.2

**27.1.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**27.1.4 - History instance n.2 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by vinCAsign Global Authority*

**Name** [ es ] *Certificados Reconocidos emitidos por vinCAsign Global Authority*

**Service digital identities****X509SubjectName**

**Subject CN:** *vinCAsign Global Authority*

**Subject SERIAL NUMBER:** *B62913926*

**Subject OU:** *EC-VINTEGRIS*

**Subject L:** *Barcelona (see current address at <https://www.vincasign.net/contact>)*

**Subject O:** *VINTEGRIS SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *B0bLS+XUjmFzRHoEILLhuow03ss=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** *2016-06-21T22:00:00Z*

**27.1.4.3 - Extension (not critical): Qualifiers [QCForLegalPerson]**

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz / QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

### Criteria list assert=atLeastOne

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

#### Policy Identifier:

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.5.2

## 27.2 - Service (withdrawn): Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
<b>Service type description</b>	[en]	A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.
	[es]	Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

<b>Name</b>	[es]	Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority
<b>Name</b>	[en]	Qualified Certificates issued by vinCAsign nebulaSUITE Authority

### Service digital identities

#### Certificate fields details

<b>Version:</b>	3
<b>Serial Number:</b>	580247578624264002174382824980712041798116291597



**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.vincasign.net>  
 CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

**Subject Alternative Name** [info@vincasign.net](mailto:info@vincasign.net)

**CRL Distribution Points** <http://crl3.vincasign.net/casub.crl>  
<http://crl4.vincasign.net/casub.crl>

**Authority Info Access** <http://ocsp3.vincasign.net>  
<http://ocsp4.vincasign.net>  
<https://www.vincasign.net/publickeys/caqualified.cer>

**Basic Constraints** IsCA: true - Path length: 1

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** D7:CD:55:49:04:DF:D2:2A:22:EB:96:5C:E0:1B:B1:A3:0C:21:51:CA:07:47:3D:4C:BD:45:DF:5D:AF:27:36:A4

**X509SubjectName**

**Subject ST:** Barcelona

**Subject CN:** vinCAsign nebulaSUITE Authority

**Subject 2.5.4.97:** VATES-B62913926

**Subject L:** Hospitalet de Llobregat

**Subject O:** Vintegris SL

**Subject C:** ES

**X509SKI**

**X509 SK I** hGvvoiedpgqtH3qv3xdefBjUpKQ=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2018-10-08T01:00:00Z

**27.2.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.1.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.6.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.11
-------------------	------------	----------------------------------

**Description****27.2.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
------------	------	---

**27.2.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals
------------	------	--

**27.2.4 - History instance n.1 - Status: granted**

<b>Service Type Identifier</b>	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
--------------------------------	---

**Service Name**

<b>Name</b>	[es]	Certificados cualificados emitidos por vinCAsign nebulaSUITE Authority
-------------	------	--

<b>Name</b>	[en]	Qualified Certificates issued by vinCAsign nebulaSUITE Authority
-------------	------	--

**Service digital identities****X509SubjectName**

Subject ST: *Barcelona*

Subject CN: *vinCAsign nebulaSUITE Authority*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *Hospitalet de Llobregat*

Subject O: *Víntegris SL*

Subject C: *ES*

**X509SKI**

X509 SK I *hGvvoiedpgqtH3qv3xdefBjUpKQ=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2017-12-20T01:00:00Z*

**27.2.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.1.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.2.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.6.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.2.11
------------	-------------	----------------------------------

**Description****27.2.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI

[ en ]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

27.2.4.3 - Extension (critical): additionalServiceInformation

AdditionalServiceInformation

URI

[ en ]

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals

27.3 - Service (granted): Certificados Cualificados emitidos por vinCASign nebulaSUITE2 Authority

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

Service type description

[ en ]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[ es ]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[ es ]

Certificados Cualificados emitidos por vinCASign nebulaSUITE2 Authority

Name

[ en ]

Qualified Certificates issued by vinCASign nebulaSUITE2 Authority

Service digital identities

Certificate fields details

Version:

3

Serial Number:

637401987826912361881659849906312446373074387053

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIHjCCBeagAwIBAgIUb6YX+... [Certificate content truncated for brevity]

-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer ST:

Barcelona

Issuer CN:

vinCASign Qualified Authority

**Issuer 2.5.4.97:** VATES-B62913926

**Issuer L:** Hospitalet de Llobregat

**Issuer O:** Vintegris SL

**Issuer C:** ES

**Subject CN:** vinCASign nebulaSUITE2 Authority

**Subject O:** VINTEGRIS SL

**Subject OU:** vinCASign

**Subject 2.5.4.97:** VATES-B62913926

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject ST:** BARCELONA

**Subject C:** ES

**Valid from:** Wed Sep 27 16:20:46 CEST 2017

**Valid to:** Fri Sep 27 16:20:46 CEST 2030

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CF:CE:75:30:A8:77:4F:A3:AF:61:07:19:6B:91:D7:8F:34:57:1D:06:1E:84:74:3D:4A:0E:46:BC:EA:9:11:E9:E7:5A:F  
4:D2:BB:53:3B:4F:78:E7:0F:29:1E:5C:FE:C9:04:BB:5A:16:67:A5:6C:0B:95:8D:82:70:91:92:3B:A8:48:67:9E:D9:68:68:37:C8:71:0A:44:F9:D4:55:66:4B:E6:FE:90:36:A1:DF:80:3E:F7:56:5E:CB:76:8F:7F:69:8E:4B:83:BD:5  
6:A7:1F:06:F8:D9:81:B1:81:F0:CF:C6:B6:C8:0B:45:D1:10:D5:87:16:6B:99:90:F9:A5:FB:CF:B1:3A:B7:B6:1D:B3:06:AD:54:9D:89:AE:69:8C:8D:93:0F:2B:2E:CD:CD:A7:21:CD:F5:20:57:09:06:13:B0:B6:D7:3F:BE:60:68:  
B0:17:DA:51:ED:8C:B7:9A:16:7C:B4:28:F9:F4:3C:F8:E9:5E:FA:0E:D3:0E:CE:F8:96:31:74:C5:05:9A:ED:37:A8:87:90:87:6D:ED:7F:F7:7F:40:1E:1B:4D:B6:B6:B1:78:B1:19:E5:60:73:BF:11:58:57:63:B0:72:58:16:B2:EF:A  
F:0D:C8:4A:38:9C:A9:BA:28:24:33:8F:47:21:BB:2D:34:8B:93:99:AF:EA:D6:62:39:36:19:4E:5E:79:59:80:D4:57:45:9B:24:0A:7E:E4:66:66:3A:CC:CA:59:6D:5B:99:C4:8B:BF:8E:11:DD:31:4F:58:B4:08:F0:7D:9B:3C:A  
B:E0:47:EF:A4:F0:53:83:6C:9A:8A:BS:06:37:68:90:F9:AC:D2:29:8C:9B:52:3E:C1:FD:2E:AA:00:30:7E:CA:90:E2:E5:B4:FF:34:6D:7A:4B:94:70:B9:67:75:A3:13:6C:9E:89:F6:82:AD:DC:3C:82:03:4C:8D:53:27:18:1A:A0:84  
46:27:25:38:72:03:57:51:B5:7F:0D:31:AC:9B:8D:C5:5D:8E:BB:8D:8B:AE:3A:F0:A0:3E:52:A6:C8:67:EC:D5:1A:EA:E3:E2:A6:EB:57:2D:09:C9:A5:54:02:97:B2:BE:83:A7:D7:DB:34:B0:25:8A:95:61:6E:42:15:B0:A8:7B:8  
D:88:6B:30:4D:56:9B:2B:28:AF:D7:85:BB:AE:AD:81:E5:8A:79:73:80:D8:5C:E3:E1:5A:AC:12:04:4B:04:77:61:6B:5C:34:6A:01:77:DE:14:C6:CB:EC:3D:16:E6:4B:F9:05:46:4F:99:EC:0E:5B:79:7B:12:6F:CD:AA:51:7C:07:  
C:37:E2:EA:BF:9F:5A:3E:27:78:DC:9D:B0:07:C9:82:98:0D:F4:D7:C1:02:03:01:00:01

**Authority Key Identifier** D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0

**Subject Key Identifier** 4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.vincasign.net>  
CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

**Subject Alternative Name** info@vincasign.net

**CRL Distribution Points**  
<http://crl3.vincasign.net/casub.crl>  
<http://crl4.vincasign.net/casub.crl>

**Authority Info Access**  
<http://ocsp3.vincasign.net>  
<http://ocsp4.vincasign.net>  
<https://www.vincasign.net/publickeys/caqualified.cer>

**Basic Constraints** IsCA: true - Path length: 1



**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *DA:13:26:D2:2E:64:F7:C2:1F:38:81:21:F6:8C:8F:70:0D:30:5C:69:FB:0B:5E:8B:9F:C2:84:6F:7A:E7:CB:70*

**X509SubjectName**

**Subject CN:** *vinCAsign nebulaSUITE2 Authority*

**Subject O:** *VINTEGRIS SL*

**Subject OU:** *vinCAsign*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject ST:** *BARCELONA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *TdZ6hiuc9kt699v96VFML3fcFn4=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2019-11-06T01:00:00Z*

**27.3.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.47155.1.1.1*

**Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.47155.1.2.1*

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.6.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.4.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.5.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.2.11
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.1.51
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.2.51
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.2.151
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.4.11
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.6.51
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.10.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.10.51
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.1.11.1
<b>Description</b>		

**27.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**27.3.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**27.3.4 - History instance n.1 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ es ]	<i>Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority</i>
-------------	--------	--

<b>Name</b>	[ en ]	<i>Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority</i>
-------------	--------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>vinCAsign nebulaSUITE2 Authority</i>
--------------------	---

<b>Subject O:</b>	<i>VINTEGRIS SL</i>
-------------------	---------------------

<b>Subject OU:</b>	<i>vinCAsign</i>
--------------------	------------------

<b>Subject 2.5.4.97:</b>	<i>VATES-B62913926</i>
--------------------------	------------------------

<b>Subject L:</b>	<i>HOSPITALET DE LLOBREGAT</i>
-------------------	--------------------------------

<b>Subject ST:</b>	<i>BARCELONA</i>
--------------------	------------------

<b>Subject C:</b>	<i>ES</i>
-------------------	-----------

**X509SKI**

<b>X509 SK I</b>	<i>TdZ6hiuc9kt699v96VFML3fcFn4=</i>
------------------	-------------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---

<b>Status Starting Time</b>	<i>2019-10-28T01:00:00Z</i>
-----------------------------	-----------------------------

**27.3.4.1 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.1.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.6.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.4.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.5.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.11

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.1.51

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.51

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.2.151

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.4.11

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47155.1.6.51

**Description****27.3.4.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	--------	---

**27.3.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
------------	--------	---

**27.3.5 - History instance n.2 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ es ]	<i>Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority</i>
-------------	--------	--

<b>Name</b>	[ en ]	<i>Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority</i>
-------------	--------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	<i>vinCAsign nebulaSUITE2 Authority</i>
--------------------	---

<b>Subject O:</b>	<i>VINTEGRIS SL</i>
-------------------	---------------------

<b>Subject OU:</b>	<i>vinCAsign</i>
--------------------	------------------

<b>Subject 2.5.4.97:</b>	<i>VATES-B62913926</i>
--------------------------	------------------------

<b>Subject L:</b>	<i>HOSPITALET DE LLOBREGAT</i>
-------------------	--------------------------------

<b>Subject ST:</b>	<i>BARCELONA</i>
--------------------	------------------

<b>Subject C:</b>	<i>ES</i>
-------------------	-----------

**X509SKI**

<b>X509 SK I</b>	<i>TdZ6hiuc9kt699v96VFML3fcFn4=</i>
------------------	-------------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---

Status Starting Time

2019-08-02T00:00:00Z

**27.3.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.1.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.6.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.4.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.5.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.11
-------------------	------------	----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.1.51
-------------------	------------	----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.51
-------------------	------------	----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.2.151
-------------------	------------	-----------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47155.1.4.11
-------------------	------------	----------------------------------

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47155.1.6.51

**Description****27.3.5.5 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**27.3.5.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**27.3.6 - History instance n.3 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Cualificados emitidos por vinCAsign nebulaSUITE2 Authority*

**Name** [ en ] *Qualified Certificates issued by vinCAsign nebulaSUITE2 Authority*

**Service digital identities****X509SubjectName**

**Subject CN:** *vinCAsign nebulaSUITE2 Authority*

**Subject O:** *VINTEGRIS SL*

**Subject OU:** *vinCAsign*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject ST:** *BARCELONA*

**Subject C:** *ES*

**X509SKI****X509 SK I***TdZ6hiuc9kt699v96VFML3fcFn4=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2018-04-09T00:00:00Z***27.3.6.7 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	<i>[en]</i>	<i>undefined.</i>
	<i>[es]</i>	<i>undefined.</i>

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.1.1</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.2.1</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.6.1</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.4.1</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.5.1</i>
-------------------	--------------------	--

**Policy Identifier:**

<b>Identifier</b>	<i>[ OIDsURN ]</i>	<i>urn:oid:1.3.6.1.4.1.47155.1.2.11</i>
-------------------	--------------------	---

**Description****27.3.6.8 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	<i>[ en ]</i>	<i>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</i>
------------	---------------	--





**Issuer 2.5.4.97:** VATES-B62913926

**Issuer L:** HOSPITALET DE LLOBREGAT

**Issuer ST:** BARCELONA

**Issuer C:** ES

**Subject C:** ES

**Subject ST:** BARCELONA

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject O:** VINTEGRIS SL

**Subject 2.5.4.97:** VATES-B62913926

**Subject OU:** vinCAsign

**Subject CN:** vinTSAsign nebulaSUITE1 Authority

**Valid from:** Thu Jul 11 15:58:42 CEST 2019

**Valid to:** Tue Jul 09 15:58:42 CEST 2024

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:82:3A:E4:0F:4C:2B:91:03:4B:0F:50:80:78:0E:42:18:01:EA:1F:B8:66:41:34:25:59:C7:67:2A:D5:7F:9D:1C:6D:49:D6:2C:D3:52:CC:2E:11:5B:8A:51:48:39:22:3E:D9:16:22:BF:36:0C:30:E4:48:A4:DD:9D:8C:4E:2E:00:A3:01:32:13:87:29:A6:E0:58:12:03:P6:62:33:FD:64:E0:84:98:3F:FD:12:01:C9:CF:D5:AE:91:4D:2:19:07:EA:B7:57:58:D7:9C:DE:18:EA:72:AA:0A:DD:89:80:91:83:89:2B:22:26:39:7D:86:4B:BD:74:EE:47:92:04:DE:CD:F4:07:98:EB:CS:B3:E1:5D:0B:BD:1F:DC:4C:92:C4:2F:2B:AB:26:35:FE:DC:8C:43:0F:B0:86:F1:7A:26:A1:D8:ED:CB:E4:D4:0A:C8:EA:56:73:EB:94:24:9C:15:6A:ES:1C:CE:6A:64:C7:7D:0D:D7:0D:3D:37:FA:3A:8A:48:CC:14:2A:ES:CE:8E:F2:0C:DB:66:68:4F:8A:87:C8:A4:D5:C9:36:DB:AD:CC:EA:39:27:B7:10:8B:C9:30:AB:9A:ED:B6:C8:D A:8F:FD:C8:9D:D9:C0:E6:AC:96:56:9D:85:22:16:C5:62:55:BD:28:38:46:EC:5D:96:D0:34:99:1B:F6:57:CD:C1:10:BC:14:56:69:36:DE:34:62:BE:50:5C:3B:07:B1:87:66:37:44:AF:DA:16:07:F6:AD:CE:6E:59:6B:71:D3:59:8 6:23:1E:A1:C4:79:8E:4C:10:F8:2A:FE:0C:2D:41:0C:6F:91:AF:FA:67:46:43:A0:69:46:70:1B:0B:CF:BS:B6:1A:CA:04:4F:5D:E6:E6:6A:7F:29:C1:EC:FA:73:03:CB:8C:F4:DA:0B:78:FD:8C:8F:76:18:C8:03:C1:98:ES:BS:00:B 2:1C:62:F1:5F:7F:D2:DC:EA:DF:99:19:49:8A:72:67:A4:2D:35:9D:FC:DB:CD:00:E9:08:A1:10:ES:AF:ES:1D:8E:64:B8:38:D6:17:7C:92:1A:6F:87:67:DE:9A:88:59:A7:45:D5:B0:A3:B6:C4:1C:6F:67:5B:67:52:36:71:BE:AD: 26:EB:12:1E:D9:C5:30:19:A3:02:24:F6:46:9D:96:66:03:52:B7:57:35:C2:39:CA:1B:86:75:4B:63:1A:35:76:37:A4:3D:FF:0F:A7:04:EB:A0:09:A9:0B:D9:2F:34:9B:93:79:B9:40:AB:B7:E6:07:00:D5:B3:FC:03:2C:F3:49:E1:01: 21:DB:FB:CB:23:05:E1:0F:6A:69:F4:30:24:04:7A:FE:53:34:68:8B:D4:D0:8E:CB:02:03:01:00:01

**Authority Info Access**  
<http://www.vincasign.net/publickeys/canebula2.crt>  
<http://ocsp.vincasign.net>

**Subject Key Identifier**  
93:73:A4:CE:A0:BE:79:96:07:2E:73:1A:40:F9:E2:F6:42:B0:22:EB

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47155.1.9.1  
CPS pointer: <https://policy.vincasign.net>  
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]  
Policy OID: 0.4.0.194112.1.1

**CRL Distribution Points** *http://cr1.vincasign.net/canebula2.crl*  
*http://cr2.vincasign.net/canebula2.crl*

**Extended Key Usage** *id\_kp\_timeStamping*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *17:57:14:7A:3A:13:1C:C4:9C:FA:DE:37:4B:00:65:59:FB:A3:F0:EB:2D:9F:6A:4A:FF:41:DE:7B:2F:11:96:9D*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *BARCELONA*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject O:** *VINTEGRIS SL*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject OU:** *vinCAsign*

**Subject CN:** *vinTSAsign nebulaSUITE1 Authority*

**X509SKI**

**X509 SK I** *k3OkzqC+eZYHLnMaQPni9kKwIus=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2019-08-02T00:00:00Z*

**27.5 - Service (granted): Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*  
*[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.*

**Service Name**

**Name** *[es] Sellos de tiempo cualificados emitidos por vinTSAsign nebulaSUITE2 Authority*



**Subject OU:** *vinCAsign*

**Subject CN:** *vinTSAsign nebulaSUITE2 Authority*

**Valid from:** *Thu Jul 11 16:44:51 CEST 2019*

**Valid to:** *Tue Jul 09 16:44:51 CEST 2024*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100CEAB05CB379E8892C03489855211187031A37491C8DC10F160467232CDF62A5666FE598FB8298DC2935992A0E824061D4BF59448C198563A2E2B8C89FBEA07A777867189CCBA09B8457FB1ED8B6C8A6E8C73EA1D2985101657A7B315F1B39F36159A06400A2CF8814B48C170A2CD7FB7A480818D419EE2091A017F2F2892EE21C63609BAD205954C0DE0ADA9940B0D725192260420AD53D82EA1F0C2073FC10FC90CCB883FF0EEF2EA0D0F9A7DE8AD170E5B552F66450DC9BA8065C77257321737CEAD59E9D60ADC42CBE6BDBA122A5EBE1716F997EFB3368F8E2FB80483D2613D08B2562C30A5BE44DD7D15AF096945BA91BE10611CF90F5A49147A0E391A014E5EA62FA9106FE05051492ED2CFB41B99244892FD1FA8BE2DS2DF0E537B40D2543CEA8684E76B6C4F148F53C3E7E7CB1351B448F3EA67E3DA5EB7BA33315913136F85F73FA11C24BA1A4CC4DBS27CD7E447BC40E606E3165BF7BF3C078CA1C1C44E8BD6A57B61BDB35C858E8011D4D84E831C606CE4A8FD918A23CEF2D51E6149239DD233A121A8EC1DFB05EA94556DA59A8681AC90BE22AB1F61370A2D2825F75C3541E043E3E43548B10793D2B8641713B123B8F11574E2FC352E90954C34943A5ACE07C71059EB5F4E417F691F667398B17CC49F4DB3B26F637ACFD269226629DDFB C483C8BA3FA8132D0AE8DF2ABF94E06EB4EC4ACB670203010001

**Authority Info Access**  
<http://www.vincasign.net/publickeys/canebula2.crt>  
<http://ocsp.vincasign.net>

**Subject Key Identifier** *F0:1D:A5:5B:67:05:9E:EC:C1:20:F6:2E:F4:38:8C:3B:0F:BB:81:32*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier** *4D:D6:7A:86:2B:9C:F6:4B:7A:F7:DB:FD:E9:51:4C:2F:77:DC:16:7E*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47155.1.9.1*  
*CPS pointer: https://policy.vincasign.net*  
*CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
*Policy OID: 0.4.0.194112.1.1*

**CRL Distribution Points**  
<http://cr1.vincasign.net/canebula2.crl>  
<http://cr2.vincasign.net/canebula2.crl>

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Key Usage:**  
*digitalSignature - nonRepudiation*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*FB:75:52:A8:36:0A:2D:4D:89:4B:F3:8C:4E:B4:A6:A0:9C:8E:CF:1E:25:C5:4F:B1:E2:02:D1:85:76:61:3A:51*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *BARCELONA*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject O:** VINTEGRIS SL

**Subject 2.5.4.97:** VATES-B62913926

**Subject OU:** vinCAsign

**Subject CN:** vinTSAsign nebulaSUITE2 Authority

**X509SKI**

**X509 SK I** 8B2IW2cFnuzBIPYu9DiMOw+7gTI=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time**

2019-08-02T00:00:00Z

**27.6 - Service (withdrawn): Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority

**Name** [es] Certificados Cualificados emitidos por vinCAsign nebulaSUITE4 Authority

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 592846264893196737726411358607176543381952486368



**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.vincasign.net>  
 CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

**Subject Alternative Name**  
 info@vincasign.net

**CRL Distribution Points**  
<http://crl3.vincasign.net/casub.crl>  
<http://crl4.vincasign.net/casub.crl>

**Authority Info Access**  
<http://www.vincasign.net/publickeys/caqualified.cer>

**Basic Constraints**  
 IsCA: true - Path length: 1

**Key Usage:**  
 keyCertSign - cRLSign

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 1C:A3:C0:A2:84:F8:94:DB:A0:A9:7C:83:53:1E:8C:06:2D:1D:54:F6:E7:F9:66:FA:32:3E:52:8E:F7:  
 B9:B8:47

**X509SubjectName**

**Subject CN:**  
 vinCAsign nebulaSUITE4 Authority

**Subject O:**  
 VINTEGRIS SL

**Subject OU:**  
 vinCAsign

**Subject 2.5.4.97:**  
 VATES-B62913926

**Subject L:**  
 HOSPITALET DE LLOBREGAT

**Subject ST:**  
 BARCELONA

**Subject C:**  
 ES

**X509SKI**

**X509 SK I**  
 o+e+fRSSSt3Ur8GiWzHhEgJfuLgM=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2023-09-14T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>



URI [ es ]  
<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 27.6.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ]  
<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

### 27.6.2 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name [ en ]  
 Qualified Certificates issued by vinCAsign nebulaSUITE4 Authority

Name [ es ]  
 Certificados Cualificados emitidos por vinCAsign nebulaSUITE4 Authority

#### Service digital identities

##### X509SubjectName

Subject CN: *vinCAsign nebulaSUITE4 Authority*

Subject O: *VINTEGRIS SL*

Subject OU: *vinCAsign*

Subject 2.5.4.97: *VATES-B62913926*

Subject L: *HOSPITALET DE LLOBREGAT*

Subject ST: *BARCELONA*

Subject C: *ES*

##### X509SKI

X509 SK I *o+e+fRSSSt3Ur8GiWzHhEgJfuLgM=*

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time *2020-11-18T22:00:00Z*

### 27.6.2.1 - Extension (critical): additionalServiceInformation



**Issuer C:** ES

**Subject CN:** vinCASign nebulaSUITE5 Authority

**Subject O:** VINTEGRIS SL

**Subject OU:** vinCASign

**Subject 2.5.4.97:** VATES-B62913926

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject ST:** BARCELONA

**Subject C:** ES

**Valid from:** Wed Nov 11 16:46:15 CET 2020

**Valid to:** Fri Nov 11 16:46:15 CET 2033

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A166FD918C8441266BC1D52B5ED8BF79416A03644CB36614F197CC5F0D99793481F9685B2D4A6DEB43786701337DAA01C38013EACAEFE66C876358013EACA3BAD0859776F1B30B78A6A509C1658A377ABA8B6C4F361053C97DBD8C0B18A26C318051457CEBF9903D5B7DECD099CEB547FBDDAC789838E93E4B3B1929919E29A8C72E338DC6A6FE1C979ECAA753FD814114F40B725F5A62BE1988754E134DCAB50026B6D1D2CDD54F7BB2866A631D3390EDBA8ECC788C92B45A7D9E09BEF0AF6B54F736742BC2C4CAAFCA2A1D5029C750794A8265DA9750DS57981B1654E6D0209D1F324F7961C763610987DCDDE712E812486835E2168583CA117BEDBE21AC9CFEESB4CE5D7277383B6B560A890981D1B476EC24B3DD099406DEC1A1E7FE21DA992E26BE3E1D75522D831613018D8F91868460C8E411504D2DB96E8B62FAFF90CCBE9E84F9FC6C7CEAB29E23B35F91718A786A9D4F0F243532349E2402876EBF083A70A0EC11DB3177082E3D1C0B051C2DF0C9F80AF6C1762DB4788AAFD8D7D93C02C646C7B44E3B1F66B3C063327E7EADE972E6692EF8D405CDECF497E6D1720D690AA7D03B861699EC84EC88D89C15C89E62D792BF623A930669A9607B5E19C9F4FD8FC502912BF4F6E5D0FFD117FE15323D7D11F9707DA31D0D343C0131F974E17DE12CFASDA85B81D552F69DABC465231D141A0649E8E6330203010001

**Authority Key Identifier** D0:3E:4A:6A:92:6F:4D:B3:86:47:5C:74:E4:56:A3:02:F4:16:C8:D0

**Subject Key Identifier** 29:B0:A3:C6:79:6B:2A:8D:9F:58:35:AC:B1:FC:24:DA:7E:92:7C:11

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 CPS pointer: <https://policy.vincasign.net>  
 CPS text: [Certificado CA Subordinada. Ver <https://policy.vincasign.net>]

**Subject Alternative Name** info@vincasign.net

**CRL Distribution Points**  
<http://crl3.vincasign.net/casub.crl>  
<http://crl4.vincasign.net/casub.crl>

**Authority Info Access** <http://www.vincasign.net/publickeys/caqualified.cer>

**Basic Constraints** IsCA: true - Path length: 1

**Extended Key Usage** id\_kp\_serverAuth

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** AA:AF:2F:29:EF:52:44:71:CB:4F:15:B7:2D:E6:A5:54:26:29:97:8F:B5:A9:14:A6:11:95:5C:75:AE:5E:F3:C3

**X509SubjectName**

**Subject CN:** *vinCAsign nebulaSUITE5 Authority*

**Subject O:** *VINTEGRIS SL*

**Subject OU:** *vinCAsign*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject ST:** *BARCELONA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *KbCjxnIrkO2fWDWssfwk2n6SfBE=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-09-14T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**27.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**27.7.2 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[en] Qualified Certificates issued by vinCAsign nebulaSUITE5 Authority*

**Name** [ es ] *Certificados cualificados emitidos por vinCAsign nebulaSUITE5 Authority*

### Service digital identities

#### X509SubjectName

**Subject CN:** *vinCAsign nebulaSUITE5 Authority*

**Subject O:** *VINTEGRIS SL*

**Subject OU:** *vinCAsign*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject ST:** *BARCELONA*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *KbCjxnlrKo2fWDWssfwk2n6SfBE=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2021-01-26T01:00:00Z*

#### 27.7.2.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

#### 27.8 - Service (granted): Certificados Cualificados emitidos por «CA Vintegris TrustServices»

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

#### Service Name

**Name** [ es ] *Certificados Cualificados emitidos por «CA Vintegris TrustServices»*

**Name** [ en ] *Qualified Certificates issued by «CA Vintegris TrustServices»*



**Public Key:**

```

30820222300D06092A864886F70D01010105000382020F003082020A0282020100DA4A7315A4811096733B3D5860471524739885E
FB223AA95A266E799FCB1CAB2AEF821F5E3D005599FC2FA1514732ECFB299EC1017D8033ED689A7DB7CD57DA607E133E2D5A955F6A73D001D2E5F2862DD1664929220AB84C
BC77F94F627EDE05CF8D4E23DB557F00D9F1780F2A1E74E09D47263C03B77DE88DD2B1011C534D50CE18269259C8204719115895F9D103E44C6A874F817BB6A47F46477BE46903C1E
DB843E6E0564BC1F8874538544617B3599FF547128BFAC75DD34069B7C887D3FC1B0A0D70BFB71B4B3953D90DE11A3DFE7SCA2E0E793E40DB1F24EB8634F8C
BD413193768C3879A4F1F120DC465679351C7E39973F96AC5870FF57A7A858048521B2CDAF36CA02D2019F9380138E554B1B75C14A1A9567F87E0805D54E77DE598A2096175D
EE9FC52A9DFF80E8984C3E24C76D5A3D509CFE1D1045C77E3E36D8DC5DB4627393E26A4DE5AAE76E2044B9FB29CA3525E5F8AD514DBBF6DFD59C5216B3A01560E
AA93106839653DA896EB1C23A91EE896B6CE54130CECCD1AEDD9E260FE7CFD8B5D75AFDB717376CC8A403E1D11877D1E403DA26AA815077878F81D83F8674C
7C5798B6E3B2D381D5AAD97409F8E995B64997E459E789045D92FCA6F6B801B603A735707F5E9E29B003477CF80A915FC7E7451CCED6B8CA2886E5FE0F62B06F61
344285D3B7684AD68AC5339FE32BE656A848B19A30203010001

```

**Basic Constraints**

IsCA: true - Path length: 1

**Authority Key Identifier**

FB:70:16:61:37:9E:DB:E7:32:97:40:3B:44:76:A2:7C:14:E3:B1:24

**Authority Info Access**<http://www.vincasign.net/publickeys/cavintegris.cer>**Certificate Policies**

Policy OID: 2.5.29.32.0

CPS pointer: <https://policy.vincasign.net>**CRL Distribution Points**<http://crl1.vincasign.net/cavintegris.crl><http://crl2.vincasign.net/cavintegris.crl>**Subject Key Identifier**

99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42

**Key Usage:**

keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

75:A6:33:0E:D1:67:B2:87:7A:43:87:93:13:03:BA:93:D7:8F:72:F5:5A:13:7A:A5:50:6F:D3:29:30:B7:E2:97

**X509SubjectName****Subject C:**

ES

**Subject ST:**

BARCELONA

**Subject L:**

HOSPITALET DE LLOBREGAT

**Subject O:**

VINTEGRIS SLU

**Subject 2.5.4.97:**

VATES-B62913926

**Subject CN:**

CA Vintegris TrustServices

**X509SKI****X509 SK I**

mSDQwgt dwJ0jXtjbTiE29P0sKkl=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2022-10-10T00:00:00Z

**27.8.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

**27.8.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**27.8.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.1.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.1.51
------------	-------------	----------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.2.1
------------	-------------	---------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.2.51
------------	-------------	----------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.2.11
------------	-------------	----------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.2.151
------------	-------------	-----------------------------------

**Policy Identifier:**

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.4.1
------------	-------------	---------------------------------

**Policy Identifier:**



<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.4.11
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.10.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.10.51
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.11.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.5.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.6.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47155.2.6.51
<b>Description</b>		

## 27.9 - Service (granted): Sellos de tiempo cualificados emitidos por «CA Vintegris TSA1 TrustServices»

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST">http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</a>
<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.
<b>Service Name</b>		
<b>Name</b>	[es]	Sellos de tiempo cualificados emitidos por «CA Vintegris TSA1 TrustServices»
<b>Name</b>	[en]	Qualified time stamps issued by «CA Vintegris TSA1 TrustServices»

### Service digital identities

#### **Certificate fields details**

<b>Version:</b>	3
<b>Serial Number:</b>	76172955933336056506690947715413989888149560314



**Authority Key Identifier** *99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42*

**Authority Info Access** *http://www.vincasign.net/publickeys/catrusterservices.crt*  
*http://ocsp.vincasign.net*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.47155.2.9.1*  
*CPS pointer: https://policy.vincasign.net*  
*CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
*Policy OID: 0.4.0.194112.1.1*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://crl1.vincasign.net/catrusterservices.crl*  
*http://crl2.vincasign.net/catrusterservices.crl*

**Subject Key Identifier** *9E:14:7B:B5:C9:00:95:3E:F1:0B:A5:4F:D7:9D:4D:AE:C5:F4:50:33*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A5:0B:0A:34:BE:70:FD:13:4F:F2:F4:8E:3D:7F:65:51:7D:46:BE:20:04:CB:7A:F0:17:8E:C2:04:38:3E:B5:24*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *BARCELONA*

**Subject L:** *HOSPITALET DE LLOBREGAT*

**Subject O:** *VINTEGRIS SLU*

**Subject 2.5.4.97:** *VATES-B62913926*

**Subject CN:** *CA Vintegris TSAI TrustServices*

**X509SKI**

**X509 SK I** *nhR7tckAIT7xC6VP151NrsX0UDM=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*



**Issuer CN:** CA Vintegris TrustServices

**Subject C:** ES

**Subject ST:** BARCELONA

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject O:** VINTEGRIS SLU

**Subject 2.5.4.97:** VATES-B62913926

**Subject CN:** CA Vintegris TSA2 TrustServices

**Valid from:** Thu Mar 03 16:12:33 CET 2022

**Valid to:** Tue Mar 02 16:12:33 CET 2027

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A028202010085B53694B980AF1AE8310F4694F5A60B3BF82DA0DD6690C60C65BFDABA0A59075F7  
9895FA7BDA0BDA3CB159E20A158B01208613C856A970D0F51733B4ED712420BC9C16B566D9E9F38A80A6118531A98B74FD040B6EA2864EE8E5A0CF8971F58F9CF  
06F8ADAD9AAFE2D2A6BAA01C8CC697C6020F66400B0E4BC0C7A9BC625143007C4CD44851B143ABB00208E76FB62A2EFC882BFDE195CBF85F1B0FE5C8896A61A65  
D14E4C2208E6ECDE2EA037F06D662410C103582E3F8A79D261076182FCE0A3C7E859C1CB039624CF5899CEFF15A815194F78180829DEB846C5028EA9067311A88C  
C2341588257E6C2BC707468ED50BC556FD1AA3D9A6608A0CBE5206C8BD99882EFA456E4C53DFE8D3464C580C59BA5623C9401CC9C83EEAE59A7AC5B47201A  
37C409F3F9A35D6AE49C8B131357BB1E962E4D083482B817B31FE5D94AF37CAFC6562DFDA15E71373F9C46CD42ABC669643141856B51A6EDEE87000SD198E04E3  
5CB9E46B64AA22AC15D81E3D3B65C413DD449B136651B40E92ECDE2E8A8020844A9775F2C39B95DB13AEFEAB46D7B9D83972D1CEB28C8346E5BD54AC1719E31AA  
192627B865E0E94C47811E7F0CE6D71B1BE45196C77E91DEF9BC41A4B4176D74675A144F4B5523FFD4E401A689ED13FF4ED3F5E6D625AD1C75AC0FA4BC73A7D520  
A6D3E9A6CA7AD325C10BC58EB296E2BF395FCB1DC1A310D0203010001

**Basic Constraints** IsCA: false

**Authority Key Identifier** 99:20:D0:C2:0B:5D:C0:9D:23:5E:D8:DB:4E:21:36:F4:FD:2C:2A:42

**Authority Info Access**  
<http://www.vincasign.net/publickeys/catrustservices.crt>  
<http://ocsp.vincasign.net>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47155.2.9.1  
CPS pointer: <https://policy.vincasign.net>  
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]  
Policy OID: 0.4.0.194112.1.1

**Extended Key Usage** id\_kp\_timeStamping

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15

**CRL Distribution Points**  
<http://cr1.vincasign.net/catrustservices.crl>  
<http://cr2.vincasign.net/catrustservices.crl>

**Subject Key Identifier** EE:FE:81:F8:13:67:83:85:AA:7F:29:F6:4B:49:A0:A5:5A:97:F9:C4

**Key Usage:** digitalSignature - nonRepudiation

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 7F:05:13:8F:19:91:8E:6F:38:D2:86:75:A1:E9:C1:D5:A2:A5:E9:5D:13:1B:47:32:D2:31:21:CA:B6:25:05:5D

## X509SubjectName

**Subject C:** ES

**Subject ST:** BARCELONA

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject O:** VINTEGRIS SLU

**Subject 2.5.4.97:** VATES-B62913926

**Subject CN:** CA Vintegris TSA2 TrustServices

## X509SKI

**X509 SK I** 7v6B+BNng4Wqfyn2S0mgpVqX+cQ=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

## Status Starting Time

2022-10-10T00:00:00Z

## 27.11 - Service (granted): Certificados Cualificados emitidos por «CA Vintegris SSL TrustServices»

### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

### Service Name

**Name** [es] Certificados Cualificados emitidos por «CA Vintegris SSL TrustServices»

**Name** [en] Qualified Certificates issued by «CA Vintegris SSL TrustServices»

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 469253651109736763393634430385287111766620827742



**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.vincasign.net>

**Extended Key Usage** id\_kp\_serverAuth

**CRL Distribution Points** <http://crl1.vincasign.net/cavintegris.crl>  
<http://crl2.vincasign.net/cavintegris.crl>

**Subject Key Identifier** 11:26:8E:9A:93:EF:0D:83:3A:54:1C:D8:70:17:29:CE:FD:D0:49:1B

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** ED:3F:7F:E9:38:D9:53:AF:0B:E0:99:18:D7:E5:9E:A2:0B:66:2A:FC:46:25:18:7C:A2:44:63:D6:55:20:A2:3F

**X509SubjectName**

**Subject C:** ES

**Subject ST:** BARCELONA

**Subject L:** HOSPITALET DE LLOBREGAT

**Subject O:** VINTEGRIS SLU

**Subject 2.5.4.97:** VATES-B62913926

**Subject CN:** CA Vintegris SSL TrustServices

**X509SKI**

**X509 SK I** ESaOmpPvDYM6VBzYcBcpzv3QSRs=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2022-10-10T00:00:00Z

**27.11.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>



**28 - TSP: ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.****TSP Name**

**Name** [ en ] *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

**Name** [ es ] *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

**TSP Trade Name**

**Name** [ en ] *esFIRMA*

**Name** [ es ] *esFIRMA*

**Name** [ en ] *VATES-A50878842*

**Name** [ en ] *AULOCE S.A.U.*

**Name** [ en ] *ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.*

**Name** [ en ] *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

**PostalAddress**

**Street Address** [ en ] *Calle Bari 39 (Edificio Binary Building)*

**Locality** [ en ] *Zaragoza*

**State Or Province** [ en ] *Zaragoza*

**Postal Code** [ en ] *50197*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Calle Bari 39 (Edificio Binary Building)*

**Locality** [ es ] *Zaragoza*

**State Or Province** [ es ] *Zaragoza*

**Postal Code** [ es ] *50197*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *<http://www.esfirma.com>*



**Issuer L:** Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

**Issuer O:** AULOCE S.A.U.

**Issuer OU:** AUTORIDAD DE CERTIFICACION ESFIRMA

**Issuer CN:** ESFIRMA AC RAZ

**Issuer 2.5.4.97:** VATES-A50878842

**Subject C:** ES

**Subject L:** Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

**Subject O:** AULOCE S.A.U.

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

**Subject CN:** ESFIRMA AC AAPP

**Subject 2.5.4.97:** VATES-A50878842

**Valid from:** Thu Apr 28 18:05:14 CEST 2016

**Valid to:** Sat Apr 28 18:05:14 CEST 2029

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201009C9B2CF307C99E9EED20662B84BCB021DE78377619B3ED8CF19D127084AA714618BC09DB760EF8F1E7F42AE1A39C76CD691710BBCA6C6F0B673B19FF01979801A70E6163FE125A84E236CF23A3A5579419084CC127DC635A8EC242921C62339F08058FDC648741D4074053BC9A585968B940C7FAE8FC3B7776722B0DD90A09C88DD70230754F6CB8EB324F390E57BA33F148E8E5DFD7558F86704B2669BF3215C3284EA7704A05E577AC6B316AAD5E029603894B40AF724E550E601E39B54BEBF90747A61E3C33694ABDEC6F4050AE977BEB95FCAB45DDCB027996B6D10164473045ARBD74C8A9B5C79157761A69F5183A226FA3CBFBEB85F9A724940A83D90D478759A70082ED478A7A9321F348DD5E9DA337425625265CF883D6090B338F76A118607864F138824ADD2116D8FF55D9476D8990CD6264507C3CDA1A0B2095DDAC99BF0311B1F3CA23EFSAF184066C76D5A42C0CFD39B45BB7659A8095CB5D955F3E97751C42C27CFD2158702B377E7CD0F098C1E1B3501B5BA2FBDFAC2765880F612332D46E88CDA4D9864249F2ID539E0B58EA932880CE2563AA30CB4AE2F52F39DC20A7AA8153BA2278A6AE88B93F451EAT76E76CD93A3B7BA7BDD898BA39984C1FAE9741F59F8D0E04D5451391B0313F8D6781A990A30446D6C88C288F53F8BFD666AC75E91F05A8B0441F2A936F6249D37B80620C75206D547C6F30203010001

**Authority Info Access** <https://www.esfirma.com/doc-pki/esfirma-acraiz.crt>

**Subject Key Identifier** 61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50

**Basic Constraints** *IsCA: true - Path length: 0*

**Authority Key Identifier** FC:EF:B3:1E:C8:78:35:F7:2B:39:3F:16:D4:F5:8C:C1:D1:71:B2:99

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: <https://www.esfirma.com/doc-pki/>*  
*CPS text: [Autoridad de certificación Intermedia de esFirma. Ver <https://www.esfirma.com/doc-pki/>]*

**CRL Distribution Points** <https://crls1.esfirma.com/acraiz/acraiz.crl>  
<https://crls2.esfirma.com/acraiz/acraiz.crl>

**Subject Alternative Name** *info@esfirma.com*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** A2:8B:23:0D:EF:38:3D:C6:A0:39:5F:37:63:E1:01:CC:8C:3F:F6:4D:96:2C:6A:F3:3A:59:28:41:A9:61:26:82

## X509SubjectName

**Subject C:** ES

**Subject L:** Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

**Subject O:** AULOCE S.A.U.

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

**Subject CN:** ESFIRMA AC AAPP

**Subject 2.5.4.97:** VATES-A50878842

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2018-06-25T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 28.1.1 - Extension (critical): Qualifiers [NotQualified]

**Qualifier type description** [en] undefined.

[es] undefined.

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47281.1.2.1

### 28.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**28.1.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

**28.1.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</a>
-----	--------	---

**28.1.5 - History instance n.1 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ en ]	Qualified Certificates issued by ESFIRMA AC AAPP
-------------	--------	--

<b>Name</b>	[ es ]	Certificados Reconocidos emitidos por ESFIRMA AC AAPP
-------------	--------	---

**Service digital identities****X509SubjectName**

<b>Subject C:</b>	ES
-------------------	----

<b>Subject L:</b>	Zaragoza (see current address at <a href="https://www.esfirma.com/doc-pki/">https://www.esfirma.com/doc-pki/</a> )
-------------------	--

<b>Subject O:</b>	AULOCE S.A.U.
-------------------	---------------

<b>Subject OU:</b>	AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP
--------------------	---

<b>Subject CN:</b>	ESFIRMA AC AAPP
--------------------	-----------------

<b>Subject 2.5.4.97:</b>	VATES-A50878842
--------------------------	-----------------

**X509SKI**

<b>X509 SK I</b>	YYIsuzwevS1E4MvwZ0ApgE21o1A=
------------------	------------------------------

<b>Service Status</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a>
-----------------------	---

<b>Status Starting Time</b>	2018-05-24T00:00:00Z
-----------------------------	----------------------

**28.1.5.1 - Extension (critical): Qualifiers [NotQualified]**

Qualifier type description	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47281.1.2.1

**28.1.5.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**28.1.5.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**28.1.5.4 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**28.1.6 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [en] *Qualified Certificates issued by ESFIRMA AC AAPP*

**Name** [es] *Certificados Reconocidos emitidos por ESFIRMA AC AAPP*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

**Subject O:** AULOCE S.A.U.

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

**Subject CN:** ESFIRMA AC AAPP

**Subject 2.5.4.97:** VATES-A50878842

**X509SKI**

**X509 SK I** YYIsuzwevS1E4MvwZ0ApgE21o1A=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2016-06-30T22:00:00Z

**28.1.6.5 - Extension (critical): Qualifiers [NotQualified]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47281.1.2.1
-------------------	------------	---------------------------------

**Policy Identifier:**

<b>Identifier</b>	[OIDAsURN]	urn:oid:1.3.6.1.4.1.47281.1.2.2
-------------------	------------	---------------------------------

**28.1.6.6 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[en]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	------	---

**28.1.7 - History instance n.3 - Status: undersupervision**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

<b>Name</b>	[en]	Qualified Certificates issued by ESFIRMA AC AAPP
-------------	------	--

<b>Name</b>	[es]	Certificados Reconocidos emitidos por ESFIRMA AC AAPP
-------------	------	---

Service digital identities**X509SubjectName**

**Subject C:** ES

**Subject L:** Zaragoza (see current address at <https://www.esfirma.com/doc-pki/>)

**Subject O:** AULOCE S.A.U.

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP

**Subject CN:** ESFIRMA AC AAPP

**Subject 2.5.4.97:** VATES-A50878842

**X509SKI**

**X509 SK I** YYIsuzwevS1E4MvwZ0ApgE21o1A=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision>

**Status Starting Time** 2016-06-23T22:00:00Z

28.1.7.7 - Extension (not critical): Qualifiers [QCForLegalPerson]

<b>Qualifier type description</b>	[en]	it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that all Qualified Certificates issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person ARE issued to Legal Persons.
	[es]	está garantizado por el proveedor de servicios de confianza y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro de referencia (respectivamente su organismo de supervisión o de acreditación) que todos los certificados reconocidos expedidos dentro del servicio (CA raíz/ QC o CA / CC ) identificado en "Service digital identity" y precisado por la información de filtros se utiliza para identificar aún más bajo el "Sdi" servicios fiduciarios identificados, que se emitió el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a personas jurídicas a personas jurídicas.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47281.1.2.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47281.1.2.2

28.2 - Service (withdrawn): Qualified timestamps issued by ESFIRMA TSA

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.





**Subject C:** ES

**Valid from:** Tue May 23 15:28:05 CEST 2017

**Valid to:** Fri May 23 15:28:05 CEST 2025

**Public Key:**  
30:82:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:91:60:A9:3F:AE:03:C8:F9:27:DC:B9:61:DB:18:FA:CD:F5:95:E8:F1:4B:94:47:42:E6:22:C2:EB:10:70:45:87:4B:34:7  
E:D2:72:DC:6A:0A:F4:79:57:1E:5F:A6:52:53:7B:96:A0:23:B3:02:97:DD:03:0D:A2:8B:6D:BB:B2:55:F8:83:A1:F9:21:AA:D4:12:3E:77:DF:3B:EC:AD:31:0E:EB:86:B0:25:50:A1:E3:F7:88:1C:B9:9C:2E:EB:FA:4B:10:AA:  
91:D3:68:0A:7E:A5:0B:01:BB:1B:1B:A7:48:AC:11:6E:18:DB:61:0B:DD:01:08:C4:27:5F:DA:93:E5:88:E3:CF:66:A5:CS:E4:52:42:62:CE:7E:E9:D3:F0:AB:9B:8B:4E:DC:48:5A:6B:B3:95:6C:E3:6E:F0:78:9B:AD:6C:96:D1:  
B4:3D:AA:D3:6F:0B:4C:74:93:F5:1F:24:95:5E:DD:46:AA:07:86:27:3A:C7:FF:B8:F0:32:CF:83:15:1E:1A:5D:23:B7:E9:62:C6:72:EE:01:49:6C:CE:44:E6:29:E0:06:F0:6B:CC:3C:6D:99:DB:3E:E3:EB:14:0F:E2:F8:CD:F6:4C:  
50:E2:38:55:57:42:4E:0B:CD:F2:8B:DB:62:31:CC:F0:79:C8:09:0C:27:43:43:46:15:BE:09:36:7E:FB:DF:FE:1B:36:70:8F:BC:82:FF:98:65:03:7D:7B:1E:66:F6:61:39:D1:1C:BE:D1:D7:56:5A:E4:69:F4:F0:76:EF:75:AF:6D:D8:  
C6:BE:00:F2:E3:D6:E6:91:E3:5E:46:E6:15:00:89:3A:BB:70:97:72:6A:04:61:9A:A3:36:60:51:93:D9:3C:15:C7:0F:0A:7B:14:35:98:D5:C9:89:7A:E4:B7:D3:2B:3D:D4:0D:64:AD:65:39:84:61:C0:F2:79:3B:9C:29:55:7E:50:6D:  
7E:DA:12:D3:83:1C:28:33:84:CS:78:D2:E7:E9:9B:D3:97:02:60:D7:15:85:AF:CB:64:31:EB:11:90:3E:86:D4:39:04:0B:5B:14:C8:A8:B9:10:AA:C6:FC:BD:C2:9F:D2:38:B9:FD:6D:31:15:BE:FA:37:04:05:EB:7A:DE:71:14:DC:  
68:94:73:D7:27:44:35:AB:D9:FE:5F:BI:AA:A3:E8:1E:15:84:46:1B:65:A0:72:A9:CB:81:E4:72:0E:BF:3C:9B:BF:85:67:33:42:2D:CE:9F:CE:3C:B3:78:E7:AE:93:14:70:22:AD:57:4F:D8:A7:AC:86:F9:53:F9:A0:69:AD:A1:C  
D:26:8B:15:13:A5:59:50:44:EB:E3:EE:CO:95:6F:72:52:7D:B4:A6:DB:31:B7:02:03:01:00:01

**Certificate Policies**  
Policy OID: 0.4.0.194112.1.1  
Policy OID: 1.3.6.1.4.1.47281.1.5.2  
CPS pointer: <https://www.esfirma.com/doc-pki/>  
CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte <https://www.esfirma.com/doc-pki/>]

**Subject Key Identifier**  
34:6A:D2:15:11:32:DD:1C:DD:A7:59:8F:E9:09:D4:8E:A6:FC:8E:77

**Authority Key Identifier**  
61:89:6C:BB:3C:1E:BD:2D:44:E0:CB:F0:67:40:29:80:4D:B5:A3:50

**Basic Constraints**  
IsCA: false

**Extended Key Usage**  
id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crls1.esfirma.com/acaapp/acaapp.crl>  
<http://crls2.esfirma.com/acaapp/acaapp.crl>

**Authority Info Access**  
<http://ocsp1.esfirma.com/acaapp/>  
<http://ocsp2.esfirma.com/acaapp/>  
<http://www.esfirma.com/doc-pki/esfirma-acaapp.crt>

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15

**Issuer Alternative Name**  
info@esfirma.com

**Key Usage:**  
nonRepudiation

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
A7:DC:18:B2:E8:2F:38:19:8E:AC:20:69:90:EE:5C:62:B9:85:92:82:A5:AB:B7:7A:C2:A8:65:A5:85  
:2C:97:A2

**X509SubjectName**

**Subject CN:**  
ESFIRMA TSA

**Subject 2.5.4.97:**  
VATES-A50878842

**Subject OU:**  
AUTORIDAD DE CERTIFICACION ESFIRMA

**Subject O:** AULOCE S.A.U.

**Subject L:** Zaragoza

**Subject C:** ES

## X509SKI

**X509 SK I** NGrSFREy3Rzdp1mP6QnUjqb8jnc=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2018-06-25T00:00:00Z

## Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 28.2.1 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

## Service Name

**Name** [en] Qualified timestamps issued by ESFIRMA TSA

**Name** [es] Sellos de tiempo cualificados emitidos por ESFIRMA TSA

## Service digital identities

### X509SubjectName

**Subject CN:** ESFIRMA TSA

**Subject 2.5.4.97:** VATES-A50878842

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA

**Subject O:** AULOCE S.A.U.

**Subject L:** Zaragoza

**Subject C:** ES



**Issuer O:** *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

**Issuer L:** *ZARAGOZA*

**Issuer C:** *ES*

**Subject CN:** *ESFIRMA AC AAPP 2*

**Subject SERIAL NUMBER:** *A50878842*

**Subject OU:** *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

**Subject O:** *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

**Subject L:** *ZARAGOZA*

**Subject C:** *ES*

**Valid from:** *Thu Nov 02 14:12:47 CET 2017*

**Valid to:** *Sat Nov 02 14:12:47 CET 2030*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A028202010088B0A422B9A1D616217B070D523E8D1879D07D16C54FA2EA2DF1D61890F7047030B04  
F856009C9223E9189E372E72903962A3E609277C25B4E71133AC530B3C0D4F6D5D5CB315A16B63A60D8D645143D2C5540FC9C2887CA814E0D0A536D8E5F1EA  
00DC7DE56C01823A7EC910F623FD2C237C0537F10F025A0DFB447ED10D8BA3B1C8CS8A433E5A74D8A6A1B782BBA3B75A6B0E2B2E63DA9E7E2B76B7FFC3367D  
37CF64E4E4DAFF73C4F2C123EE69A9CB764E8EA967C0F1034506023CA1C380AE59E68FA73C730278E9F065B382387B806F666A12D8443ADA7F4D2427F095172421E  
B274305DAA2EB468CE3E35D830034CAE52CB23B9845023945076870635F13C237909321C45AE43293F3119677264A92B08212E5F938E4FBCABE9381D12F4E1C70B  
EDA6E4E87074800B2F956FA73A3D199A0306FB279A8FAA054A97960911A6DB16CC42EC188841C172A20C4AB0D6C86A0FED05A86165CFC41ECF7EE0A2DBFCFA71  
8932681F47A7A8D65D58EF4B2F9277390A68D42B829324D881BD A2ECFA492FBED5DA0873AE658C7D61FCE7E7349AB9F1B0567DA7794F0EB1A03B2A7B7985FBB  
C5CC651B42A854AE9A30AD9514AE1D364E1189C8BFA36DA484A95F4D85CC2FD0BCE0E50D5991A699E3D155C08CF30C1857FC2CE286C47BC3C619C3E89595CA4A  
8DB7E9D4CF2D491C74AF16694E6EEDEE65EBD60212F239D0203010001

**Authority Info Access**  
<https://www.esfirma.com/doc-pki/esfirma-acraiz2.crt>  
<http://ocsp.esfirma.com/acraiz2/>

**Subject Key Identifier**  
*F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Authority Key Identifier**  
*83:80:E5:D6:27:BD:EF:30:B2:AE:1D:9D:CA:A8:F2:32:14:C7:13:32*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <https://www.esfirma.com/doc-pki/>*  
*CPS text: [Autoridad de certificación AAPP 2 de esFirma. Ver <https://www.esfirma.com/doc-pki/>]*

**CRL Distribution Points**  
<https://crls1.esfirma.com/acraiz/acraiz2.crl>  
<https://crls2.esfirma.com/acraiz/acraiz2.crl>

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*2C:18:23:61:9D:80:73:11:6C:8F:14:8B:D3:85:79:DE:9C:05:39:16:02:DB:CE:B9:65:73:E4:A1:88:E  
1:32:6E*

Subject CN: *ESFIRMA AC AAPP 2*

Subject SERIAL NUMBER: *A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject L: *ZARAGOZA*

Subject C: *ES*

**X509SKI**

X509 SK I *9kDvw6crTeW/Men67sN5eR8qA1g=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Service status description *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2021-10-26T01:00:00Z*

**Scheme Service Definition URI**

URI *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**28.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**28.3.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**28.3.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** [ en ] *Qualified Certificates issued by ESFIRMA AC AAPP 2*

**Name** [ es ] *Certificados Cualificados emitidos por ESFIRMA AC AAPP 2*

### Service digital identities

#### X509SubjectName

**Subject CN:** *ESFIRMA AC AAPP 2*

**Subject SERIAL NUMBER:** *A50878842*

**Subject OU:** *AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP*

**Subject O:** *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

**Subject L:** *ZARAGOZA*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *9kDvw6crTeW/Men67sN5eR8qA1g=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-06-25T00:00:00Z*

#### 28.3.3.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

#### 28.3.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

#### 28.3.3.3 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*





**Subject 2.5.4.97:** VATES-A50878842

**Subject SERIAL NUMBER:** A50878842

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA

**Subject O:** ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

**Subject L:** ZARAGOZA

**Subject C:** ES

**Valid from:** Wed Jun 20 11:28:38 CEST 2018

**Valid to:** Tue Jun 20 11:28:38 CEST 2023

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A028202010094C859192C681AA80E47E7ED6266828360D17011B917768D9143924EA3C02E01B38C39DD34B5B3CE99917F5E5978BE51FBEB25722A5D5E5E979E843C9AE7B6076D50CAB92F7E8DD3305046A3E2A9C16EA7294EAS833D99715C07E1D0B2FFD950880ABD1C372CC185AADFD03F44E3C3B3D838DE4A92000DA6968F9A04ED23E3EB3E0EFD64AE3EC62BC7E1D4332A9148D3ED2CF6328638EA CD4C565E9EFD57DD47A3CE24BBD7E88053D452DC4446DB4FC823B2AF90DD6C595FA450E95454BCF9CA4217416C0819C0746BF03122D7EE6493BE394A28F0763A9C735DB9F3B4B6291E1CF0CD E2847A3016C594C13A7008C4369B1D74BA475E8CA1042DE8B6136C743B2019D4D202510193A9FFEE9129AB97B3323F29F73A78CAAE4E2927E4B3F7BD08EB5CBEAF64B142A9D711B059FAE0FB4933FFE3CD E357FFBF7679989F20FF40AB5160CEA4C8127E DB5C598899BF83DE3E9053DE02A842CE5C42C6F6D26734B1B09AF20D893D81D4DA7805A063DA1773B8C94413E72AE414AF56B98FC535B40B1133EBC E7AA75FC E19A1B22FC C7684AB96FB2DF7332D210AE29D38B39B8E9D28FBD CF D369CF1B3E4C1BBAS37739341DB5727F54FC A36C9BBCC8B64AF43F1BF5425CB37FE B9F7B593CC E897C400A506DD EE999E56D0C88A41083E0274DD D977997B0B64872B D53F344257EE7EE61782FCA4C7C6D729B646D6B8599D75BA2810203010001

**Certificate Policies**  
 Policy OID: 0.4.0.194112.1.1  
 Policy OID: 1.3.6.1.4.1.47281.1.5.2  
 CPS pointer: <https://www.esfirma.com/doc-pki/>  
 CPS text: [Servidor de sellado de tiempo de esFIRMA. Consulte <https://www.esfirma.com/doc-pki/>]

**Subject Key Identifier**  
 2D:A6:23:DD:87:8F:07:E7:D8:3D:32:1F:EE:69:E4:37:7F:55:F5:5D

**Authority Key Identifier**  
 F6:40:EF:C3:A7:2B:4D:E5:BF:31:E9:FA:EE:C3:79:79:1F:2A:03:58

**Basic Constraints**  
 IsCA: false

**Extended Key Usage**  
 id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crls1.esfirma.com/acaapp/acaapp2.crl>  
<http://crls2.esfirma.com/acaapp/acaapp2.crl>

**Authority Info Access**  
<http://ocsp1.esfirma.com/acaapp2/>  
<http://ocsp2.esfirma.com/acaapp2/>  
<https://www.esfirma.com/doc-pki/acaapp2.crl>

**QCStatements - crit. = false**  
 id\_etsi\_qcs\_QcCompliance  
 id\_etsi\_qcs\_RetentionPeriod: 15

**Key Usage:**  
 nonRepudiation

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 F7:D4:39:1C:50:C3:42:98:9B:94:63:F8:5F:DB:BB:71:18:AC:03:A5:64:4A:3A:68:A1:83:65:AB:A5:07:9E:52

**X509SubjectName**

Subject CN: *ESFIRMA TSA 2*

Subject 2.5.4.97: *VATES-A50878842*

Subject SERIAL NUMBER: *A50878842*

Subject OU: *AUTORIDAD DE CERTIFICACION ESFIRMA*

Subject O: *ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA*

Subject L: *ZARAGOZA*

Subject C: *ES*

**X509SKI**

X509 SK I *LaYj3YePB+fYPTIf7mnkN39V9V0=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

Service status description *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2023-12-21T00:00:00Z*

**Scheme Service Definition URI**

URI *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**28.4.1 - History instance n.1 - Status: granted****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

Name *[en]* *Qualified timestamps issued by ESFIRMA TSA 2*

Name *[es]* *Sellos de tiempo cualificados emitidos por ESFIRMA TSA 2*

**Service digital identities****X509SubjectName**

Subject CN: *ESFIRMA TSA 2*

**Subject 2.5.4.97:** VATES-A50878842

**Subject SERIAL NUMBER:** A50878842

**Subject OU:** AUTORIDAD DE CERTIFICACION ESFIRMA

**Subject O:** ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

**Subject L:** ZARAGOZA

**Subject C:** ES

**X509SKI**

**X509 SK I** LaYj3YePB+fYPTIf7mnkN39V9V0=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2018-06-25T00:00:00Z

**28.5 - Service (granted): Sellos de tiempo cualificados emitidos por ESFIRMA TSA - QTSU 2023**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [es] Sellos de tiempo cualificados emitidos por ESFIRMA TSA - QTSU 2023

**Name** [en] Qualified timestamps issued by ESFIRMA TSA - QTSU 2023

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 90804929519106285598314512538477159492



**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.47281.1.5.2  
 CPS pointer: <https://www.esfirma.com/doc-pki/>  
 Policy OID: 0.4.0.194112.1.1

**Extended Key Usage**  
 id\_kp\_timeStamping

**QCStatements - crit. = false**  
 id\_etsi\_qcs\_QcCompliance  
 id\_etsi\_qcs\_RetentionPeriod: 15

**CRL Distribution Points**  
<http://crls1.esfirma.com/acaapp/acaapp2.crl>  
<http://crls2.esfirma.com/acaapp/acaapp2.crl>

**Subject Key Identifier**  
 07:E7:54:A6:76:71:04:C8:27:7F:C3:BF:11:84:66:CA:88:F2:0C:82

**Key Usage:**  
 nonRepudiation

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 A3:F6:62:B0:19:C7:5D:A7:82:3B:A5:BF:5F:EE:B2:AC:77:A9:C2:04:FD:7E:C6:4B:2B:F0:15:9C:57:89:36:A0

**X509SubjectName**

**Subject CN:**  
 ESFIRMA TSA - QTSU 2023

**Subject 2.5.4.97:**  
 VATES-A50878842

**Subject O:**  
 ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

**Subject C:**  
 ES

**X509SKI**

**X509 SK I**  
 B+dUpnZxBMgnf8O/EYRmyojyDII=

**Service Status**  
<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**  
 [en] undefined.  
 [es] undefined.

**Status Starting Time**  
 2023-04-20T00:00:00Z

**29 - TSP: SIGNATURIT SOLUTIONS, S.L.U.****TSP Name**

**Name** [ en ] *SIGNATURIT SOLUTIONS, S.L.U.*

**Name** [ es ] *SIGNATURIT SOLUTIONS, S.L.U.*

**TSP Trade Name**

**Name** [ en ] *Signaturit Solutions S.L.*

**Name** [ en ] *VATES-B66024167*

**Name** [ en ] *SIGNATURIT SOLUTIONS, SL*

**Name** [ en ] *SIGNATURIT SOLUTIONS, S.L.U.*

**PostalAddress**

**Street Address** [ en ] *Avila Street 29*

**Locality** [ en ] *Barcelona*

**State Or Province** [ en ] *Barcelona*

**Postal Code** [ en ] *08005*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Calle Ávila 29*

**Locality** [ es ] *Barcelona*

**State Or Province** [ es ] *Barcelona*

**Postal Code** [ es ] *08005*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:legal@signaturit.com*

**URI** [ es ] *mailto:legal@signaturit.com*

**URI** [ en ] *https://www.signaturit.com/en*



**Issuer O:** *Signaturit Solutions S.L.*

**Issuer 2.5.4.97:** *VATES-B66024167*

**Subject CN:** *Signaturit TSA*

**Subject C:** *ES*

**Subject L:** *Barcelona*

**Subject O:** *Signaturit Solutions S.L.*

**Subject 2.5.4.97:** *VATES-B66024167*

**Valid from:** *Tue Jul 03 11:21:11 CEST 2018*

**Valid to:** *Sun Jul 02 11:21:11 CEST 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100F0778D50CF9A2FF4AD7F11881213B54E4A6265E05CC07C8FEE6B0CB3C795A6B061506FB3FAB64E85810BCEDF76A61FFFAEDFFBA DA3607354B9859AF7C5216C7528B C01E7752073B3C859CAAE830DD6E4582D22D32D5C12A98C25021B58AF36C3BB13720C5CB964B1A5DF95B94B4242120211EDAB7521ED3D48931385A4D2D302CS D8769EB44C3564DBF59F6D3BF34FA9BD919A3C746B89DC93D90686DFEE2D63C322F7DA D F5 AF 72 F2 D3 0E 55 53 91 46 D6 7A 70 FD A6 D4 5B 1A 01 27 D0 BC FD B7 E2 55 73 95 E9 DA 60 E6 34 A5 11 02 73 5F A1 11 70 0D 9F 14 50 AF 9D A7 23 2A 3C 39 95 46 DF 74 E1 9D 71 74 24 4A 6F 5E D3 55 B0 8C 78 F9 1E ED A1 D8 10 FF 74 BD 12 6A 08 17 DA 1A F8 02 F0 12 5D 06 31 C3 02 03 01 00 01

**Subject Key Identifier** *48:A3:10:E6:69:DA:C3:EC:47:A1:BB:6C:34:F5:15:24:48:20:4E:DF*

**Authority Key Identifier** *8A:AD:21:CB:B2:26:6C:30:CC:D2:D3:24:78:87:21:2E:5E:BA:01:29*

**CRL Distribution Points** *<http://pki.signaturit.com/crl/Signaturit%20Issuing%20CA.crl>*

**Authority Info Access** *[http://pki.signaturit.com/cert/CA02.signaturit.com\\_Signaturit%20Issuing%20CA.crt](http://pki.signaturit.com/cert/CA02.signaturit.com_Signaturit%20Issuing%20CA.crt)  
<http://pki.signaturit.com/ocsp>*

**Extended Key Usage** *id\_kp\_timeStamping*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.50646.3.1  
CPS pointer: <http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf>*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *49:77:F6:AA:EA:C4:E2:A0:45:E8:37:10:1D:CE:BA:10:A3:FE:5E:57:F7:41:55:87:FD:04:30:0F:B2:19:87:86*

**X509SubjectName**

**Subject CN:** *Signaturit TSA*

**Subject C:** *ES*

**Subject L:** *Barcelona*



**Subject O:** *Signaturit Solutions S.L.*

**Subject 2.5.4.97:** *VATES-B66024167*

## X509SKI

**X509 SK I** *SKMQ5mnaw+xHobtsNPUVJEggTt8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2024-01-24T02:00:00Z*

### 29.1.1 - History instance n.1 - Status: granted

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

## Service Name

**Name** *[es] Sellos de tiempo cualificados emitidos por Signaturit TSA*

**Name** *[en] Qualified timestamps issued by Signaturit TSA*

## Service digital identities

### X509SubjectName

**Subject CN:** *Signaturit TSA*

**Subject C:** *ES*

**Subject L:** *Barcelona*

**Subject O:** *Signaturit Solutions S.L.*

**Subject 2.5.4.97:** *VATES-B66024167*

## X509SKI

**X509 SK I** *SKMQ5mnaw+xHobtsNPUVJEggTt8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-11-22T01:00:00Z*

### 29.2 - Service (withdrawn): Qualified certificates issued by Signaturit Qualified Issuing CA



**Subject 2.5.4.97:** VATES-B66024167

**Valid from:** Fri Feb 08 15:29:03 CET 2019

**Valid to:** Thu Feb 08 15:39:03 CET 2029

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100E67F21F461B5040F36D92CE38EB68E578A635B74AE80DE2B58C7C32CA374FB8B0A7C  
FA2EFC8512BF19480F08A72F88888BD8E1C0F5993FB6B1EF1E31717753ED32DB7375E5CE16949318E57A59E96EEDC194A2E394BC7BFAD932E167B15E5F85A9E22  
5AD9911DA7A79B8EBE37E91E40C1DF31DC0E6CCECB9A939E64D9AD31E206DC685965F743016E88C9F52F896058EEBA16E30A3A9E41ABEE7CB4471F5E1A756C0  
A4770F88A266995D0A55B8500D703AA5E6DF9A96464E803E176BA5E1E86F3487B9D556231991375220C951BC20B1014F442D2A37155A869911B9962C669D3E70E087F  
C171EA878449A1E59A081DE726663CEA0B721B49250DC8AAEDD43C53F7166F853B9EA22F49FB5C886603D3D779EB0E1CD990F34F9AC1A3AC1DE2E4E150E35121D1  
E592F686194AC6E72D4A92B87926A8E470BFA31A7B6D58FEE5E28F77225B88C47439991A5668892670DE938334E3D9087C40E9362FA7F9F8B5DB1DD6CDDA4DC530  
E86D39FE31C77DD9E5A329BCDE869836E55EAC3CAA1ED8EE21FF843B3A2E31A826D293BEA4C965A456512384F9DB0E6227296D135A2E17F2EF9C2C9600BF16C90  
2183FCE5B518F4E27F6F653D82521173DA6F46EC00A508B41A0897A88428CA690FA9A61BFA81B5FD1C1A1A55DE0F18D80682601815BE47D985E3AC928EC7079E3  
AF624439D784BCAECE9A4C6614B7E568467B149DF70203010001

**Subject Key Identifier** 73:C5:0A:5C:CC:9A:93:F0:CD:C5:2F:7A:B0:16:CA:40:AB:02:5B:D8

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.50646.2.1  
CPS pointer: <http://pki.signaturit.com/pki/CP.Natural.Persons.pdf>  
Policy OID: 1.3.6.1.4.1.50646.3.1  
CPS pointer: <http://pki.signaturit.com/pki/CP.Legal.Representatives.pdf>  
Policy OID: 1.3.6.1.4.1.50646.4.1  
CPS pointer: <http://pki.signaturit.com/pki/CP.Electronic.Seals.pdf>  
Policy OID: 0.4.0.194112.1.2  
Policy OID: 0.4.0.194112.1.3

**Basic Constraints** IsCA: true

**Authority Key Identifier** DF:7C:52:E1:06:CA:6D:30:C2:7C:67:8D:0C:18:9D:0C:EF:0B:7C:7D

**CRL Distribution Points** <http://pki.signaturit.com/crl/Signaturit%20Root%20CA.crl>

**Authority Info Access** [http://pki.signaturit.com/cert/CA01\\_Signaturit%20Root%20CA.crt](http://pki.signaturit.com/cert/CA01_Signaturit%20Root%20CA.crt)

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** C9:DD:26:58:A3:05:CA:25:75:1E:35:90:D5:5D:61:9A:22:AE:67:D9:98:F1:E7:E9:8A:BE:91:F6:3A:9B:2A:90

**X509SubjectName**

**Subject CN:** Signaturit Qualified Issuing CA

**Subject DC:** signaturit

**Subject DC:** com

**Subject C:** ES

**Subject O:** Signaturit Solutions S.L.

**Subject 2.5.4.97:** VATES-B66024167

**X509SKI**

**X509 SK I** *c8UKXMyak/DNxS96sBbKQKsCW9g=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2024-01-24T02:00:00Z*

**29.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**29.2.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDA sURN ] urn:oid:1.3.6.1.4.1.50646.2.1*

**Description****29.2.3 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service Name**

**Name** *[ en ] Qualified certificates issued by Signaturit Qualified Issuing CA*

**Name** *[ es ] Certificados cualificados emitidos por Signaturit Qualified Issuing CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *Signaturit Qualified Issuing CA*

**Subject DC:** *signaturit*

Subject DC: com

Subject C: ES

Subject O: Signaturit Solutions S.L.

Subject 2.5.4.97: VATES-B66024167

**X509SKI**

X509 SK I c8UKXMyak/DNxS96sBbKQKsCW9g=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Status Starting Time 2019-10-01T01:00:00Z

**29.2.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**29.2.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

Qualifier type description [ en ] undefined.

[ es ] undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

Identifier [ OIDsURN ] urn:oid:1.3.6.1.4.1.50646.2.1

**Description****29.3 - Service (withdrawn): Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"**

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description [ en ] An electronic delivery service providing qualified electronic deliveries.

[ es ] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

**Service Name**

Name [ en ] Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"



**Subject OU:** *LEGAL*

**Subject 2.5.4.97:** *VATES-B66024167*

**Subject CN:** *SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER*

**Valid from:** *Fri Jan 24 09:18:42 CET 2020*

**Valid to:** *Mon Jan 23 09:18:42 CET 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100E26D10D29F6E8DBD38FB95DDF8C80E01E80BC240FFA29CD2E833DC8E1E1BFE90289EEA390A460BDAD03E733369E2A82B7DA43B7A2AA26001D5756EBD9858879F619D9BE6C23E2EE8B122989AEAA3EBE8AEC7A626B357D2B140D87C7ECE751437E93D E635C8BC3DD68027094D7B452B8C09DEE753EB8E499D49E3E15FDD4B5115A131C5036C994A6497D85E1CE9E04448B5EA0B32E426B33FE188639879C098B4A801DB B7D25A37FE06AA8A1363416756AC79247AF475EBDAAB3C680B884CA3AB60E011A1F8EC7A84F61A09427AA2EFD74477B86FDE0D936C8DA99818D3FD11CA7610A 208B897A8435688CBAC074E6A12A01D25030EE4E21E142DECF4DC8F0203010001

**Basic Constraints** *IsCA: false*

**Extended Key Usage** *id\_kp\_clientAuth*

**Subject Key Identifier** *B1:0E:7D:B4:B9:8E:7B:DF:00:7E:1F:D7:7C:B4:C9:12:87:A6:27:0D*

**Authority Info Access**  
*http://www.camerfirma.com/certs/ac\_camerfirma\_legal\_persons-2016.crt*  
*http://ocsp.camerfirma.com*

**Authority Key Identifier** *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

**CRL Distribution Points**  
*http://crl.camerfirma.com/ac\_camerfirma\_legal\_persons-2016.crl*  
*http://crl1.camerfirma.com/ac\_camerfirma\_legal\_persons-2016.crl*

**Subject Alternative Name**  
*legal@signaturit.com*  
*OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO*

**Issuer Alternative Name** *ca@camerfirma.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2*  
*CPS pointer: https://policy.camerfirma.com*  
*CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]*  
*Policy OID: 0.4.0.194112.1.1*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *E1:89:8C:7B:47:8C:21:F3:CB:45:48:D7:A6:CA:F5:AC:F2:C9:DE:B5:6D:9D:70:65:BA:B2:E1:4D:1E:3D:BD:14*

**X509SubjectName**

**Subject C:** ES

**Subject O:** SIGNATURIT SOLUTIONS, SL

**Subject OU:** LEGAL

**Subject 2.5.4.97:** VATES-B66024167

**Subject CN:** SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER

**X509SKI**

**X509 SK I** sQ59tLmOe98Afh/XfLTJEoemJw0=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2021-07-01T01:00:00Z

**29.3.1 - History instance n.1 - Status: granted****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

**Service Name**

**Name** [en] Qualified electronic registered delivery service "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"

**Name** [es] Servicio cualificado de entrega electrónica certificada "SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER"

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject O:** SIGNATURIT SOLUTIONS, SL

**Subject OU:** LEGAL

**Subject 2.5.4.97:** VATES-B66024167

**Subject CN:** SIGNATURIT SOLUTIONS, S.L., QUALIFIED TRUST SERVICES PROVIDER

**X509SKI**





**Issuer ST:** VALENCIA

**Issuer C:** ES

**Subject CN:** Signaturit Global CA

**Subject O:** Signaturit Solutions S.L.U.

**Subject 2.5.4.97:** VATES-B66024167

**Subject ST:** BARCELONA

**Subject C:** ES

**Valid from:** Thu Mar 02 10:51:30 CET 2023

**Valid to:** Fri Mar 02 10:51:30 CET 2035

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:CC:97:29:EA:0F:D8:A9:6B:10:27:30:32:C4:14:B8:A1:AB:33:92:D7:E2:2A:76:20:C3:53:B2:87:62:BB:5F:4D:EF:DF:DC:1A:5E:59:62:38:B1:EA:F3:95:E1:E4:44:9A:2A:A7:E4:F9:D7:53:B9:96:28:D8:36:88:11:CC:7D:2E:50:54:50:ED:EB:65:A7:49:BC:75:93:75:0C:6F:DE:4D:C9:D9:1E:25:87:D5:BE:07:23:49:0B:E8:80:B4:6B:EC:05:CC:6E:7E:CD:6E:48:EF:AD:BB:1B:47:F0:59:1D:E6:1A:A1:49:AA:34:2D:03:9B:33:42:54:72:A4:6F:C2:08:27:1C:01:04:59:0A:90:4F:42:C9:33:0F:2B:EB:20:03:79:0E:33:63:62:4C:5B:2F:FC:59:16:33:21:25:67:4B:6D:3B:80:59:9:9:25:83:E7:AA:25:3E:D5:7B:E4:53:FB:41:AC:5B:D9:97:95:2F:CC:84:29:1B:04:6F:9E:D8:93:43:06:79:A2:EF:5C:67:EC:1B:C0:E2:4E:21:D8:17:9D:CE:C5:1A:25:98:63:99:39:EE:DE:5E:40:D3:DF:02:74:F8:45:21:EE:83:FA:07:8A:F5:D6:8F:31:70:B7:F3:C1:A3:9A:7D:69:BA:86:ES:CE:D1:97:14:7F:C3:33:9E:61:9B:FF:6E:15:CB:03:1:43:46:13:97:E4:28:8C:F7:03:A5:BB:0D:B6:38:24:C5:6A:34:9E:32:2F:09:8A:5A:AC:F5:CB:D0:CB:2C:1E:A3:F7:49:BF:80:91:38:BA:51:02:80:DC:00:98:44:80:54:7D:5E:B4:16:75:2B:A5:90:20:19:1A:8A:6E:68:A1:DD:BF:94:DC:00:9F:23:14:C5:6F:4F:07:76:F9:D8:80:E9:80:61:63:94:ED:DE:65:96:08:EB:23:5D:23:97:33:9E:1A:B7:C:FBD:41:3A:8E:B2:97:9C:40:D1:39:7B:6E:76:49:35:81:7A:55:24:01:62:6B:6F:DA:64:74:0B:25:D4:BF:92:75:BF:3C:59:54:BD:FC:AB:22:F5:39:21:36:49:10:F7:49:74:AC:A4:B3:F1:16:E8:5F:EF:87:7C:9D:22:5F:AA:AA:B2:2A:9C:CE:B0:6F:34:4C:EC:97:1B:D4:E9:80:A2:02:3A:53:94:3C:D1:2B:8A:37:C7:44:38:97:37:CF:52:18:8A:9A:9B:2F:1E:1C:48:36:B6:11:E1:E3:A5:AB:65:48:CE:EC:62:6A:14:59:21:DE:BA:04:42:F4:1A:20:6E:CB:0E:06:78:43:C7:03:3D:42:50:8B:C1:BB:F4:DC:67:1A:B2:A2:2A:78:77:02:03:01:00:01

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 12:30:E9:1B:12:E6:3F:40:D3:E3:EE:9C:E1:EF:FF:64:EC:AF:25:97

**Authority Key Identifier** 38:D0:55:F8:59:2B:12:53:08:44:48:8A:2F:70:03:49:71:80:13:1E

**Authority Info Access**  
<http://ca.ivsign.com/certs/ivsignrootca.crt>  
<http://ocsp.ivsign.com>  
<http://ocsp2.ivsign.com>

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://policy.signaturit.com>  
CPS text: [Signaturit Global CA. Certification Practice Statements and Certificate Policies: <https://policy.signaturit.com>]

**CRL Distribution Points**  
<http://crl1.ivsign.com/ivsignroot.crl>  
<http://crl2.ivsign.com/ivsignroot.crl>

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 3B:E0:56:DA:32:62:3D:5E:00:6C:90:00:6A:84:66:15:EF:C4:A7:57:3F:F3:39:60:7F:A0:14:4B:F9:20:FA:F4

**X509SubjectName**

**Subject CN:** Signaturit Global CA

**Subject O:** *Signaturit Solutions S.L.U.*

**Subject 2.5.4.97:** *VATES-B66024167*

**Subject ST:** *BARCELONA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *EjDpGxLmP0DT4+6c4e//ZOyvJZc=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-10-24T00:00:00Z*

**29.4.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**30 - TSP: IVNOSYS SOLUCIONES S.L.U.****TSP Name**

**Name** [ es ] *IVNOSYS SOLUCIONES S.L.U.*

**Name** [ en ] *IVNOSYS SOLUCIONES S.L.U.*

**TSP Trade Name**

**Name** [ en ] *IVNOSYS*

**Name** [ en ] *IVNOSYS SOLUCIONES S.L.*

**Name** [ en ] *VATES-B98333362*

**Name** [ es ] *VATES-B98333362*

**Name** [ en ] *SIGNATURIT-IVNOSYS*

**PostalAddress**

**Street Address** [ en ] *C/Acceso Ademuz 12-1º-Oficina 1*

**Locality** [ en ] *Paterna*

**State Or Province** [ en ] *Valencia*

**Postal Code** [ en ] *46980*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/Acceso Ademuz 12-1º-Oficina 1*

**Locality** [ es ] *Paterna*

**State Or Province** [ es ] *Valencia*

**Postal Code** [ es ] *46980*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:administracion@ivnosys.com*

**URI** [ es ] *https://www.ivnosys.com*



**Issuer O:** AC CAMERFIRMA S.A.

**Issuer 2.5.4.97:** VATES-A82743287

**Issuer SERIAL NUMBER:** A82743287

**Issuer OU:** CHAMBERS OF COMMERCE ROOT - 2016

**Issuer OU:** see current address at [www.camerfirma.com/address](http://www.camerfirma.com/address)

**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject CN:** IVSIGN CA

**Subject O:** IVNOSYS SOLUCIONES S.L.

**Subject 2.5.4.97:** VATES-B98333362

**Subject OU:** see current address at <https://psec.ivnosys.com/address>

**Subject L:** PATERNA

**Subject C:** ES

**Valid from:** Thu Oct 05 12:09:20 CEST 2017

**Valid to:** Fri Mar 16 11:09:20 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100D6CB0457B92019CE3FA4D96B7A15EF05BBF7ACFEFA3598BCB5F1827978C9CEFB0CB7  
41558779CA7142FE54260912986B3A066F6A0FC41915E42538D9599FC031C8984FB88A9650BA0E7F4D7C1D0E519B06C6594DAD65A0F0054F2A29138EE94DB0742B  
F55BF01AB2576E3E85A2D76113C058C6264C8359F065BAA36AF4B0E59324ED989CD3E6C562A10EE2774A1FE05DBEBE9C9C94FA014DBA5B060187D100BD3DD  
B3AB917FF25BB8DA7AF64056D8E8C4667FF9B346491A95C64785E752A8A04DB871DCFEAC67CD23E0023A341D1F67753E3C4AD7157B123A3EFA0487505CD68E73  
6A8B9B55B3B9B6AD70C38163AB6B5C1C09285994783EA1AF5720EAC930E87E8CD58607417F237D20FDD735C0DFE969C88BA60D1367509742C3F9BD16FD887034C1  
889FC8F7E60D541C63C6E337CFBC16E27C5C85A49BD735A787C800F87CAB61835E224B2B520F095B9B67F096C44781D1CD3935597A3746D361BA22C4EE42B033433  
B484C13ACDD700AD12F8B9C8FC66F574578FD15328FDCA34748F93AC5D06576CFC1621EDFD1FE1E8291D8AD2A6F22BE221598F6891B4DADF52E41CC415A14A5  
46848EAK5094ACAB99857B858561AE3D95039E104B9CB9A26969064563654644D081F3AC4F7B72613F26B585BBF2C77F4D9133C9AB8E70968F0D48BC31A1D9F96D66  
8B436B63A26F0F2F97B4E100D20B10086B1828BF3A752D0203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *05:2D:62:F4:9B:C8:FD:62:24:F9:26:8C:21:35:1F:3D:2E:7C:12:0A*

**Authority Key Identifier** *9E:2E:65:4F:3E:57:F5:AB:7D:96:C6:8B:DF:B3:35:6D:4A:E8:9E:8B*

**Authority Info Access**  
<http://www.camerfirma.com/certs/chambersofcommerceroor-2016.crt>  
<http://ocsp.camerfirma.com>

**Extended Key Usage** *id\_kp\_clientAuth*

**Certificate Policies**  
Policy OID: 2.23.140.1.2.2  
CPS pointer: <https://policy.camerfirma.com>

**CRL Distribution Points** <http://crl.camerfirma.com/chambersofcommerceroot-2016.crl>  
<http://crl1.camerfirma.com/chambersofcommerceroot-2016.crl>

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *92:19:3F:42:7D:FD:45:D1:F7:EE:0C:0A:3B:1A:97:4E:A7:AF:76:79:18:39:90:E2:87:62:C1:3A:26:3D:B9:78*

**X509SubjectName**

**Subject CN:** *IVSIGN CA*

**Subject O:** *IVNOSYS SOLUCIONES S.L.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject OU:** *see current address at <https://psec.ivnosys.com/address>*

**Subject L:** *PATERNA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *BS1i9JvI/WIk+SaMITUfPS58Ego=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2023-05-22T00:00:00Z*

**30.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**30.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3
<b>Description</b>		

**30.1.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ en ] *Qualified Certificates issued by IVSIGN CA*

**Name** [ es ] *Certificados cualificados emitidos por IVSIGN CA*

**Service digital identities****X509SubjectName**

**Subject CN:** *IVSIGN CA*

**Subject O:** *IVNOSYS SOLUCIONES S.L.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject OU:** *see current address at <https://psec.ivnosys.com/address>*

**Subject L:** *PATERNA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *BS1i9JvI/Wik+SaMITUfPS58Ego=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2019-10-28T01:00:00Z*



**30.1.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

<b>URI</b>	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
------------	--------	---

**30.1.3.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[ en ]	undefined.
	[ es ]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3">urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3</a>
-------------------	-------------	---

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3">urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3</a>
-------------------	-------------	---

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3">urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3</a>
-------------------	-------------	---

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	<a href="urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3">urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3</a>
-------------------	-------------	---

**Description****30.1.4 - History instance n.2 - Status: granted**

<b>Service Type Identifier</b>	<a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a>
--------------------------------	---

**Service Name**

<b>Name</b>	[ en ]	Qualified Certificates issued by IVSIGN CA
-------------	--------	--

<b>Name</b>	[ es ]	Certificados cualificados emitidos por IVSIGN CA
-------------	--------	--

**Service digital identities****X509SubjectName**

<b>Subject CN:</b>	IVSIGN CA
--------------------	-----------

**Subject O:** *IVNOSYS SOLUCIONES S.L.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject OU:** *see current address at <https://psec.ivnosys.com/address>*

**Subject L:** *PATERNA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *BS1i9JvI/WIk+SaMITUfPS58Ego=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2018-11-22T01:00:00Z*

**30.1.4.3 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>*

**30.1.4.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.4.16.1.2.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.4.16.1.3.1.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.4.16.1.3.2.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.4.16.1.3.3.3*

**Description**



**Subject O:** *IVNOSYS SOLUCIONES S.L.U.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject OU:** *TRUST SERVICES*

**Subject ST:** *VALENCIA*

**Subject C:** *ES*

**Valid from:** *Fri Sep 11 11:59:33 CEST 2020*

**Valid to:** *Sat Sep 11 11:59:33 CEST 2032*

**Public Key:**  
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:B5:D9:11:D2:CC:61:0A:97:75:0D:25:3D:B5:2D:70:47:04:03:59:70:0D:40:56:1E:6F:B0:77:0E:D1:A2:CF:37:6F:FB:2  
14C:57:61:47:78:84:51:2F:DC:DB:C3:B5:A9:D2:BB:7B:12:09:E1:1B:52:A6:78:F3:82:62:D8:B5:53:91:63:BD:C9:14:99:9C:69:7C:09:DF:15:31:D8:18:21:1C:C5:56:83:0E:6A:2D:6A:AD:02:CC:3C:74:48:CB:7A:15:21:5E:B2  
09:ED:BA:14:1B:27:DE:29:75:BD:BD:95:A5:E9:C8:20:0B:62:47:7B:FD:57:45:5B:89:09:CE:E5:F2:8C:A0:9C:1F:3B:65:1D:6E:C3:FE:67:A3:53:F8:EB:2E:1E:D1:7B:90:2F:97:E4:D3:EE:4A:33:95:C5:87:AB:2E:B8:32:91:41  
4B:8D:15:F7:B7:F9:BB:E5:D0:C2:BD:21:BE:26:86:68:B6:4A:B6:F8:7C:31:51:44:C4:5E:51:44:79:F7:8B:37:85:06:E2:36:3D:2A:18:5E:50:54:3C:29:5B:3C:BA:2C:4A:8F:09:67:B0:E8:14:95:1E:7B:37:A9:DF:9C:F7:79:59:22  
24:87:9A:9C:6E:45:EE:0A:18:03:09:B3:6B:A0:27:0C:7E:75:FE:7E:84:F9:65:77:D1:31:DA:2E:D9:0B:F2:87:9E:F6:0A:55:A7:DC:FF:32:27:4D:7C:1D:48:67:86:BE:7D:A0:69:F6:46:A3:DD:38:02:90:EB:F8:16:19:2B:11:5  
5:CF:98:B0:57:41:44:2E:BC:59:48:57:67:28:7B:FD:F2:F0:E8:8C:D7:9D:5B:6D:0F:71:CF:AC:C5:1CA:280:18:52:52:A1:0F:D3:E3:FD:4F:F9:0F:4C:71:52:BB:D2:58:EE:CA:0D:FE:C6:1D:C7:19:EA:4D:3D:5B:1E:F1:CA:68:  
92:42:07:D3:72:98:2B:0F:0F:88:62:BA:B8:2E:42:12:F2:FD:BD:22:C8:FF:AS:AF:27:32:09:90:09:75:30:53:1D:0F:E0:E2:58:DE:45:62:AE:E7:18:06:58:9D:03:CC:0E:71:30:EB:F8:16:04:0C:B6:0A:1A:7E:13:75:17:76:8B:8E:E  
1:16:66:6A:15:DB:C3:91:8A:48:5C:54:10:0F:5A:50:81:AF:3D:FF:A9:0A:D6:C2:6C:53:EE:BB:5D:F1:91:7F:9A:DD:34:A5:21:C8:2C:E0:6E:A7:56:3F:66:0B:CA:03:5F:EF:5E:13:21:F2:C4:79:DA:5D:6F:72:26:9E:2C:85:D0:  
00:64:20:68:1C:7B:A3:DD:37:26:85:C1:FE:78:66:D1:15:65:1E:B7:02:03:01:00:01

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

**Authority Key Identifier** *38:D0:55:F8:59:2B:12:53:08:44:48:8A:2F:70:03:49:71:80:13:1E*

**Authority Info Access**  
*http://ca.ivsign.com/certs/ivsignrootca.crt*  
*http://ocsp.ivsign.com*  
*http://ocsp2.ivsign.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: https://policy.ivsign.com*  
*CPS text: [IvSign Global CA. Certification Practice Statements and Certificate Policies:  
https://policy.ivnosys.com]*

**CRL Distribution Points**  
*http://crl1.ivsign.com/ivsignroot.crl*  
*http://crl2.ivsign.com/ivsignroot.crl*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *D6:EA:13:D3:B7:70:57:17:E3:AD:56:07:3B:1A:9D:DE:00:57:97:60:3B:9A:A7:3A:71:04:48:E9:62:  
F5:41:C5*

**X509SubjectName**

**Subject CN:** *IvSign Global CA*

**Subject O:** *IVNOSYS SOLUCIONES S.L.U.*

**Subject 2.5.4.97:** *VATES-B98333362*

Subject OU: TRUST SERVICES

Subject ST: VALENCIA

Subject C: ES

## X509SKI

X509 SK I 6mFaLpsfvPgpDPrE3pLHTu4xMjM=

Service Status <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.

[es] undefined.

Status Starting Time 2023-07-04T00:00:00Z

### 30.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 30.2.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 30.2.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [en] undefined.

[es] undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3

##### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3

##### Policy Identifier:

Identifier [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.2.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.12.3.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.1.3

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.1.3

**Description****30.2.4 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados Cualificados emitidos por IvSign Global CA*

**Name** [en] *Qualified Certificates issued by IvSign Global CA*

Service digital identities**X509SubjectName**

Subject CN: *IvSign Global CA*

Subject O: *IVNOSYS SOLUCIONES S.L.U.*

Subject 2.5.4.97: *VATES-B98333362*

Subject OU: *TRUST SERVICES*

Subject ST: *VALENCIA*

Subject C: *ES*

**X509SKI**

**X509 SK I** *6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2022-11-17T00:00:00Z*

30.2.4.1 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

30.2.4.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

30.2.4.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3*

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3.1

**Policy Identifier:**

**Identifier** [ OIDsURN ] urn:oid:1.3.6.1.4.1.47304.3.16.1.5.2.3.1

**Description**

**30.2.5 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [ es ] *Certificados Cualificados emitidos por IvSign Global CA*

**Name** [ en ] *Qualified Certificates issued by IvSign Global CA*

**Service digital identities**

**X509SubjectName**

**Subject CN:** *IvSign Global CA*



**Subject O:** *IVNOSYS SOLUCIONES S.L.U.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject OU:** *TRUST SERVICES*

**Subject ST:** *VALENCIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *6mFaLpsfvPgpDPrE3pLHTu4xMjM=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2021-03-17T01:00:00Z*

**30.2.5.4 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**30.2.5.5 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**30.2.5.6 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[ en ]* *undefined.*

*[ es ]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.3.16.1.4.2.3*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.47304.3.16.6.4.2.3*

**Policy Identifier:**

<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.6.2.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.1.1.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.1.2.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.1.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.2.3
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.47304.3.16.1.3.3.3
<b>Description</b>		

### 30.3 - Service (granted): Qualified electronic registered delivery service "SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS"

<b>Service Type Identifier</b>		<a href="http://uri.etsi.org/TrstSvc/Svctype/EDS/Q">http://uri.etsi.org/TrstSvc/Svctype/EDS/Q</a>
<b>Service type description</b>	[ en ]	An electronic delivery service providing qualified electronic deliveries.
	[ es ]	Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.
<b>Service Name</b>		
<b>Name</b>	[ en ]	Qualified electronic registered delivery service "SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS"
<b>Name</b>	[ es ]	Servicio cualificado de entrega electrónica certificada "SERVICIOS ELECTRONICOS DE CONFIANZA – IVNOSYS"

#### Service digital identities

#### Certificate fields details

<b>Version:</b>	3
<b>Serial Number:</b>	1201545153274936677250



**Public Key:**

30820122300D06092A864886F70D010105000382010F003082010A0282010100B2979840EBAA627B0CBBAF77FD5D18A74C4C8EDF75B9F6008676A4012ECE6C99802E  
 E4148036FB991C4F63F22223F3A875F82B31B66F32AC084A39510A1B4D850C5FDC095AE3066584A02617FC2DA2C85C37835AF198C24CF39ED30A93DADBD1C9F  
 17D59CA802DCFB2CDD158B068032C808BA0F2A2ED66191E59127C69F1BE08430A7A86A11664B87B340B92E38EDD6E88A5092D9FEC4908B109483E044C698  
 E502207BC0FC7AA84706873DFDA8B10D36BA7097AA0BC11B09BD2C9ED266F2B15F92C6EB180B1808B1B93DADAD2FF3E16F65412651A5AE42064028B07656A6B4E  
 2686C51FA929FCF415C4656A79C2E42F784E3E74C97AE1095CA67C90203010001

**Basic Constraints***IsCA: false***Extended Key Usage***id\_kp\_clientAuth***Subject Key Identifier***AD:A9:06:A9:AA:80:F5:47:5B:2B:95:6D:4B:71:07:4F:6D:63:1F:91***Authority Info Access***http://www.camerfirma.com/certs/ac\_camerfirma\_legal\_persons-2016.crt**http://ocsp.camerfirma.com***Authority Key Identifier***C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42***CRL Distribution Points***http://crl.camerfirma.com/ac\_camerfirma\_legal\_persons-2016.crl**http://crl1.camerfirma.com/ac\_camerfirma\_legal\_persons-2016.crl***Subject Alternative Name***administracion@ivnosys.com**OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO***Issuer Alternative Name***ca@camerfirma.com***Certificate Policies***Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2**CPS pointer: https://policy.camerfirma.com**CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en https://policy.camerfirma.com]**Policy OID: 0.4.0.194112.1.1***QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15***Key Usage:***digitalSignature - nonRepudiation - keyEncipherment***Thumbprint algorithm:***SHA-256***Thumbprint:***DB:9B:AF:22:84:63:BA:F4:AD:C8:3D:6A:AA:2E:88:69:2A:AD:0C:D3:A4:B6:C3:CD:27:00:1B:5A:86:AE:DD:AA***X509SubjectName****Subject C:***ES***Subject O:***IVNOSYS SOLUCIONES S.L.U.***Subject OU:***GERENCIA***Subject OU:***DIRECCION IT***Subject 2.5.4.97:***VATES-B98333362*



**Issuer O:** *IVNOSYS SOLUCIONES S.L.U.*

**Issuer 2.5.4.97:** *VATES-B98333362*

**Issuer OU:** *TRUST SERVICES*

**Issuer ST:** *VALENCIA*

**Issuer C:** *ES*

**Subject C:** *ES*

**Subject O:** *IVNOSYS SOLUCIONES S.L.U.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject CN:** *IvSign Qualified TSA 2021*

**Valid from:** *Wed Mar 10 11:06:18 CET 2021*

**Valid to:** *Sun Mar 09 11:06:17 CET 2025*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100B2E985729387800D1FABDB1188A8198E4D6DC6879A6DC8D37E89DEF05104090ADD25C9BA7E3E219B674B88D87B1C828C47FB7722D1808BA1EA66BC81C87992D5528C7039AA86AA8B542CDD114543CC187E88BC16483DF857872DF8662DAE8B0175331F7A5FAB6B33232B3CD6B5A5D275E69F9FAEA1E9DDAA4084D0BBDF30B9AC3B42A625855BFF1910F8D5F426AED1E338B55E6C70D3F17E70C42D41CCEAC4E925F30752B0414B4C5411D0C2C0E25ADF1ECB61B8687A6725F99EC08F36AD6990AA950C6C3CB50F4DAB600499AECCEFFB65B03646697F10CFB1D2F2D5B521F23D01935BF5CF8A057B6092840EF895C266743901AD3FCF3326C13034F615A3E1EA409CC70203010001

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *EA:61:5A:2E:9B:1F:BC:F8:29:0C:FA:C4:DE:92:C7:4E:EE:31:32:33*

**Authority Info Access** *http://ca.ivsign.com/certs/ivsignglobalca.crt*  
*http://ocsp.ivsign.com*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.47304.3.16.6.8.4*  
*CPS pointer: https://policy.ivnosys.com*  
*CPS text: [Certificado cualificado de sello electrónico de TSA. Consulte las condiciones de uso en https://policy.ivnosys.com]*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**CRL Distribution Points** *http://crl1.ivsign.com/ivsignglobal.crl*  
*http://crl2.ivsign.com/ivsignglobal.crl*

**Subject Key Identifier** *FF:DA:12:CA:D5:64:1C:9C:3C:50:76:99:EC:3E:6E:E8:5A:4A:FC:18*

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A5:C2:AA:07:A1:59:F4:ED:C9:F5:67:EC:5D:01:BC:D1:46:91:52:30:58:9E:4B:B7:E4:41:08:DA:93:B3:2E:AF*

### **X509SubjectName**

**Subject C:** *ES*

**Subject O:** *IVNOSYS SOLUCIONES S.L.U.*

**Subject 2.5.4.97:** *VATES-B98333362*

**Subject CN:** *IvSign Qualified TSA 2021*

### **X509SKI**

**X509 SK I** */9oSytVkHJw8UHaZ7D5u6FpK/Bg=*

### **Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2021-10-26T01:00:00Z*

**31 - TSP: Logalty Prueba por Interposición, S.L.****TSP Name**

**Name** [ en ] *Logalty Prueba por Interposición, S.L.*

**Name** [ es ] *LOGALTY SERVICIOS DE TERCERO DE CONFIANZA, S.L*

**TSP Trade Name**

**Name** [ en ] *Logalty Servicios de Tercero de Confianza SL*

**Name** [ es ] *Logalty Servicios de Tercero de Confianza SL*

**Name** [ en ] *VATES-B84492891*

**Name** [ es ] *VATES-B84492891*

**Name** [ en ] *Logalty Prueba por Interposicion SL*

**Name** [ es ] *Logalty Prueba por Interposicion SL*

**PostalAddress**

**Street Address** [ en ] *Calle Valportillo Primera, 22, 1ª planta modulo 7 y 8*

**Locality** [ en ] *Alcobendas*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28108*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info.ca@logalty.com*

**URI** [ en ] *https://www.logalty.com/en/*

**URI** [ es ] *https://www.logalty.com*

**TSP Information URI**

**URI** [ en ] *https://www.logalty.com/en/*

**URI** [ es ] *https://www.logalty.com/*





**Subject C:** ES

**Subject ST:** Madrid

**Subject L:** Alcobendas

**Subject O:** Logalty Servicios de Tercero de Confianza SL

**Subject 2.5.4.97:** VATES-B84492891

**Subject OU:** Logalty Trust Services

**Subject CN:** Logalty Qualified CA G2

**Valid from:** Wed Jun 06 13:08:49 CEST 2018

**Valid to:** Fri Jun 06 13:08:49 CEST 2031

**Public Key:**

```
3082:02:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:05:00:03:82:02:0F:00:30:82:02:0A:02:82:02:01:00:D1:51:75:BF:DB:1F:FC:53:26:34:7D:BB:C9:72:8B:8F:BC:B4:28:D8:C3:9C:8C:06:0E:0C:5E:77:BB:4E:FA:5D:9E:1
B:39:A:D2:1E:5D:05:E7:E4:E1:33:CA:AB:BA:CB:35:82:29:6C:B4:45:20:A8:2F:CA:53:B4:1F:8C:81:95:96:89:9A:4E:27:5B:AD:72:E9:C7:7B:96:30:CD:20:58:33:AE:7E:49:06:DD:D9:8B:82:CE:C7:CB:BF:26:2E:BA:37:E5
8A:26:17:5F:A7:B0:7B:1B:87:6E:67:86:98:DE:76:C5:11:84:92:E6:47:F2:05:19:A1:EC:FC:2A:C1:FA:5C:D9:35:E8:AB:2E:4E:61:F9:5D:77:6F:77:CD:DF:9B:B7:6C:56:F0:A3:27:A2:F0:D8:15:DA:B8:D1:36:60:10:D9:53:50:4
B:45:9E:0F:D3:73:DD:AC:D8:EA:D8:0A:4D:C5:EB:7C:B5:F1:10:34:69:08:85:5C:87:C0:FD:21:07:AC:55:2B:50:79:3F:B9:23:47:47:A6:9D:66:9E:FC:C5:F4:1A:88:F2:F2:F1:E1:9B:09:BD:EA:B9:27:F1:C6:60:EE:4A:1B:
CD:0D:76:CA:02:81:2D:69:66:26:E5:05:AB:EB:AD:9E:92:29:F9:92:94:44:88:85:4E:A2:23:2D:78:13:74:0E:59:F7:3F:D9:22:7B:77:40:84:28:4D:F5:E6:E0:00:AB:59:72:67:99:13:30:25:46:7E:FE:AD:D7:64:91:17:58:18:01:7E
3F:3E:F5:32:18:7B:B6:0D:CD:51:75:EA:DC:3E:0C:B9:19:B3:2B:D7:84:AB:F2:89:C8:E1:A9:D6:17:04:4C:E3:86:95:51:62:5D:67:26:FD:2C:88:FE:57:E4:C9:FC:15:4B:00:AB:87:D8:AC:26:18:50:3D:CF:79:E1:95:22:C0:A5:
64:F1:82:78:9C:FE:37:DA:0D:41:3D:E2:C8:5F:64:30:73:5F:59:26:50:2D:52:A7:FE:F6:23:3A:58:B1:5C:32:01:53:07:AE:A4:AS:5D:0F:18:98:CF:F2:6C:44:39:AD:17:AB:3C:BC:F0:4C:FE:72:CC:49:FD:31:67:35:88:54:51:3B
F7:75:E9:2F:E9:C6:EA:09:33:18:77:E1:BC:87:7E:F3:3D:54:BC:9A:F4:53:1A:06:34:5B:EA:81:A3:3E:4D:AF:10:B4:21:1D:B1:62:F0:02:23:24:3B:DE:18:32:80:8D:EE:A3:40:2A:C4:17:2E:AE:8C:3C:D0:66:C3:24:8A:6F:97:
33:D6:D2:F7:88:93:9A:45:72:F5:E7:B1:84:98:1F:B4:1E:C9:76:EB:B1:02:03:01:00:01
```

**Basic Constraints** IsCA: true - Path length: 0

**Authority Key Identifier** 7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82

**Authority Info Access** <https://www.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt>  
<http://ocsp1.logalty.es>; <http://ocsp2.logalty.es>

**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS pointer: <https://www.logalty.es/PKI/documentacion/>

**CRL Distribution Points** <http://crl1.logalty.es/logaltyCARoot03.crl>  
<http://crl2.logalty.es/logaltyCARoot03.crl>

**Subject Key Identifier** 26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

**Key Usage:** keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 05:95:C5:69:7A:6A:90:AE:41:15:6F:BF:8A:79:52:40:F9:54:B6:4D:77:61:8A:AC:81:2A:55:62:3E:9  
 A:13:6F

#### Certificate fields details

**Version:** 3

**Serial Number:** 2682646734725033920



**Authority Key Identifier** *7B:31:4D:AA:C0:A8:8E:2B:E3:ED:AD:88:14:08:49:8C:C6:AA:2E:82*

**Authority Info Access** *http://crt.logalty.es/certificateauthority/LogaltyCAROOT03.cacert.crt*  
*http://ocsp1.logalty.es*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: https://www.logalty.es/PKI/documentacion/*

**CRL Distribution Points** *http://crl1.logalty.es/logaltyCARoot03.crl*  
*http://crl2.logalty.es/logaltyCARoot03.crl*

**Subject Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *C0:70:69:EB:4A:AE:CF:16:0B:7D:EC:65:52:69:5F:28:8F:8D:75:2B:DA:C9:2B:E2:0B:C6:C1:C3:F6:C5:7A:C8*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified CA G2*

**X509SKI**

**X509 SK I** *Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2024-01-24T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

URI [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 31.1.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 31.1.2 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 31.1.3 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

### 31.1.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

#### Criteria list assert=atLeastOne

##### Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.1.1
------------	-------------	---------------------------------

##### Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.3.1
------------	-------------	---------------------------------

##### Description

### 31.1.5 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

#### Service Name

Name	[ es ]	Certificados cualificados emitidos por Logalty Qualified CA G2
------	--------	--

**Name** *[ en ]* *Qualified Certificates issued by Logalty Qualified CA G2*

**Service digital identities**

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified CA G2*

**X509SKI**

**X509 SK I** *Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2019-10-28T01:00:00Z*

**31.1.5.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**31.1.5.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**31.1.5.3 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**31.1.5.4 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

<b>Qualifier type description</b>	[en]	undefined.
	[es]	undefined.

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.1.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.2.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.6.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.7.1

**Policy Identifier:**

**Identifier** [OIDAsURN] urn:oid:1.3.6.1.4.1.30210.1.3.1

**Description****31.1.6 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service Name**

**Name** [es] *Certificados cualificados emitidos por Logalty Qualified CA G2*

**Name** [en] *Qualified Certificates issued by Logalty Qualified CA G2*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject ST:** Madrid

**Subject L:** Alcobendas

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified CA G2*

**X509SKI**

**X509 SK I** *Jkk+pa/3ZUk6lChXW+EbOKNS4mw=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time** *2018-11-28T01:00:00Z*

**31.1.6.5 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**31.1.6.6 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**31.1.6.7 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**31.1.6.8 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en]* *undefined.*

*[es]* *undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.30210.1.1.1*

**Policy Identifier:**



<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.2.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.6.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.7.1
<b>Policy Identifier:</b>		
<b>Identifier</b>	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.30210.1.3.1
<b>Description</b>		

## 31.2 - Service (withdrawn): Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005

### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

<b>Service type description</b>	[en]	A time-stamping generation service creating and signing qualified time-stamps tokens.
	[es]	Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

### Service Name

<b>Name</b>	[es]	Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005
<b>Name</b>	[en]	Qualified timestamps issued by Logalty Qualified TSA TSU005

### Service digital identities

#### Certificate fields details

<b>Version:</b>	3
<b>Serial Number:</b>	2600299901454462975



**Subject Key Identifier** *E2:43:C3:51:53:46:A0:32:47:35:3C:30:9C:3D:2B:3F:69:D5:A7:9E*

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.1*  
*Policy OID: 1.3.6.1.4.1.30210.1.5.1*  
*CPS pointer: https://www.logalty.es/certificateauthority/CPS*  
*CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*

**CRL Distribution Points**  
*http://cr1.logalty.es/qualifiedLogaltySubCA02.crl*  
*http://cr2.logalty.es/qualifiedLogaltySubCA02.crl*

**Extended Key Usage** *id\_kp\_timeStamping*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *8D:6F:1A:8B:DC:60:5B:88:10:DC:3F:F5:C0:A3:7C:A8:4A:ED:E7:13:DF:9D:87:82:E0:F7:3F:80:8D:82:F0:BA*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU005*

**X509SKI**

**X509 SK I** *4kPDUVNGoDJHNTwwnD0rP2nVp54=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2023-12-21T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[ en ]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[ es ]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 31.2.1 - History instance n.1 - Status: granted

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

#### Service Name

**Name** *[ es ]* *Sellos de tiempo cualificados emitidos por Logalty Qualified TSA TSU005*

**Name** *[ en ]* *Qualified timestamps issued by Logalty Qualified TSA TSU005*

#### Service digital identities

##### X509SubjectName

**Subject C:** *ES*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU005*

##### X509SKI

**X509 SK I** *4kPDUVNGoDJHNTwwnD0rP2nVp54=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2018-11-28T01:00:00Z*

### 31.3 - Service (withdrawn): Servicio cualificado de entrega electrónica certificada

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

**Service type description** *[ en ]* *An electronic delivery service providing qualified electronic deliveries.*

*[ es ]* *Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

#### Service Name

**Name** *[ es ]* *Servicio cualificado de entrega electrónica certificada*



**Subject CN:** *Sello de entrega electrónica certificada cualificada de Logalty*

**Valid from:** *Wed Sep 12 11:08:48 CEST 2018*

**Valid to:** *Sat Sep 11 11:08:48 CEST 2021*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A028201010095FF377B7E2CD970D910EA BDAAD1B2E06F0E7FD78747EDF0CC35D96D9FA4E4D59E85  
AD45AD61B4F1831E06B6A9E5E636AD9F9A872E058A560D09FA1205763940896D931E84762ADB C15F4A47C2BC08F98733AC371A3F1C41EF8A87EEEC6471B03240C8  
C23422D02235F6BFCD8D9E07EB5D8C43275ADFB5F5C3ACD08F1A6A353CFE5D17526DA9801D96FA3DA A9C55008958F0C27801E1AE EB998ACD0B0E7E33F3372  
9E916A8597339875D20DC4F7D825584136AE DA6D19B99576CB70D3E6CB0C9E66CA11E36DB6B0AD F22504CEA21FBCFE B64EE5779D22C199B22DA9E8027FC93F2AA  
4C4325B9DA8727D72A157B7084682D247AA AA570691A25777E0782F8F0203010001

**Authority Info Access** *https://www.logalty.es/certificateauthority/LogaltyQualifiedCAG1.cacert.crt*  
*http://ocsp1.logalty.es*

**Subject Key Identifier** *86:D4:F8:CF:75:9C:01:89:F8:FA:58:DE:8B:38:3C:05:D0:C1:EC:8B*

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.30210.1.3.3*  
*CPS pointer: https://www.logalty.es/PKI/documentacion/*  
*CPS text: [Certificado cualificado de sello electrónico avanzado de persona jurídica]*  
*Policy OID: 0.4.0.194112.1.1*

**CRL Distribution Points** *http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*  
*http://crl2.logalty.es/qualifiedLogaltySubCA02.crl*

**Extended Key Usage** *id\_kp\_clientAuth*

**Subject Alternative Name** *info.ca@logalty.com*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *92:B6:E3:71:3C:78:86:89:D6:52:E7:59:83:6C:D9:6E:75:85:BF:B5:A1:CC:DE:22:D7:F2:1E:80:A3:  
4E:88:01*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject SERIAL NUMBER:** *B84492891*

**Subject CN:** *Sello de entrega electrónica certificada cualificada de Logalty*

**X509SKI**

**X509 SK I** *htT4z3WcAYn4+ljeizg8BdDB7Is=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-04-22T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**31.3.1 - History instance n.1 - Status: granted**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

**Service Name**

**Name** *[es] Servicio cualificado de entrega electrónica certificada*

**Name** *[en] Qualified electronic registered delivery service*

**Service digital identities****X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Servicios de Tercero de Confianza SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject SERIAL NUMBER:** *B84492891*





**Issuer ST:** *Madrid*

**Issuer L:** *Alcobendas*

**Issuer O:** *Logalty Servicios de Tercero de Confianza SL*

**Issuer 2.5.4.97:** *VATES-B84492891*

**Issuer OU:** *Logalty Trust Services*

**Issuer CN:** *Logalty Qualified CA G2*

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Prueba por Interposicion SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU006*

**Valid from:** *Thu Dec 10 14:56:31 CET 2020*

**Valid to:** *Tue Dec 09 14:56:31 CET 2025*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100938210403CD689D1B50C234CB1786452BC2C9928F1CE0EC6EA4CA4622C8BA9B84A7FB315351B780E4588E97D9A8F43283E6090C4E22BF0E301C66D424E268A32CE8FC74E1AC4A5E59B3DA33752066B38376F8490BD4524C3E03853C7B7C5CFE2672D6C9C630FA1B467E084E65E0674622A4B71BDAE3ED0EBD26FFA842476080168730E60FF7E9BDB944AF2433813D91DE84420BE90405ABDAD1B530671A185FB12548D7454368400DC34A705C13586F8296E01BF3DAD964E966EB5DF6507E1379288CBDB7E7F592697B4B905E0F40343A1451B03AB6A0103287D6E582CBBAF98CBA0FB95625F8E4024D5BF4AB745C1707160DC9A9A0010F854F8A3359A812747462CBDB84FC9854CD4BDD176DE872881169C0D4E74C91A6C0B85D975989D03C5F4D4FD92D5EA4028B368DF3528A7B068B1368C304D11534DE9EBD1C4A0DBE0CD84F3C0395244C63AA033FA0252F4168FCE183F0BF910428DBE797442A301297B7ED83FE007E6099F660A6AC9DA3E44B673EC8D35B385E548A56CDS3E0238FD2552FC8E9B3A8B9D0027B9870986283E8F877A5D5F139BC5633B73A7D3DC4F4AA0BD0A5FA776CF910A53E3BAA06F5641609FCEA17284BA69882457CF58364FC5FCE5539856EDCCD2483D44E18027014A8E8A44767CF80FAE9A4F4EA5ED6FC9834DC3842FD0EE44E857056EB84D709DF9DFB8A3A77D7068FB8AE537FA150203010001

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**Authority Info Access**  
<http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>  
<http://ocsp1.logalty.es>

**Certificate Policies**  
 Policy OID: *0.4.0.194112.1.1*  
 Policy OID: *1.3.6.1.4.1.30210.1.5.1*  
 CPS text: *[Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
 CPS pointer: <https://www.logalty.com/certificateauthority/>

**Extended Key Usage**  
*id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
<http://cr11.logalty.es/qualifiedLogaltySubCA02.crl>  
<http://cr12.logalty.es/qualifiedLogaltySubCA02.crl>

**Subject Key Identifier**  
 86:38:96:DC:F8:77:04:90:71:1F:15:2D:81:0F:FD:B3:2D:47:A6:7E

**Key Usage:**  
 digitalSignature

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 D0:0B:B9:7B:7A:BA:BF:95:F5:78:A8:63:95:BA:8B:01:6B:C1:79:8C:57:40:08:12:D7:31:17:97:A0:A2:C1:C2

**X509SubjectName**

**Subject C:**  
 ES

**Subject ST:**  
 Madrid

**Subject L:**  
 Alcobendas

**Subject O:**  
 Logalty Prueba por Interposicion SL

**Subject 2.5.4.97:**  
 VATES-B84492891

**Subject OU:**  
 Logalty Trust Services

**Subject CN:**  
 Logalty Qualified TSA TSU006

**X509SKI**

**X509 SK I**  
 hjiW3Ph3BJBxHxUtgQ/9sy1Hpn4=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2021-03-17T01:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 31.5 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU007



**Subject ST:** Madrid

**Subject L:** Alcobendas

**Subject O:** Logalty Prueba por Interposicion SL

**Subject 2.5.4.97:** VATES-B84492891

**Subject OU:** Logalty Trust Services

**Subject CN:** Logalty Qualified TSA TSU007

**Valid from:** Wed Apr 07 15:22:02 CEST 2021

**Valid to:** Mon Apr 06 15:22:02 CEST 2026

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C6C76F6A1DB6F0C0DBBDFC83C458B7E9600E4660AC7B7EA38FF0CDE090987859B991B  
306F9F901B836621D201D49E6B13223A8D955032F8E319229343CE01E9F56A1D216C48602DB0EFC3B3A33B4488A3D2C9F2D2B32698AE18F6618A94F8746347A  
0DB31F33BAC4520A965644B7BE1A7937AFA630CA194872DB68B7D0F0F00251A70B88066E1402B0C95FC500DDE4D9B9AB450A430818B6834F7E3C5ED7DD61B0  
9B894F1B04575DD0D6816E6E21985761B55E1D7FD6940BEBDE500F160A76CA82278057255DB3D8344A3110302A9B2623BA926030EAF3031328ACEAA46910F6484A  
A8ADE44F9930B1EB1463463112C2F89AC8C142A15EAD4E11B9256E8625E1FC79F9CF2FA342B6A963C161F49030F8CDEA3D4735A3CDE8338B1B704E8FC641986  
F63504A64712253FBC78E176767551F48F4FF3E7E7D48B7A41EF2A56CD43408AFC8D8EB6C65EC55D511C4A6AA9203460B335281F5F46A70556C8384CE22AC2F1E30B  
909220AB13AC26F1A5C8885DEA2BA97FF5CF8EA6C88C392CC9F56849C6E9ED82042A1155A73C2839DC2DAD9E9ABF0A113E55BE78ED976C68F4446129166930F00  
319439592B0EF1689F9AC95DF4C933C23722372F7869A3D8F37A88361F70501E71ED48E8EF245ACEA4D82CFE589D553BE81133A89F1A2754BE25FA82AFD7AC7084  
D171AE5EEF4A6DCFEFE1079131E86501513DAF70203010001

**Authority Key Identifier** 26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

**Authority Info Access**  
<http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>  
<http://ocsp1.logalty.es>

**Certificate Policies**  
Policy OID: 0.4.0.194112.1.1  
Policy OID: 1.3.6.1.4.1.30210.1.5.1  
CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]  
CPS pointer: <https://www.logalty.com/certificateauthority/>

**Extended Key Usage** id\_kp\_timeStamping

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15

**CRL Distribution Points**  
<http://crl1.logalty.es/qualifiedLogaltySubCA02.crl>  
<http://crl2.logalty.es/qualifiedLogaltySubCA02.crl>

**Subject Key Identifier** 85:4E:F9:3D:FA:10:11:A0:B9:02:96:B5:90:B4:24:BA:B1:37:E2:92

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 41:06:46:45:E1:06:1E:A5:87:8B:12:43:EA:82:B2:C1:1C:11:71:B7:F4:CC:F3:01:E3:6C:88:B5:8D:D  
F:A8:A6

**X509SubjectName**

Subject C: ES

Subject ST: Madrid

Subject L: Alcobendas

Subject O: Logalty Prueba por Interposicion SL

Subject 2.5.4.97: VATES-B84492891

Subject OU: Logalty Trust Services

Subject CN: Logalty Qualified TSA TSU007

**X509SKI**

X509 SK I hU75PfoQEaC5Apa1kLQkurE34pI=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

Service status description [en] undefined.  
[es] undefined.

**Status Starting Time**

2021-07-01T01:00:00Z

**Scheme Service Definition URI**

URI [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 31.6 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU008

**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

Service type description [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

Name [es] Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU008

Name [en] Qualified timestamps issued by Logalty Qualified TSA TSU008

**Service digital identities****Certificate fields details**



**Valid to:** *Mon Apr 06 15:28:37 CEST 2026*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100EA5D1A636789B20C55C902B1AB735D528909446E7F51B16C4C67FF5E90F4B457F622424C8F9EFD045262819074B1579A4ED8137315A7CEE1D5296629ED855E255F27D7E582E4CF1C0F208F13A9EA1F154C6027867FA778033410AFESA8CFC9984050049103944001CF868BA46BCA070EB7A0FE8AD85B905126A9C4A6B371E4BB31C27576D0BAAB62F2541F7A6A2DF4C3508BB823436BBF12783F1EA795C22047D0D31965D23F85EAE6DDDA366CB70D8FEFC145A8D7A306970DD21884D28DC44B4E0C616E61F5CF353D26AE904B91B32F2D355A021507A56499FEDEFCA1AE13E2EAA0F3D51F4381845930F310AE07EF2D248703888DCCDBD1E35A637F8B8BA66251D7A977430E5E7A809FC076D8301F0D7794D995E4B09E968AFB17E5DFC57D3CB243A8DCFC5C304B6F2E5F153285D7B12D44D03D0F43BF9809554AFDEED789AAD852E826DE409A75021D61AE22F3ACC8B1858AD2C91B73889AE74FE17CF511ED63DB7F05C1DES5D8270BC5CEDFFE9C21D33C416FE8E6208F223C72C78F9F39ADAC7C8E943D5199E3BF8A6B468ABB0BF7A7C4C202E8207EC705E61A54511B89C16A47C87DCB79C77344534A495F75ADBFEECE2AFBA733545CE9AA1F45DDEE8214DF31689D03E2C09CED9E77A9A9B32E83C23C15775B0980673855D011AA8E8D87959B8D7756678991B48ABC13C6A59A8222B5015F52F68B75680025BF450203010001

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**Authority Info Access**  
<http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>  
<http://ocsp1.logalty.es>

**Certificate Policies**  
Policy OID: *0.4.0.194112.1.1*  
Policy OID: *1.3.6.1.4.1.30210.1.5.1*  
CPS text: *[Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
CPS pointer: <https://www.logalty.com/certificateauthority/>

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
<http://crl1.logalty.es/qualifiedLogaltySubCA02.crl>  
<http://crl2.logalty.es/qualifiedLogaltySubCA02.crl>

**Subject Key Identifier** *E1:CD:3E:71:4A:33:7C:38:40:14:3A:C3:B4:0D:D6:B6:D4:D3:97:20*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *89:DD:A8:76:2B:40:6C:5F:63:97:26:B8:43:7B:23:5B:1F:B9:67:2E:DC:70:C6:EA:65:90:8D:83:12:B8:15:34*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Prueba por Interposicion SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU008*

**X509SKI**

**X509 SK I** *4c0+cUozfDhAFDrDtA3WttTtlyA=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2021-07-01T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**31.7 - Service (granted): Qualified electronic registered delivery service issued for “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”**

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

**Service type description** *[en] An electronic delivery service providing qualified electronic deliveries.*  
*[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

**Service Name**

**Name** *[en] Qualified electronic registered delivery service issued for “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”*

**Name** *[es] Servicio Cualificado de entrega electrónica certificada emitido para “Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada”*

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 3338844724482481780





**Authority Key Identifier** 26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C

**Authority Info Access** <http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt>  
<http://ocsp1.logalty.es>

**Certificate Policies** Policy OID: 1.3.6.1.4.1.30210.1.3.1  
CPS text: [Certificado cualificado de sello electrónico cualificado de persona jurídica con gestión de datos de creación de sello electrónico en nombre del creador de sellos]  
CPS pointer: <https://www.logalty.com/certificateauthority/>  
Policy OID: 0.4.0.194112.1.3

**Extended Key Usage** id\_kp\_clientAuth

**QCStatements - crit. = false** id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15  
id\_etsi\_qcs\_QcSSCD

**CRL Distribution Points** <http://crl1.logalty.es/qualifiedLogaltySubCA02.crl>  
<http://crl2.logalty.es/qualifiedLogaltySubCA02.crl>

**Subject Key Identifier** 85:98:6D:93:D1:AF:61:4E:D0:A2:F3:1A:E8:6A:F9:EE:E2:4F:59:92

**Key Usage:** digitalSignature - nonRepudiation - keyEncipherment

**Thumbprint algorithm:** SHA-256

**Thumbprint:** D9:8A:8D:C3:43:F2:C5:3B:2D:D2:26:9A:25:22:41:4C:E1:42:93:C7:2B:EF:35:B5:FD:6D:5F:0A:7F:FA:23:A2

**X509SubjectName**

**Subject C:** ES

**Subject L:** Alcobendas

**Subject O:** Logalty Prueba por Interposicion SL

**Subject 2.5.4.97:** VATES-B84492891

**Subject SERIAL NUMBER:** B84492891

**Subject CN:** Logalty Prueba por Interposicion SL - Entrega Electronica Cualificada

**X509SKI**

**X509 SK I** hZhtk9GvYU7QovMa6Gr57uJPWZI=

**Service Status**

**Service status description** [en] undefined.



**Issuer L:** *Alcobendas*

**Issuer O:** *Logalty Servicios de Tercero de Confianza SL*

**Issuer 2.5.4.97:** *VATES-B84492891*

**Issuer OU:** *Logalty Trust Services*

**Issuer CN:** *Logalty Qualified CA G2*

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Prueba por Interposicion SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU009*

**Valid from:** *Thu Nov 25 13:01:06 CET 2021*

**Valid to:** *Tue Nov 24 13:01:06 CET 2026*

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:SD:74:83:95:CB:FF:92:AB:62:01:01:45:D1:39:06:35:32:59:CF:8B:BD:6B:16:B1:5A:87:78:98:E1:03:9E:10:E3:40:A2:05:30:C0:10:02:D  
D:74:C7:8E:F4:4C:55:C6:F1:68:3C:DC:2C:70:E6:0D:06:D3:1A:43:F1:0B:22:01

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**Authority Info Access**  
*http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt*  
*http://ocsp1.logalty.es*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.1*  
*Policy OID: 1.3.6.1.4.1.30210.1.5.1*  
*CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
*CPS pointer: https://www.logalty.com/certificateauthority/*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
*http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*  
*http://crl2.logalty.es/qualifiedLogaltySubCA02.crl*

**Subject Key Identifier** *C4:D2:E7:3B:AC:D0:86:E5:6C:B9:9B:BE:A2:5A:B0:15:05:21:74:F5*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *0D:AE:9C:B8:7F:52:B6:CD:A7:A7:84:73:03:97:46:6A:E5:54:72:79:BB:9D:B9:BE:70:97:C2:90:9D:B6:99:8A*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Prueba por Interposicion SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU009*

**X509SKI**

**X509 SK I** *xNLnO6zQhuVsuZu+olqwFQUhdPU=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-04-22T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

### **31.9 - Service (granted): Sellos electrónicos cualificados de tiempo emitidos por Logalty Qualified TSA TSU010**

**Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*

*[es] Un servicio de generación de sellado de tiempo para crear y firmar tokens tiempo sellos cualificados.*



**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU010*

**Valid from:** *Thu Nov 25 13:07:07 CET 2021*

**Valid to:** *Tue Nov 24 13:07:07 CET 2026*

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:09:DE:3A:45:14:EF:B2:81:A0:47:83:A4:DE:5B:73:A4:0B:25:BA:86:88:7B:CF:61:DA:D8:C6:A8:E3:F5:F0:B9:78:57:60:8C:CB:4D:92:7F:61:50:38:EA:10:0C:25:DF:7E:19:D6:DE:7F:3E:DD:53:68:95:27:00:D0:E9:F1:14

**Authority Key Identifier** *26:49:3E:A5:AF:F7:65:49:3A:94:28:57:5B:E1:1B:38:A3:52:E2:6C*

**Authority Info Access**  
*http://crt.logalty.es/certificateauthority/LogaltyQualifiedCAG2.crt*  
*http://ocsp1.logalty.es*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.1*  
*Policy OID: 1.3.6.1.4.1.30210.1.5.1*  
*CPS text: [Certificado cualificado de sello electrónico de persona jurídica para la expedición de sellos cualificados de tiempo electrónico]*  
*CPS pointer: https://www.logalty.com/certificateauthority/*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
*http://crl1.logalty.es/qualifiedLogaltySubCA02.crl*  
*http://crl2.logalty.es/qualifiedLogaltySubCA02.crl*

**Subject Key Identifier** *0F:5F:E7:84:74:08:2C:AD:F4:CC:9E:D2:33:79:8F:E4:57:A1:D3:39*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *F0:30:DA:FC:7B:51:C4:BF:49:2B:C5:B0:FC:67:6B:93:72:48:0E:47:7F:12:6D:34:B2:91:9F:84:09:C  
D:44:90*

**X509SubjectName**

**Subject C:** *ES*

**Subject ST:** *Madrid*

**Subject L:** *Alcobendas*

**Subject O:** *Logalty Prueba por Interposicion SL*

**Subject 2.5.4.97:** *VATES-B84492891*

**Subject OU:** *Logalty Trust Services*

**Subject CN:** *Logalty Qualified TSA TSU010*

**X509SKI**

**X509 SK I** *D1/nhHQILK30zJ7SM3mP5Feh0zk=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-04-22T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*



**32 - TSP: LLEIDANETWORKS SERVEIS TELEMATICS, S.A.****TSP Name**

**Name** [ en ] *LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*

**Name** [ es ] *LLEIDANETWORKS SERVEIS TELEMATICS, S.A.*

**TSP Trade Name**

**Name** [ en ] *LLEIDA.NET*

**Name** [ es ] *LLEIDA.NET*

**Name** [ en ] *VATES-A25345331*

**Name** [ es ] *VATES-A25345331*

**Name** [ en ] *Lleidanetworks Serveis Telemàtics, S.A*

**Name** [ es ] *Lleidanetworks Serveis Telemàtics, S.A*

**PostalAddress**

**Street Address** [ en ] *C/ Téllez, 56 Oficina C*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28007*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ Téllez, 56 Oficina C*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28007*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info@lleida.net*



**Issuer OU:** *Certificados Cualificados*

**Issuer O:** *Firmaprofesional S.A.*

**Issuer C:** *ES*

**Subject CN:** *Lleidanetworks Serveis Telemàtics, S.A.*

**Subject SERIAL NUMBER:** *A25345331*

**Subject OU:** *TECHNICAL DEPARTMENT*

**Subject 2.5.4.97:** *VATES-A25345331*

**Subject O:** *Lleidanetworks Serveis Telemàtics, S.A.*

**Subject ST:** *LLEIDA*

**Subject C:** *ES*

**Valid from:** *Mon Feb 19 13:37:00 CET 2018*

**Valid to:** *Sat Feb 18 13:37:00 CET 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D91C2266AB75508B2A6770452AF4025FBC6961636FBB2222ABDA4613A2AA013015AC  
CD0E0A9C58D8F0D47215D4B5C8E763E761E7997861CCB4A41819CB67E876280DF9B6C681B20E3F474F4DDA8953872E21B21246325902F0C9AECEAA66A0A19D2  
A187612852019AF6B2C36ED9B0ECC472A9E1DA5E76331315B7A787AA403F3D9D293B31C77958AD029B466D6C34D1DCFFD3B974BE6C8A3C14094EAD45B7B422292D  
16208FDE0875C94359DB896BFBF95DAD3F0C245A60C99D05264C8B082A4B0E0E4660D042C49CFD10ED9E991B881703714A718A1AE0FD0E84B9A232B8241293691C  
FF8878F8378C5B76D66F5033D7F2AFCE9A079F6348C47011AF0B3D0203010001

**Authority Info Access**  
<http://crl.firmaprofesional.com/cualificados.crt>  
<http://ocsp.firmaprofesional.com>

**Subject Key Identifier**  
*83:73:0A:37:EB:18:17:66:AA:E7:07:A7:7C:DC:9A:41:C4:B2:AD:46*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.13177.10.1.10.2*  
*CPS pointer: <http://www.firmaprofesional.com/cps>*  
*CPS text: [Éste es un Certificado Corporativo de Sello Empresarial cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]*  
*Policy OID: 0.4.0.194112.1.1*

**CRL Distribution Points**  
<http://crl.firmaprofesional.com/cualificados.crl>

**Extended Key Usage**  
*id\_kp\_clientAuth*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *CF:14:2F:21:78:F3:FC:04:77:E7:0A:B8:24:38:8D:8D:CB:D9:4E:1C:9D:89:20:DC:EE:BA:57:0B:7E:24:4F:7B*

**X509SubjectName**

**Subject CN:** *Lleidanetworks Serveis Telemàtics, S.A.*

**Subject SERIAL NUMBER:** *A25345331*

**Subject OU:** *TECHNICAL DEPARTMENT*

**Subject 2.5.4.97:** *VATES-A25345331*

**Subject O:** *Lleidanetworks Serveis Telemàtics, S.A.*

**Subject ST:** *LLEIDA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *g3MKN+sYF2aq5wenfNyaQcSyrUY=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-11-17T00:00:00Z*

**32.1.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

**Service Name**

**Name** *[es] Servicio cualificado de entrega electrónica certificada "Openum eIDAS"*

**Name** *[en] Qualified electronic registered delivery service "Openum eIDAS"*

**Service digital identities****X509SubjectName**

**Subject CN:** *Lleidanetworks Serveis Telemàtics, S.A.*

**Subject SERIAL NUMBER:** A25345331

**Subject OU:** TECHNICAL DEPARTMENT

**Subject 2.5.4.97:** VATES-A25345331

**Subject O:** Lleidanetworks Serveis Telemàtics, S.A.

**Subject ST:** LLEIDA

**Subject C:** ES

**X509SKI**

**X509 SK I** g3MKN+sYF2aq5wenfNyaQcSyrUY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2021-10-26T01:00:00Z

**32.1.2 - History instance n.2 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

**Service Name**

**Name** [ es ] Servicio cualificado de entrega electrónica certificada "Connectaclick"

**Name** [ en ] Qualified electronic registered delivery service "Connectaclick"

**Service digital identities****X509SubjectName**

**Subject CN:** Lleidanetworks Serveis Telemàtics, S.A.

**Subject SERIAL NUMBER:** A25345331

**Subject OU:** TECHNICAL DEPARTMENT

**Subject 2.5.4.97:** VATES-A25345331

**Subject O:** Lleidanetworks Serveis Telemàtics, S.A.

**Subject ST:** LLEIDA

**Subject C:** ES

**X509SKI**



**Issuer 2.5.4.97:** VATES-B97458996

**Issuer SERIAL NUMBER:** B97458996

**Issuer OU:** Certification Authority inDenova SL

**Issuer T:** Subordinate Certificate Authority inDenova SL

**Issuer L:** VALENCIA

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-A25345331

**Subject 2.5.4.13:** Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003

**Subject T:** Gerente

**Subject CN:** (A25345331) Lleidanetworks Serveis Telemàtics, S.A. - FRANCISCO

**Subject OU:** Gerencia

**Subject O:** Lleidanetworks Serveis Telemàtics, S.A.

**Subject GIVEN NAME:** FRANCISCO

**Subject SERIAL NUMBER:** IDCES-40897755Y

**Subject ST:** LLEIDA

**Subject L:** ALPICAT

**Subject SURNAME:** SAPENA SOLER

**Subject E:** claves@lleida.net

**Subject C:** ES

**Valid from:** Mon Oct 17 13:41:00 CEST 2022

**Valid to:** Tue Oct 17 13:51:00 CEST 2023

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100CF06795387748D116E77A50BF5B88121AD011E75373AEAD1C12DB9EDB6A450B6797E834D314D34399E72FB8B604CF7379B992848695DEE8901645D82F732D346558E71C320292703F3EESDE8790A8A2639420529016731811E01D98A43953232DC66FB1C208C6472509CF44194226F75157ADB45D572C92E77CDAS17A790EA79435AD725A170084185FBBA192FD92637003162548A83DDC38669F994712B07935AA73BACF0714A1498BE2D133E68129B20589393A45DC1F4D04DD6963CC16A851520492D34AC92C313197DF73440377B529C403F261ND099658F8C08E3EF314ND6A7F69DDC60FB4D1B85648DDF9CD806046AD5592284A6817986927260CA1E8B788307EDDA8011F52941761C8200BB514277DDA260084A283939F621426544FA76345443BE32424300AE719F38953C3D7528E18FBE8B23F29CDD661BDA68C6253EC808162C1779A76EDEF068819ADA372B5A93CA03679A0643443CFBC68604CE5C7D1BA38A7EA2F0F60FB49DD1CB27990C04FC1F98E23A98979EA4B767D78D37618FA35F01DB8383B7D12557E466DA4B2D790DB6379131E886D12BEAD8F6F342DE7251F87C316979F3A959A3753B1AD4A24A2984F00F7C41C7A2159D74D015977AD13BCA07CSDB70359B21A494FAFAF3DA2E93142E97765A0348F15F61C3A2293E831DCC431CDA44AF11ECFF3701FC31A734373ADD4FE74EEAF573F490203010001

**Basic Constraints** IsCA: false

**Extended Key Usage** Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id\_kp\_clientAuth - id\_kp\_smartcardlogon

**Subject Key Identifier** 32:D2:C8:42:B1:B4:F9:82:2E:5A:FA:B4:BA:74:17:5A:A7:E8:E0:5E

**Authority Info Access**  
<http://ocsp2.esigna.es>  
[http://certs.esigna.es/ca/indenova\\_pki\\_003.crt](http://certs.esigna.es/ca/indenova_pki_003.crt)

**Authority Key Identifier** C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46

**CRL Distribution Points**  
[http://crl1.esigna.es/sub/indenova\\_pki\\_003.crl](http://crl1.esigna.es/sub/indenova_pki_003.crl)  
[http://crl.esigna.es/sub/indenova\\_pki\\_003.crl](http://crl.esigna.es/sub/indenova_pki_003.crl)

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.1  
 CPS pointer: [http://cps.esigna.es/sub/cps\\_sub003\\_ca.pdf](http://cps.esigna.es/sub/cps_sub003_ca.pdf)  
 CPS text: [Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio. Consulte las condiciones de uso en [http://cps.esigna.es/sub/cps\\_sub003\\_ca.pdf](http://cps.esigna.es/sub/cps_sub003_ca.pdf)]  
 Policy OID: 0.4.0.194112.1.1  
 Policy OID: 2.16.724.1.3.5.6.2

**QCStatements - crit. = false**  
 id\_etsi\_qcs\_QcCompliance  
 id\_etsi\_qcs\_RetentionPeriod: 15

**Key Usage:** digitalSignature - nonRepudiation - keyEncipherment

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 07:2A:C4:A8:1C:43:E3:E5:9D:FB:7B:5B:BA:08:D2:C3:0A:67:E5:09:F6:10:2A:F5:E6:73:C3:E1:63:7B:64:E9

**X509SubjectName**

**Subject 2.5.4.97:** VATES-A25345331

**Subject 2.5.4.13:** Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003

**Subject T:** Gerente

**Subject CN:** (A25345331) Lleidanetworks Serveis Telemàtics, S.A. - FRANCISCO

**Subject OU:** Gerencia

**Subject O:** Lleidanetworks Serveis Telemàtics, S.A.

**Subject GIVEN NAME:** FRANCISCO

**Subject SERIAL NUMBER:** IDCES-40897755Y

**Subject ST:** LLEIDA

**Subject L:** ALPICAT



**Subject SURNAME:** *SAPENA SOLER*

**Subject E:** *claves@lleida.net*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *MtLIQrG0+YIuWvq0unQXWqfo4F4=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-11-17T00:00:00Z*

**33 - TSP: TrustCloud Solutions, S.L.****TSP Name**

**Name** [ en ] *TrustCloud Solutions, S.L.*

**Name** [ es ] *TrustCloud Solutions, S.L.*

**TSP Trade Name**

**Name** [ en ] *Branddocs SL*

**Name** [ es ] *Branddocs SL*

**Name** [ en ] *BRANDDOCS SL*

**Name** [ en ] *VATES-B87142618*

**Name** [ es ] *VATES-B87142618*

**Name** [ en ] *TRUSTCLOUD*

**PostalAddress**

**Street Address** [ en ] *PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*

**Locality** [ en ] *POZUELO DE ALARCON*

**State Or Province** [ en ] *MADRID*

**Postal Code** [ en ] *28223*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *PASEO CLUB DEPORTIVO NUMERO 1, EDIFICIO 15 A*

**Locality** [ es ] *POZUELO DE ALARCON*

**State Or Province** [ es ] *MADRID*

**Postal Code** [ es ] *28223*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:contact@trustcloud.tech*



**Issuer CN:** UANATACA CA1 2016

**Issuer OU:** TSP-UANATACA

**Issuer O:** UANATACA S.A.

**Issuer L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B87142618

**Subject CN:** Servicio preservación de firmas y sellos cualificados

**Subject SERIAL NUMBER:** B87142618

**Subject O:** Branddocs SL

**Subject C:** ES

**Valid from:** Thu Mar 14 20:24:00 CET 2019

**Valid to:** Sun Mar 13 20:24:00 CET 2022

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100DDFFCB97765B4E3C77D3E0805540759BA3CF35409A73B130FC1CC966B82217CB1CB6E4BADE07A494EFBA98559773BB57C0F0609434141C4B8E1941091D7E205B3C03580685C660F4B99C08E6E08B02314F1FE7E1D81C52FE80220EAE26FD0602E7B3AC2EBC415144339E9A65E0B1E68BED6941347F4AB78938E794FC24CBAD0F7E36CE4707A9C1740B520D93F22EE956068608588C705A64BCB5E3815E30EFD7A7B0A058F24EF0B137FA979040760767B7B71FCF30719FA30B1397BA1C1856F2A04EF37ACBDB8581B4A16A696E450DD89B7CBEC403C6844331C6F4AE564F3952E63737638B6CB58820C07A551AE107DE9C574E50CA616DA22E118D47423E5250D750203010001

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crl](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crl)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
CA:49:7B:9E:71:FF:22:2A:73:BF:E0:D0:41:D0:36:C9:32:C9:2F:A4

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5

**Certificate Policies**  
Policy OID: 0.4.0.194112.1.3  
Policy OID: 1.3.6.1.4.1.47286.1.9.6  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Qualified certificate for e-seal in Remote QSCD]

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage** *id\_kp\_clientAuth*

**Subject Alternative Name** *certificates@brand-docs.com*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *65:04:C5:1D:4F:9F:6B:E4:C2:6F:AD:85:03:B5:CC:6E:3D:39:E9:40:C7:0B:1F:5E:75:4D:2A:DA:BE:17:66:AC*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B87142618*

**Subject CN:** *Servicio preservación de firmas y sellos cualificados*

**Subject SERIAL NUMBER:** *B87142618*

**Subject O:** *Branddocs SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *ykl7nnH/Iipzv+DQQdA2yTLJL6Q=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-10-10T00:00:00Z*

**33.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**33.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**33.1.3 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/PSES/Q>

### Service Name

**Name** [ en ] *Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L.*

**Name** [ es ] *Servicio cualificado de preservación de firmas electrónicas cualificadas y sellos electrónicos cualificados del proveedor BRANDDOCS, S.L.*

### Service digital identities

#### X509SubjectName

**Subject 2.5.4.97:** *VATES-B87142618*

**Subject CN:** *Servicio preservación de firmas y sellos cualificados*

**Subject SERIAL NUMBER:** *B87142618*

**Subject O:** *Branddocs SL*

**Subject C:** *ES*

#### X509SKI

**X509 SK I** *ykl7nnH/lipzv+DQQdA2yTLJL6Q=*

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** *2019-06-24T00:00:00Z*

#### 33.1.3.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 33.1.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 33.2 - Service (granted): Qualified preservation service for qualified electronic signatures and qualified electronic seals by BRANDDOCS, S.L. (2022)



**Subject O:** *BRANDDOCS SL*

**Subject C:** *ES*

**Valid from:** *Tue Mar 15 10:35:00 CET 2022*

**Valid to:** *Fri Mar 14 10:35:00 CET 2025*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D4C8A03F90BE6976FA C41C04953091022894FB33563065132185A6787113FDE1BE90D6  
505C0AA2C33BBD05B43DD01D611E45492237CD74F3B75C66886BCED578FCB96AE7CE1F0F6D0E9CF8E5AC12D2E39E3FE2AFESA235201013D111D361742B46  
895C44087C872B9533DB8DF31981CF995C2B9C62545A8EF31C82165CBFFEBCS2AA29398119F1E D36D DA17E59EEFC7D E7E96CC0E5FB2D043543C2B932AF C5278  
33F24AD8669D9A68F87F7201A3C027A05821B D0A6CD5317AEAE4122401F82FEED0A03DA9A233D124569C0E3DB6A110E1311317AD E5521583E239129F15DF4AA65F6  
041DA82EAEF161B2A55BDC1932A522BB2FB9DC EF37B7C949CD370203010001

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*D6:83:3D:D6:08:D6:88:D9:20:B0:7D:FD:95:93:C3:79:85:8D:D8:4B*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.3*  
*Policy OID: 1.3.6.1.4.1.47286.1.9.6*  
*CPS pointer: https://www.uanataca.com/public/cps/*  
*CPS text: [Qualified certificate for e-seal in Remote QSCD]*

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage**  
*id\_kp\_clientAuth*

**Subject Alternative Name**  
*certificates@branddocs.com*

**Key Usage:**  
*digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*09:CC:A5:F5:EC:32:42:FE:FA:C0:38:5E:27:CF:CD:75:28:B7:84:DB:9B:1D:AB:63:D8:C8:40:F5:C  
4:B4:4A:00*

**X509SubjectName**

**Subject 2.5.4.97:**  
*VATES-B87142618*

**Subject CN:**  
*Servicio preservación de firmas y sellos cualificados*



**Subject SERIAL NUMBER:** B87142618

**Subject O:** BRANDDOCS SL

**Subject C:** ES

**X509SKI**

**X509 SK I** 1oM91gjWiNkgsH39lZPDeYWN2Es=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2022-10-10T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**33.2.1 - Extension (not critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**33.2.2 - Extension (not critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

## 34 - TSP: Ecertic Digital Solutions, S.L.

### TSP Name

**Name** [ en ] *Ecertic Digital Solutions, S.L.*

**Name** [ es ] *Ecertic Digital Solutions, S.L.*

### TSP Trade Name

**Name** [ en ] *ECERTIC*

**Name** [ es ] *ECERTIC*

**Name** [ en ] *VATES-B87428728*

**Name** [ es ] *VATES-B87428728*

### PostalAddress

**Street Address** [ en ] *Avda. Europa, 24, Edificio B, Planta 1, Parque Empresarial de La Moraleja*

**Locality** [ en ] *Alcobendas*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28108*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *mailto:info@ecertic.com*

**URI** [ en ] *http://www.ecertic.com*

### TSP Information URI

**URI** [ en ] *http://www.ecertic.com*

## 34.1 - Service (withdrawn): Qualified timestamps issued by ECERTIC

### Service Type Identifier

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** [ en ] *A time-stamping generation service creating and signing qualified time-stamps tokens.*

[ es ] *Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

### Service Name



**Valid to:** Sun Oct 17 13:31:47 CEST 2027

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0E:00:30:82:01:0A:02:82:01:01:00:C5:77:C2:DF:B1:2C:1F:71:EB:A5:CC:AD:E3:76:8A:A1:F2:3D:1A:94:4D:49:3D:DF:1F:79:D6:82:B3:83:B7:42:D2:6  
B:74:41:5E:AF:88:CE:91:B7:0E:4D:8C:C1:4E:17:B3:CD:86:6A:70:20:0E:90:BF:1F:13:80:EC:6A:9A:F8:70:66:ED:0E:5A:6C:0A:83:AD:81:3B:83:1F:CB:BA:44:4E:ED:17:AA:6E:2D:A3:2A:95:CF:64:80:A0:03:2C:DF:D6:05  
:9B:1B:B7:E2:35:D8:5E:D3:6F:81:0C:7C:AE:27:D1:7B:6B:FD:CC:35:7D:E6:5A:56:D3:74:F9:A2:24:05:18:D4:2B:78:9D:72:C2:AB:A6:A8:8D:C0:F0:38:4D:BA:B4:D3:4C:9F:D9:0A:13:AC:25:E8:6C:37:EC:4D:2C:19:BD:3  
A:7E:D0:BE:2C:46:8F:FE:91:30:78:6C:B3:87:F0:CD:AF:0C:55:EA:90:76:67:A9:2E:33:65:88:2D:9B:B4:14:8F:44:41:95:B0:FB:90:31:A4:9C:7A:BE:CA:1A:1B:C3:8E:D5:A5:FC:79:E4:3E:1F:64:96:D3:7D:2D:DA:61:01:13:8  
4:4A:7D:57:2E:13:A4:65:54:A8:E7:CF:95:02:65:E8:70:CF:F3:F9:BD:97:A1:2E:55:5C:92:E6:19:49:02:03:01:00:01

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
C1:1A:67:92:D4:E3:D8:30:84:24:3D:D5:1A:4C:35:27:97:18:5D:99

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47286.2.5  
CPS text: [Certificado de sello de tiempo electrónico.]  
CPS pointer: <https://www.uanataca.com/public/cps/>  
Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Subject Alternative Name**  
info@ecertic.com

**Key Usage:**  
digitalSignature

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
0C:74:B1:2B:AE:CE:B8:32:22:44:C2:03:69:CA:00:2F:AE:74:CA:F3:61:5D:C0:FC:9D:C2:4B:39:5  
E:DC:EC:78

**X509SubjectName**

**Subject 2.5.4.97:**  
VATES-B87428728

**Subject CN:**  
ECERTIC QUALIFIED TSU01

**Subject OU:**  
ECERTIC TSP

**Subject O:**  
ECERTIC DIGITAL SOLUTIONS SL

**Subject L:**  
MADRID

**Subject C:**  
ES

X509SKI

**X509 SK I***wRpnktTj2DCEJD3VGkw1J5cYXZk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2021-10-26T01:00:00Z***34.1.1 - History instance n.1 - Status: granted****Service Type Identifier***http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST***Service Name****Name***[en]**Qualified timestamps issued by ECERTIC***Name***[es]**Sellos de tiempo cualificados emitidos por ECERTIC***Service digital identities****X509SubjectName****Subject 2.5.4.97:***VATES-B87428728***Subject CN:***ECERTIC QUALIFIED TSU01***Subject OU:***ECERTIC TSP***Subject O:***ECERTIC DIGITAL SOLUTIONS SL***Subject L:***MADRID***Subject C:***ES***X509SKI****X509 SK I***wRpnktTj2DCEJD3VGkw1J5cYXZk=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Status Starting Time***2019-11-06T01:00:00Z*

**35 - TSP: DIGITEL ON TRUSTED SERVICES S.L.U.****TSP Name**

**Name** [ es ] DIGITEL ON TRUSTED SERVICES S.L.U.

**Name** [ en ] DIGITEL ON TRUSTED SERVICES S.L.U.

**TSP Trade Name**

**Name** [ es ] DIGITEL ON TRUSTED SERVICES

**Name** [ en ] DIGITEL ON TRUSTED SERVICES

**Name** [ en ] VATES-B47447560

**Name** [ en ] DIGITEL ON TRUSTED SERVICES SLU

**PostalAddress**

**Street Address** [ es ] C/ ENRIQUE CUBERO, 9

**Locality** [ es ] VALLADOLID

**State Or Province** [ es ] VALLADOLID

**Postal Code** [ es ] 47014

**Country Name** [ es ] ES

**PostalAddress**

**Street Address** [ en ] C/ ENRIQUE CUBERO 9

**Locality** [ en ] VALLADOLID

**State Or Province** [ en ] VALLADOLID

**Postal Code** [ en ] 47014

**Country Name** [ en ] ES

**ElectronicAddress**

**URI** [ es ] <mailto:contratacion@madisonmk.com>

**URI** [ es ] <https://www.digitelts.es>

**URI** [ en ] <https://www.digitelts.es>



**Issuer SERIAL NUMBER:** A82743287

**Issuer OU:** AC CAMERFIRMA TSA - 2016

**Issuer OU:** see current address at <https://www.camerfirma.com/address>

**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject C:** ES

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject CN:** DIGITEL ON TRUSTED SERVICES

**Valid from:** Fri Aug 23 13:13:17 CEST 2019

**Valid to:** Wed Aug 21 13:13:17 CEST 2024

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009CEA:AF:CF:0A:08:67:D4:56:24:A6:E7:83:F5:CD:F8:B3:64:3B:A0:8A:2B:83:A0:ED:00:91:3C:7F:56:52:7C:A1:22:C9:0D:1A:90:B7:05:82:8B:35:57:C8:F1:4E:9F:64:C5:47:56:00:83:7C:8B:CB:EB:53:C7:43:11:05:AF:C5:AE:B3:21:F3:34:D6:21:2E:85:2F:50:8D:49:2D:9B:9F:75:8A:87:87:F9:11:E6:E1:84:73:1E:81:08:EF:A3:7A:0B:2E:86:60:EB:BE:A7:40:B5:92:E3:4E:1B:B5:70:54:5E:DF:83:17:72:23:F9:99:86:AK:36:51:D6:B4:E0:1F:CA:57:5B:D1:18:32:24:5B:C6:99:09:F8:54:9D:E1:39:DE:92:09:38:C3:DE:EB:0D:A7:66:F1:75:13:09:A6:B2:D2:71:F6:D9:80:F A:66:99:A8:EB:06:03:A7:44:C8:03:E5:FE:0D:B2:84:60:02:68:66:FE:B5:13:E9:4C:C9:7E:89:18:11:3E:A9:28:8B:53:36:69:60:C5:75:51:BF:55:AA:DE:43:42:53:8B:BB:EE:54:13:DC:D1:3D:3E:63:B1:5A:C3:21:57:DC:C8:FC E3:E9:D0:7E:31:35:04:EB:AA:6D:79:35:4B:2B:00:62:65:0C:E3:22:9D:AB:F1:C5:02:03:01:00:01

**Basic Constraints** *IsCA: false*

**Extended Key Usage** *id\_kp\_timeStamping*

**Subject Key Identifier** *F5:80:B3:6F:A3:FA:39:44:54:4F:13:C7:61:EF:06:F0:88:CC:D6:E1*

**Authority Info Access**  
[http://www.camerfirma.com/certs/ac\\_camerfirma\\_tsa-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt)  
<http://ocsp.camerfirma.com>

**Authority Key Identifier** *1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*

**CRL Distribution Points**  
[http://crl.camerfirma.com/ac\\_camerfirma\\_tsa-2016.crl](http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma\\_tsa-2016.crl](http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl)

**Issuer Alternative Name** *ca@camerfirma.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1*  
*CPS pointer: <https://policy.camerfirma.com>*  
*CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en <https://policy.camerfirma.com>]*  
*Policy OID: 0.4.0.194112.1.3*



**QCStatements - crit. = false**      *id\_etsi\_qcs\_QcCompliance*  
    *id\_etsi\_qcs\_RetentionPeriod: 15*  
    *id\_etsi\_qcs\_QcSSCD*

**Key Usage:**                                *nonRepudiation*

**Thumbprint algorithm:**                *SHA-256*

**Thumbprint:**                              *B9:90:57:F8:85:AD:50:70:55:A0:34:D0:29:5C:12:CD:E9:10:EA:47:51:61:51:18:DC:E2:9A:81:4F:AB:B0:FA*

**X509SubjectName**

**Subject C:**                                 *ES*

**Subject O:**                                 *DIGITEL ON TRUSTED SERVICES SLU*

**Subject 2.5.4.97:**                        *VATES-B47447560*

**Subject CN:**                                *DIGITEL ON TRUSTED SERVICES*

**X509SKI**

**X509 SK I**                                    *9YCzb6P6OURUTxPHYe8G8IjM1uE=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description**    *[en]                    undefined.*

*[es]                    undefined.*

**Status Starting Time**

*2022-02-08T00:00:00Z*

**35.1.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service Name**

**Name**                                        *[es]                    Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES*

**Name**                                        *[en]                    Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES*

**Service digital identities****X509SubjectName**

**Subject C:**                                 *ES*

**Subject O:**                                 *DIGITEL ON TRUSTED SERVICES SLU*

**Subject 2.5.4.97:** VATES-B47447560

**Subject CN:** DIGITEL ON TRUSTED SERVICES

**X509SKI**

**X509 SK I** 9YCzb6P6OURUTxPHYe8G8IjM1uE=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2019-12-16T01:00:00Z

**35.2 - Service (withdrawn): Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description**

[en] A time-stamping generation service creating and signing qualified time-stamps tokens.

[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

**Service Name**

**Name** [en] Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020

**Name** [es] Sellos de tiempo calificados emitidos por DIGITEL ON TRUSTED SERVICES 2020

**Service digital identities**

**Certificate fields details**

**Version:** 3

**Serial Number:** 870476239836202459339

**X509 Certificate**

```
-----BEGIN CERTIFICATE-----
MIIRCCB2gAwIBAgILBICZ2I0DLMA0GCSqGSIb3DQEBCwUAMIBBDELMAAGAUUEBMMCRVMs
DzANBgNVBAEMBkIBFRJURDEPMAOGAUEBwwGTFUFEUEKEMUwOAYDVQQQLDZlZWUyY3YyemVudCBh
ZGRyZnZlZGF0IGh0dHBoO8vds3l.mNbbWVyzmlybWUy29H2FKZHLc3MxTAIBGNVBAsMGFFD
IEABTUUSKISUUEgVFN8CIGhAANESMBAGAUEBMMCRVMsDzANBgNVBAEMBkIBFRJURDEPMAOGA
UYyBODI3NDMyODExGzAZBgNVBAoMEKFDIENBTUUSKISUUEgVFN8CIGhAANESMBAGAUEBMMCRVMs
RVJGSVJNQSBUUEgLSyMDEZMBA0XD1TMDUyNgE2MzQzNjE0MDUyNjE2MzQzNjE0MDUyNjE2MzQz
AUEBMMCRVMsDzANBgNVBAEMBkIBFRJURDEPMAOGAUEBMMCRVMsDzANBgNVBAEMBkIBFRJURDEP
NjAAKDAmBgNVBAoMH0RIR0URUwU04gVjVUURFRRCBTRVJWSUUNFUyBTTFUxZAAIBGNVBAYTAkV
MIIBJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAQEA2cMgdWes4PpmsCLQYppmRhl6QSTNY
WTF7R6f+OzrBRHV7qf6d6f6eOHEKLAkCXKpYUwaa0F6GQK7H2Z5ZYW1T0X2e8sSf
d=-NaBFQ37FPob0YPRMMYLFROMEYBSorf3dXGSGXpcPQKryhKkbpstulN03DR6YQyEaRSP
IGPFRK8+NxWdR4BbaZKj+oMKI6r3Z2J10vTrlRnkKtP33AcGmm0Gjz5RwQmSSZrSag
mcvE5+gM2uagPFV6vFMV+ANuagP9bHsDKSv7M0X4L1UgdlMvnoKsYkNpKCAU8YyJR
tgnYQIDAQAAB4DQzCCAswDAYDR0TAAQHBAHADA0BGNVBO8BAEBAEMCBKAwEgYDR0IAQH/
BAwwGyIkwYBBQUHAwsgHQYDVROBBYEFNF0EAQJ+ncpl:64PHotvUgYycMH4GcC3GAQUFBwE6
BHFwZGRBgegrgRFBQcwoV6dHRKc6wL3d3dsyYWIcmZpmlHl.mNv8S9Z3J6e9bY19YWH
cmZpmlH3RZYS0yMDE2LmNydDAmBgNVBGEtFQ0wAUYaaHR0cDovL29c3AuY2FkZUJmaXRYS5j
b29wHwYDR0RBGwfoAUHm2YspvKlVn7rbRCqut7TtwgYGAUgHwR7MHkOq4A0DaGNGb0
dH46L99cmvY2FkZUJmaXRYS5jYyYwY2FkZUJmaXRYS5jYyYwY2FkZUJmaXRYS5jYyYwY2Fk
NWh0dH46L99cmvY2FkZUJmaXRYS5jYyYwY2FkZUJmaXRYS5jYyYwY2FkZUJmaXRYS5jYyYw
A1UdEgOVMBOBEWNBQGNbbWVyzmlybWUy29MjHGBGNVHSAEg4wgsuGADSSGA0QBYcuChAF
AQEzZswKQYKRYBRU/HAgWfW0dHBo8vcs98wS1.mNbbWVyzmlybWUy29MjHGBGNVHSAEg4wgsu
BwICMGMAYENcRnZmlyYWRHENTYWspZmlyYWRvIGRIRFRVTS4gQ29uc3VsdGJgbGFzGNvbmRp
Y29vbmVzIGRIRHvzbyBibBodHRwczovL3Bv8GjE8SjYWIcmZpmlHl.mNv8S9Z3J6e9bY19YWH
MIIBAgEgRFBQcwoV6dHRKc6wL3d3dsyYWIcmZpmlHl.mNv8S9Z3J6e9bY19YWHYBBDCBKOY
BACORgEFMIGMEEWO2h0dHBo8vcs98wS1.mNbbWVyzmlybWUy29MjHGBGNVHSAEg4wgsu
cnVb012MS4wR1ucCRmEwJlyBBHjodHRwczovL3Bv8GjE8SjYWIcmZpmlHl.mNv8S9Z3J6e9b
U10KZWdhbPQZJ6z346MEV1Lm8ZBMZAMoEwYGRACORgEFMAGG9gAIBYBBDCBKOYKCoZi
hveNAQELBQADgeBAEBAETHPSZoY1s89mcWRc+K0Hndfz2XnskMgIRXtFuxaYbbVmTOnoF4
7ns73CE8BPUR9A97ZAcw0B6ELUnalAD21HzBV57Df0t0eZFY9wBnczIX3mAA4QnnyvNlm
AmXvs8kY4U1RtoWw08n8W10E2Y4ZpVFEzGW7KxTfH5bdlJodw09m8kpeOw
naDnR5pNZIQ933H3grPcOnR3UnS2ukOygyymy1WHGf49TYaz7CB4MMK1tsr5VnXcKs
AmXQqHRP9IE2kw0KXz0LBOHMEYyjuCsefRQB4IPK+L36pmXckZc9N0zL5ghH1pqg/ZO
ndEzBRNEZznpYAXHedZ06v8emV6MgnN8z8+0zPKC7K4K6eHBR3k6G1W5z0Z
bfgmTGCaxUZd1W7Y1n7LZH9vpp09R8f0BPS8B-1GcNsdA8D0vN7Yw1TqZEWqco+M8x2c8
8NX7006m89ERjYgrAmnzlnlzi7KsQcYntZg28X1d0HqLk3JUDN7Cs1088S9bDZwhYtK9
EcgfXgXcW5c8z28K5L=90UTCzR8uK3Vnm4dH46wzllbazP7Dz58R9Pw1r5986
LcVv1vhaqHjsqP
-----END CERTIFICATE-----
```

**Signature algorithm:** SHA256withRSA

**Issuer CN:** AC CAMERFIRMA TSA - 2016

**Issuer O:** AC CAMERFIRMA S.A.

**Issuer 2.5.4.97:** VATES-A82743287

**Issuer SERIAL NUMBER:** A82743287

**Issuer OU:** AC CAMERFIRMA TSA - 2016

**Issuer OU:** see current address at <https://www.camerfirma.com/address>

**Issuer L:** MADRID

**Issuer ST:** MADRID

**Issuer C:** ES

**Subject C:** ES

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject CN:** DIGITEL ON TRUSTED SERVICES

**Valid from:** Wed May 27 18:34:14 CEST 2020

**Valid to:** Mon May 26 18:34:14 CEST 2025

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C7670C71D5A0E0FA66A022D0629A7D9A54612FA950E5332859314507AD1F8EB2B2C1447553A937BA7547E7DC380B452A82CA0025EACA8E0959AA1A405AFC18143B1EC648E4362B5874F4E97801B1289FFDF30D6817EB437ECS3F46F4B183D130C7D82C5468304601E68AC58B7B57846497A5C3D02ABC1FCAB5B66CD2E94DD370D1E9842DC84B91E4F7C63D3164F3EACDC360DA47805B9D92A3FA838C2A57DE477673D9FD74BD3AF3FD19CA8AD3FFDF701E1A68B03868EBE51590AE7492E59AD26A099CC04E7E80CD9AA4A80F155EA757F14CS7E012D1A803A75F6C1EC0CAD2C88ECC5F41242D4961814330AE8246B322A7329F8200853C620211B60AE2610203010001

**Basic Constraints** *IsCA: false*

**Extended Key Usage** *id\_kp\_timeStamping*

**Subject Key Identifier** *D1:4E:10:0A:D0:4F:FC:71:B6:91:1D:1B:83:C7:A1:3B:D4:81:8C:9E*

**Authority Info Access**  
[http://www.camerfirma.com/certs/ac\\_camerfirma\\_tsa-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma_tsa-2016.crt)  
<http://ocsp.camerfirma.com>

**Authority Key Identifier** *1E:6D:B5:C6:3F:EF:92:55:5E:37:FA:DB:FD:10:AA:BA:D9:3B:4E:2C*

**CRL Distribution Points**  
[http://crl.camerfirma.com/ac\\_camerfirma\\_tsa-2016.crl](http://crl.camerfirma.com/ac_camerfirma_tsa-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma\\_tsa-2016.crl](http://crl1.camerfirma.com/ac_camerfirma_tsa-2016.crl)

**Issuer Alternative Name** *ca@camerfirma.com*

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.17326.10.16.5.1.1

CPS pointer: <https://policy.camerfirma.com>CPS text: [Certificado Cualificado de TSU. Consulte las condiciones de uso en <https://policy.camerfirma.com>]

Policy OID: 0.4.0.194112.1.3

**QCStatements - crit. = false**

id\_etsi\_qcs\_QcCompliance

id\_etsi\_qcs\_RetentionPeriod: 15

id\_etsi\_qcs\_QcSSCD

**Key Usage:**

nonRepudiation

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

D1:A9:E8:21:8D:8D:4C:33:3F:41:F3:0F:7F:03:0B:39:5F:F8:C6:5C:8E:88:07:1F:DE:09:0B:CF:63:40:21:BF

**X509SubjectName****Subject C:**

ES

**Subject O:**

DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:**

VATES-B47447560

**Subject CN:**

DIGITEL ON TRUSTED SERVICES

**X509SKI****X509 SK I**

0U4QCtBP/HG2kR0bg8ehO9SBjJ4=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-05-22T00:00:00Z

**35.2.1 - History instance n.1 - Status: granted****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>**Service Name****Name**

[en]

Qualified timestamps issued by DIGITEL ON TRUSTED SERVICES 2020

**Name**

[es]

Sellos de tiempo cualificados emitidos por DIGITEL ON TRUSTED SERVICES 2020

**Service digital identities**

X509SubjectName

Subject C: ES
Subject O: DIGITEL ON TRUSTED SERVICES SLU
Subject 2.5.4.97: VATES-B47447560
Subject CN: DIGITEL ON TRUSTED SERVICES

X509SKI

X509 SK I 0U4QCtBP/HG2kR0bg8ehO9SBjJ4=

Service Status

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

Status Starting Time

2021-02-25T01:00:00Z

35.3 - Service (granted): Qualified timestamps issued by "DIGITEL TS QUALIFIED TSU 01 G1"

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en] A time-stamping generation service creating and signing qualified time-stamps tokens.
[es] Un servicio de generacion de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name [en] Qualified timestamps issued by "DIGITEL TS QUALIFIED TSU 01 G1"

Name [es] Sellos de tiempo cualificados emitidos por "DIGITEL TS QUALIFIED TSU 01 G1"

Service digital identities

Certificate fields details

Version:

3

Serial Number:

141599651441537325004941820603765328946848918827

X509 Certificate

-----BEGIN CERTIFICATE-----
MIH4zCCBucAwIBAgIU...
-----END CERTIFICATE-----

**Signature algorithm:** *SHA512withRSA*

**Issuer C:** *ES*

**Issuer L:** *Valladolid*

**Issuer O:** *DIGITEL ON TRUSTED SERVICES SLU*

**Issuer OU:** *DIGITEL TS CERTIFICATION AUTHORITY*

**Issuer SERIAL NUMBER:** *B47447560*

**Issuer CN:** *DIGITEL TS QUALIFIED CA TSA G1*

**Subject C:** *ES*

**Subject L:** *Valladolid*

**Subject O:** *DIGITEL ON TRUSTED SERVICES SLU*

**Subject 2.5.4.97:** *VATES-B47447560*

**Subject OU:** *Digital Qualified Time Stamp Services*

**Subject SERIAL NUMBER:** *B47447560*

**Subject CN:** *DIGITEL TS QUALIFIED TSU 01 G1*

**Valid from:** *Thu Jun 30 12:08:40 CEST 2022*

**Valid to:** *Wed Jun 28 12:08:39 CEST 2028*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100BF88CD5466DFEF115E4C74FFAC1722C380BC5B491648477A1ADC0F058D158574F5538  
D847E1D3B06BE9934A2045E33D8BF01A63A4D1F48F0CEA7F7E27642A5F44AAC4B861458BF04CC2C830A0D56D21A75A93D8BD9B86FF23E2A0DA7E279B2D95F5415  
7A24B758180E5AC4F6113B7D91D445E085F4098F2693CF68E3925F5F082CEF807713DE24FAA2892D98693C5005BDF67C7EBF794B8112819A0991B076703767D30A279  
25A3DC72CE2BABC761C471E8D7B77F9BE0847171F44F273A89CC86D19A0B860B5FCCE745CD01F558FC8F09FA9E6A2F02E7B067060998526A8F9B954D2D10E7  
517871BA1D44C2D50A56C584F897C0661BE3CCFD60A9E59043FA3C4FBB1BDBE6859E83C27014E32D6E5497B4491161007E7DD761D84A8440BE692A48801DB53640C  
ECFF63B8C5E882E9870C6333BF30770EFD83D4AF8325039826A1908C356AE36CEDB79280CD66A8F34062E893A8B995C17152A58A4E3AEC3E88929823E50F97B464  
FD5E2E7230CA2DE4DEE7A5548EC02B24EF2B832D652FAA4047B1B8C77E4E1EAO94D142A2CBBF66DC99E0DEE4B575626D2D0542A3EF7D71DD2D1094A914E9250  
115B3B294305B8572C7E83A3D1A0FE33864B2A3B2591C1F1846C27E029C8E812ED29BF170AB70555D11A736823789B2F4267A4E3FB9F244D57FF18B78D5F34CDF7  
68F572E40F2A2919FB444DD75FFC0D8E7244B47450203010001

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

**Authority Info Access** *http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt*  
*http://ocsp.digitelts.es*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.54225.10.1.1*  
*CPS pointer: https://pki.digitelts.es/dpc/*  
*Policy OID: 0.4.0.2042.1.2*

**Extended Key Usage** *id\_kp\_timeStamping*

**CRL Distribution Points** *http://cr1.pki.digitel.es/DTSQualifiedCATSAG1.crl*  
*http://cr2.pki.digitel.es/DTSQualifiedCATSAG1.crl*

**Subject Key Identifier** *C6:00:6E:47:EF:24:09:E7:E0:AB:E1:04:72:B2:4D:10:E4:2B:D6:56*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *BA:7F:C0:35:E5:D2:E5:87:4C:6A:65:ED:FA:AD:C6:CC:39:31:AE:02:14:F6:0F:CC:DA:33:08:AB:14:33:74:1C*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Valladolid*

**Subject O:** *DIGITEL ON TRUSTED SERVICES SLU*

**Subject 2.5.4.97:** *VATES-B47447560*

**Subject OU:** *Digitel Qualified Time Stamp Services*

**Subject SERIAL NUMBER:** *B47447560*

**Subject CN:** *DIGITEL TS QUALIFIED TSU 01 G1*

**X509SKI**

**X509 SK I** *xgBuR+8kCefgq+EEcrJNEOQr11Y=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2022-11-17T00:00:00Z*

**35.4 - Service (granted): Qualified timestamps issued by “DIGITEL TS QUALIFIED TSU 01 G2”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*  
*[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

**Service Name**

**Name** *[en] Qualified timestamps issued by “DIGITEL TS QUALIFIED TSU 01 G2”*





**Valid from:** Thu Jun 30 13:30:58 CEST 2022

**Valid to:** Wed Jun 28 13:30:57 CEST 2028

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100BF082E255CFB90A49E4AC8635F3BCD4C81007253F3C0E7D0BE6E1B60AFA7EF0565DD45498E9B2975E4FE6D0D0F3895CD3144CB6857AB0676FC02C89D1826D07B2AFAE82ED732F2133851D8B19CF3236AE901096E622920368D66AF11C4F5B98399C121789151E12E2CED9629B657C0C5F7E3B96085EC0865AC089B6C94FC2A82934084E4E8D9CC21CC2E13DBD67167C13ECB9B4CC56AFAFD3A88E5B3A36464078DA06EB131E12AB791E85349ABD0552548A01115FC4AF63A33E16991C3D3D9A40D26398C8946D9A1D108CB6F49E1A2298BE50FC6A6AD543CE96A396040EB0A759996365151F33R2FA839540C2067D85FDAB17E854AE32FD0E0C28BE9CF0E0CC86F4BE152D1DCE26A8B72D2683661B7CA7BF8D3E130371B9B4829A71FD94C090F720600FC9601D6A2BAFE7698197FA1A1F51103EA145A8F9B04D4E7F97BFB8E0E32015B17BB7877806FE2C7D2ACC357AF3F621D16807F9D11DB5299871EF0AA9E3E3B434BE6B87DD3694A6760A9BB6E9401F3F26AA12FE0A5ED8F40A93A27721A64815B63FBD537A6E8E2E072725D7D87262D8FA9CAD1B102EB145121FBA34EB7C36A1682B85CF40B4E8B92DD161544F2158CDBA4536AE9AB0D088FD77A3CF63E8FA6ECC2017368209CD04C9D4D8A91CD9BF599916BBD35F459EF2953E72924FE720CEBD83F1C415C10F2DD6692BF7E0C31A2B252FF86375E33566BD0203010001

**Basic Constraints** IsCA: false

**Authority Key Identifier** 90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

**Authority Info Access**  
<http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt>  
<http://ocsp.digitelts.es>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.54225.10.1.1  
CPS pointer: <https://pki.digitelts.es/dpc/>  
Policy OID: 0.4.0.2042.1.2

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier** 33:13:4D:09:C7:27:E0:3B:BA:B3:5E:E5:8D:89:52:80:1A:80:70:5C

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 42:20:4F:FC:35:09:CF:25:00:F2:03:07:F5:68:6F:10:0A:FD:84:FA:CC:9C:ED:B1:91:1E:15:4E:B5:6B:F7:AC

**X509SubjectName**

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digitel Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU 01 G2

**X509SKI**



**Issuer SERIAL NUMBER:** B47447560

**Issuer CN:** DIGITEL TS QUALIFIED CA TSA G1

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digital Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU 01 G3 EDCSA

**Valid from:** Thu Mar 16 13:23:49 CET 2023

**Valid to:** Wed Mar 14 13:23:48 CET 2029

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:92:8F:03:89:B0:2F:95:58:0A:1D:37:E9:95:78:02:14:72:2D:02:9F:7E:5E:BA:F6:FC:6F:50:21:C5:3C:7F:6E:86:62:F3:E5:9A:C2:6F:9F:9E:B1:F6:69:D9:DC:94:92:C2:54:14:37:75:00:A7:AF:7A:48:16:74:36:DC:2D:76

**Basic Constraints** IsCA: false

**Authority Key Identifier** 90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

**Authority Info Access**  
<http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt>  
<http://ocsp.digitelts.es>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.54225.10.1.1  
 CPS pointer: <https://pki.digitelts.es/dpc/>  
 Policy OID: 0.4.0.2042.1.2

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier** F0:A2:B9:62:9F:51:E5:78:F2:A1:95:3E:68:06:74:61:C2:D4:09:6E

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 46:08:11:36:5D:55:B6:60:BB:73:D1:50:56:2D:06:59:68:8E:A0:9A:B5:9E:45:0F:56:18:9E:D6:EE:71:5F:C4

X509SubjectName

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digital Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU 01 G3 EDCSA

**X509SKI**

**X509 SK I** 8KK5Yp9R5XjyoZU+aAZ0YcLUCW4=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2023-05-22T00:00:00Z

### 35.6 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [es] Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

**Name** [en] Qualified timestamps issued by DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 607932644424710360540674319403629739410233125839

## X509 Certificate

-----BEGIN CERTIFICATE-----

```

MIIGHjCCBAgAwIBAgIUanYkgQEWw+sSIBBTk0wEymXOa88wDOYKozIhveNAQENBOAwbYzJzAI
BgNVBAMMHHRJRU0URUwvVFMglVVVBEIGSUVEIENBIFRFTOSBMTESMBAGAUEBRMjQzNDQ3NTYw
MSswOjY0Q0QDCESLjVEVMIERTIENFLIRkRkDQVBT09gOVVUSzNSVZMzswZjY0Q0QDB9E
SLjVEVMIe9IFRSVNVNURUQzU0VSVkIDRVMEUyVMMRMwFQYDVOQHDAWYW5sYWRybGkRQmVwCQYD
V0QGEwJFJUZAFw0yMzAaMTYyMjMwOTQzMTQzMTQzMTQzMTQzMTQzMTQzMTQzMTQzMTQzMTQz
VEVMIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTIERTI
A1UECwwiRGlmaXVkbCBBdWwvVFMglVVVBEIGSUVEIENBIFRFTOSBMTESMBAGAUEBRMjQzNDQ3
RVMjQzNDQ3NTYwMSswOjY0Q0QDB9EjY0Q0QDB9EjY0Q0QDB9EjY0Q0QDB9EjY0Q0QDB9EjY0
EQYDVOQHDAWYW5sYWRybGkRQmVwCQYDQ0QDB9EjY0Q0QDB9EjY0Q0QDB9EjY0Q0QDB9EjY0
BHRVFRYyZ3VlEwvVFMglVVVBEIGSUVEIENBIFRFTOSBMTESMBAGAUEBRMjQzNDQ3NTYwMS
qDLSyX127gggHIMIBdAMBeNVHMBARBAIAAMB8GAUdhwQYMBaAFJab3RnkyhMc9K2-M
9p3342MkCCSGAGUJFwEhBBSwaTBBrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgrgr
ZMvREHSVRFTFRUVVBEIGSUVEIENBIFRFTOSBMTESMBAGAUEBRMjQzNDQ3NTYwMSswOjY0
LmRnZ2l0ZWx0cy5lc3ZlY291bnR0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0
dHREb3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0
Bo4DCDCBQYDVR0BHhwaG90dG90aW50aHR0cC90aW50aHR0cC90aW50aHR0cC90aW50aHR0cC
dWIsaWZpZW50b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0b3R0
VEVNRWwvVFMglVVVBEIGSUVEIENBIFRFTOSBMTESMBAGAUEBRMjQzNDQ3NTYwMSswOjY0
VR0PQHBAQDAgeAMA0GCSGIB3DQEBDQAA4CAQAYSTaGON3S52sw5naIQ0wIKRAN+sGz
6vXrCpR WadoulKgdWkgG5UjGbaPQPWUE+MgbsVIBVtOXAyJYAdGLLeJskr421v51z7K
KSNtIdT0XC+ZEIE9glLyn0aAwTAgMCR0Qp9ydlImRzozsAGZSNEX1C99B-R0kYuaRC
DMY6akVSLJgZ0h8vokSAGoSt4qMYSI+6P3yqjAMvyeKs2286L7ocSLHQUSGR003Vnd
FmngDFRqV3xz2RVEkXfj6d006qL3pHfBdDpzeAhhRcO41GCtHhhKhu0GWS7ay5IbB
PHRWkz3s+Iez/TjNoRDLE049+6fms0mk60C8vBRSHZCwNECpV3ZaxCNSF4L9V2LY
jXO1a3ln1l1bF5S8KSSyTafVgleW4ZL5xjAfyS8BPkpdSOzq11IbE18H99SsqWCWw082
SAUHOxBrgrBQCLbac9WV8pnnGBvxxw0DQzgiAuNPzvccj25FECdOWmDrrOXk181pKf23
R0p9ZAcwN6BfE5AQZUEHEDZ7Ct2L1LGA7bhhA+mmuE5P8E9w40CaOprsjGeAGI2vXoC1
R9SRGNOLctGpewNjssL7hJF20xtpaqlHhXR7raPQ=

```

-----END CERTIFICATE-----

## Signature algorithm:

SHA512withRSA

## Issuer C:

ES

## Issuer L:

Valladolid

## Issuer O:

DIGITEL ON TRUSTED SERVICES SLU

## Issuer OU:

DIGITEL TS QUALIFICATION AUTHORITY

## Issuer SERIAL NUMBER:

B47447560

## Issuer CN:

DIGITEL TS QUALIFIED CA TSA GI

## Subject C:

ES

## Subject L:

Valladolid

## Subject O:

DIGITEL ON TRUSTED SERVICES SLU

## Subject 2.5.4.97:

VATES-B47447560

## Subject OU:

Digitel Qualified Time Stamp Services

## Subject SERIAL NUMBER:

B47447560

## Subject CN:

DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

## Valid from:

Thu Mar 16 13:21:58 CET 2023

## Valid to:

Wed Mar 14 13:21:57 CET 2029

## Public Key:

30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:7F:15:4C:55:91:45:8D:95:F0:4F:80:C9:0A:A6:41:D4:ED:D0:1A:12:25:16:B6:00:51:B7:3A:A8:9A:28:B9:D9:1D:6D:A7:06:8C:47:66:79

.E5:23:B9:51:0A:C3:10:32:1D:59:3A:33:74:A2:AA:48:AB:F0:CB:4B:25:ES:DB:BB

## Basic Constraints

IsCA: false

## Authority Key Identifier

90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

## Authority Info Access

<http://pki.digitel.es/DIGITELTSQUALIFIEDCATSAG1.crt><http://ocsp.digitel.es>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.54225.10.1.1  
 CPS pointer: <https://pki.digitel.es/dpc/>  
 Policy OID: 0.4.0.2042.1.2

**Extended Key Usage**  
 id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl1.pki.digitel.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitel.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier**  
 72:8B:D8:EC:D8:DC:B3:FD:B7:44:B6:F0:78:0E:FC:04:48:EC:1D:6D

**Key Usage:**  
 digitalSignature

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 E6:7A:2E:75:8C:88:73:5D:5A:76:F0:BA:53:3B:36:33:8F:5A:9D:B9:05:4C:E5:83:1C:30:A1:04:9F:12:5C:1B

**X509SubjectName**

**Subject C:**  
 ES

**Subject L:**  
 Valladolid

**Subject O:**  
 DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:**  
 VATES-B47447560

**Subject OU:**  
 Digitel Qualified Time Stamp Services

**Subject SERIAL NUMBER:**  
 B47447560

**Subject CN:**  
 DIGITEL TS QUALIFIED TSU 01 G4 EDCSA

**X509SKI**

**X509 SK I**  
 covY7Njcs/23RLbweA78BEjsHW0=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**  
 2023-05-22T00:00:00Z

### 35.7 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU 01 G5 EDCSA

**Service Type Identifier**  
<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>



**Subject SERIAL NUMBER:** *B47447560*

**Subject CN:** *DIGITEL TS QUALIFIED TSU 01 G5 EDCSA*

**Valid from:** *Thu Mar 16 13:18:36 CET 2023*

**Valid to:** *Wed Mar 14 13:18:35 CET 2029*

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:3A:B9:F9:26:FB:F0:32:9A:FF:1D:4E:81:93:E8:2D:1B:9B:BF:2C:4A:3E:F1:78:D7:80:07:6E:BB:49:63:28:30:5A:D9:14:F3:F9:70:B2:69:62:65:B1:B8:3B:48:41:DA:7A:13:05:7A:F7:AE:9F:00:A2:C6:37:E1:FC:78:30:E8

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B*

**Authority Info Access**  
*http://pki.digitel.es/DIGITELTSQUALIFIEDCATSAG1.crt*  
*http://ocsp.digitel.es*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.54225.10.1.1*  
*CPS pointer: https://pki.digitel.es/dpc/*  
*Policy OID: 0.4.0.2042.1.2*

**Extended Key Usage** *id\_kp\_timeStamping*

**CRL Distribution Points**  
*http://crl1.pki.digitel.es/DTSQualifiedCATSAG1.crl*  
*http://crl2.pki.digitel.es/DTSQualifiedCATSAG1.crl*

**Subject Key Identifier** *B7:72:0D:47:7C:A1:82:24:D9:AA:94:6E:BF:65:AE:A8:1A:DB:7B:C7*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *18:33:FE:5F:4E:B1:0F:4E:98:00:6F:29:28:1A:49:B8:57:85:73:52:59:97:0D:DF:69:FA:E3:DA:A1:0B:67:5A*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Valladolid*

**Subject O:** *DIGITEL ON TRUSTED SERVICES SLU*

**Subject 2.5.4.97:** *VATES-B47447560*

**Subject OU:** *Digital Qualified Time Stamp Services*

**Subject SERIAL NUMBER:** *B47447560*

**Subject CN:** *DIGITEL TS QUALIFIED TSU 01 G5 EDCSA*





**Issuer OU:** DIGITEL TS CERTIFICATION AUTHORITY

**Issuer SERIAL NUMBER:** B47447560

**Issuer CN:** DIGITEL TS QUALIFIED CA TSA G1

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digital Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU EDCSA 01 G6

**Valid from:** Thu Mar 16 13:16:09 CET 2023

**Valid to:** Wed Mar 14 13:16:08 CET 2029

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:40:1B:43:C7:1B:D1:B8:04:5B:55:0C:26:81:F3:27:4D:AE:95:F1:7A:E0:35:E1:12:73:FB:B2:D5:43:6D:7D:DE:0F:01:A6:3C:E7:8A:5D:A2:CE:46:76:71:AD:A3:5B:15:23:6D:80:D1:69:F0:15:48:D3:64:9F:C9:4A:D4:EA:9C

**Basic Constraints** IsCA: false

**Authority Key Identifier** 90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

**Authority Info Access**  
<http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt>  
<http://ocsp.digitelts.es>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.54225.10.1.1  
 CPS pointer: <https://pki.digitelts.es/dpc/>  
 Policy OID: 0.4.0.2042.1.2

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier** 21:02:63:16:C1:F8:84:80:77:D6:EC:8B:DE:59:AF:A2:5B:4C:2F:54

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 4E:5A:0E:99:9E:1C:D9:12:75:C5:7D:F2:94:C4:8A:23:00:D0:4E:A7:06:5D:58:31:25:63:C2:59:42:86:E8:D7

**X509SubjectName**

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digital Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU EDCSA 01 G6

**X509SKI**

**X509 SK I** IQJfFsH4hIB31uyL3lmvoltML1Q=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2023-05-22T00:00:00Z

**35.9 - Service (granted): Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU RSA2048 01 G7**

**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos cualificados.

**Service Name**

**Name** [es] Sellos de tiempo cualificados emitidos por DIGITEL TS QUALIFIED TSU RSA2048 01 G7

**Name** [en] Qualified timestamps issued by DIGITEL TS QUALIFIED TSU RSA2048 01 G7

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 371184069619154176167623148387204370136767472539

X509 Certificate

-----BEGIN CERTIFICATE-----
MIIG6sCBNOgAwIBAgIUQOR4ImGgiGHnkFGvMYz2RIJ5swDOYkZlHvcNAOENBOAwgByZzAl
BgNVBAMMHHRJRUURUwVFMglVVBTEIGSUVEINEBIFERTOSHMTESMBAGAUEBRMJOQ3NDQ3NTYw
M5swK0YDQQDCZESIjVEVEMIRTIENFLIRKIDVRI7096GVVUS9S5VZM5gWjYDVOQKDB9E
SLdVVEVME90FRSVNURUQsU0V5VlDRVMgl0sYMRMwFQYDVOQHDApWYWasYWRwbcGRQmCQYD
VQOGEwJFUzafW0yMzAaMTAwOTQwMTdafaW0yOTAzMjgwOTQwMTZaMHhMS8wLQYDVQDDZCESUdI
VEVMIHRITFFVQURKIFRBU1UgUjU0NDMjA0CAwMSBINEESMBAGAUEBRMJOQ3NDQ3NTYwM5sw
LAYDVQDDZCESIjVEVEMIRTIENFLIRKIDVRI7096GVVUS9S5VZM5gWjYDVOQKDB9E
QVRFUyIjNDQ3NDQ3NTYwM5swK0YDQQDCZESIjVEVEMIRTIENFLIRKIDVRI7096GVVUS9S5VZM5gWjYDVOQKDB9E
EzARBgNVBAskZm9udC9zaW9uW0cAIBGVNVAITAVYVMIHBAjBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBGKCAQEAgPw0P9yRk1VnMSD3SALb7SR8bB4AZ16a4ZPdc1K0akQspdwsc3U5G3DB
hzi19PCxAG5HndhCPaD39OWmpDSIOGSLIcydNvLvB-SSVaoVRPILGMSpPqHODgC89ozMpij
FMESIjVEVEMIRTIENFLIRKIDVRI7096GVVUS9S5VZM5gWjYDVOQKDB9E
sq3p4PnsVOWWA WKY2HdUjUjIDGySwkEjKagw0GUE2AMERIHoh3vApe2Rerw0T1uA8Jt
gVUBXcyvczT747923eYSc2xPvvdsc4W8VB0ckODMYDnwIDAQABo4IBDCCAcOwDAVDVROT
A0HBAwwADAjBgNVMSMEDA WgBjQ94E23MoTHTFVwYKp09wNmzB3BggrIglBQkBAQRAGlGw
QOYKwYBBQlHMAKGNWb0dHA6L9ywa2kzGlnaXRIBHkZLmVLRJRUURU1U1FVQURKIFREN
BVFNBzEaY3J0MCCGCGCsGAQUFBzAbhhdHRwO8vb2NzcSkaWpdGVsdHMuzXUwTwYDV80gBEgw
RjABBggrIglEAYOLQkBA1A1MCCGCGCsGAQUFBzAbhhdHRwO8vb2NzcSkaWpdGVsdHMuzXUw
ZHBjLzABGyEAI86A0wFgYDVR0MAQHBAwwCgYIKwYBBQUHAwEgEYGAUdHwR6MHgwOq4o4o4o4
NGB0HAA6L9yemwLmBraSkaWpdGVsdHMuzXUwRFRU1U1FVQURKIFREN
HOYDVR00BBYEFBzSEBC8s4ISLLdncypGOEYUAMAGAIUdDwEBwQEAWHGDANBgkqhkiG9w0B
AQOFAAOCAgEAd2SE00KSc3B6o1LLZ9pVQ0M57u0Z2oug8gyU9hHGfYc94eOxrpv8vXU
NkWSA0zzzE30mVwY1HED0w-BTzAd2c0w8s3p8akK3T87KbYz0L8mXAbmKvVPR
zesBRynG79OLQ99PLBU2mql0S0pyCgU3g13V6ruSUHrouhw70TXblTcw1GxCKjndLROT0w
SvambFdvSQWCUozZnyCclpUW59emL7m0GS7FWPjZ29HCW4zk03VEQDaXIOp0b00YpCb
evHms7p0q996kaj3BHHdI1zBTkQs10p7110KpwFXQATr0lgzxr42EwGfmd960py
DkzraAGSdCq8796G-MjyjarzeYON1gd1GFhR2mUmmWwGcSNVYiH8ZHRSLHDn74VcD
Tz29hOxscceIFNVEF0VndHf0GmpMbzuzQ11wJ2UWb77J0vT16vaVpGzZa0MN00S4g
S0k2Lp1FkGV1v0BNMMQR9h42h39p9jglTdx48Zzvc0q4E0v122ajwvse7E2me
0lPB0v0H2Zcdgkh6PsSIRvL1+st76vQFGRO6CW9eLvQZNIbcj3RQ0DRPaNpMmutorQBYV
eDMiqecWwUE=
-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer C:

ES

Issuer L:

Valladolid

Issuer O:

DIGITEL ON TRUSTED SERVICES SLU

Issuer OU:

DIGITEL TS CERTIFICATION AUTHORITY

Issuer SERIAL NUMBER:

B47447560

Issuer CN:

DIGITEL TS QUALIFIED CA TSA GI

Subject C:

ES

Subject L:

Valladolid

Subject O:

DIGITEL ON TRUSTED SERVICES SLU

Subject 2.5.4.97:

VATES-B47447560

Subject OU:

Digitel Qualified Time Stamp Services

Subject SERIAL NUMBER:

B47447560

Subject CN:

DIGITEL TS QUALIFIED TSU RSA2048 01 G7

Valid from:

Fri Mar 10 10:40:17 CET 2023

Valid to:

Thu Mar 08 10:40:16 CET 2029

Public Key:

3082.01.22.30.0D.06.09.2A.86.48.86.F7.0D.01.01.01.05.00.03.82.01.0E.00.30.82.01.0A.02.82.01.01.00.A8.F6.E2.BC.E7.7D.CE.32.3C.73.55.67.33.90.F7.49.A5.21.ED.24.61.05.ED.00.67.5E.A7.E1.93.DD.A1.CD.64.3A.
E2.90.A9.90.C3.34.AC.73.72.79.1B.70.C1.87.3B.F5.F4.A0.5C.6E.47.AA.E7.5F.84.23.DA.0F.6F.50.5A.F9.A9.0D.22.0E.19.22.D3.73.27.4D.BD.4B.C1.F9.24.88.25.AA.15.46.9D.4B.18.CA.A9.38.F8.07.40.38.06.F3.
DA.33.32.98.A3.F7.7B.44.49.46.0D.F6.EE.80.17.A1.0D.14.CD.57.C1.99.46.8A.8B.FE.14.63.A8.EE.34.85.04.64.7E.75.C3.81.75.04.85.7E.41.19.AD.9F.CD.10.89.96.2F.78.AD.22.CE.51.23.2F.80.E2.A1.82.E6.AE.EE.E0
.F9.BC.54.E5.96.01.8B.4A.63.61.DD.75.43.A3.B5.F8.C3.1B.24.B0.90.52.60.2A.78.3F.A3.EA.06.50.4D.80.30.44.48.1E.88.77.CD.5A.44.D9.17.A9.C3.FA.13.95.7B.BF.6F.12.6D.81.55.21.5C.2C.AF.79.94.FB.E3.B2.7D.D
F.67.98.E5.ED.F1.F3.AB.E2.76.C8.5C.7.85.BC.54.13.9E.92.34.05.31.80.EF.B7.02.03.01.00.01

Basic Constraints

IsCA: false

Authority Key Identifier

90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

**Authority Info Access**  
<http://pki.digitelts.es/DIGITELTSQUALIFIEDCATSAG1.crt>  
<http://ocsp.digitelts.es>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.54225.10.1.1  
 CPS pointer: <https://pki.digitelts.es/dpc/>  
 Policy OID: 0.4.0.2042.1.2

**Extended Key Usage**  
*id\_kp\_timeStamping*

**CRL Distribution Points**  
<http://crl1.pki.digitelts.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitelts.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier**  
 16:79:94:50:42:F3:1E:08:4B:C2:DD:9E:D7:32:A4:64:04:11:85:00

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 F6:D3:2D:AB:31:27:F5:0B:88:A1:A5:36:AA:83:22:A1:73:A3:4B:82:C6:BE:CF:4B:DD:9A:5D:36:FB:49:08:04

**X509SubjectName**

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digital Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU RSA2048 01 G7

**X509SKI**

**X509 SK I**  
 FnmUUeLzHghLwt2e1zKkZAQRhQA=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time**

2023-05-22T00:00:00Z



**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** VATES-B47447560

**Subject OU:** Digitel Qualified Time Stamp Services

**Subject SERIAL NUMBER:** B47447560

**Subject CN:** DIGITEL TS QUALIFIED TSU RSA2048 01 G8

**Valid from:** Fri Mar 10 10:47:43 CET 2023

**Valid to:** Thu Mar 08 10:47:42 CET 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100ADCD38C4BEF2C2D616BA24A50A463BA734CD132337EAF2D0A6E8614334D5F0A75B17EC71ED75DDE7508D884BBF384F7FBF1AE97520E06C0E4D5E8176F006CF1A1F08985FE9888E344A3D1DA411E682DD7AB66A9589EDK13BE0E40537931AE173587487C66698A0C8DAD3E774B5096380E42DBE4482603744CD2B39FEE3B6F18E6D0D2866EA26129631780D7E534AD9D06B8919E60AE3E2244DDA031A3A4D9B8C8416990D7D46070E6B750DE11EBDCC8A3DA35DE702878D19427EECD28DEE7CA19919BC3A9FDFF1DA82550C91B126F8ED0815D462D258FD908C33326A80FDEA3A72D2C10C51DFD337144F037F90C2BC6EFD1C76BC88E1E6D6806A39A9F3EC10203010001

**Basic Constraints** IsCA: false

**Authority Key Identifier** 90:1B:DE:04:67:93:28:4C:73:D8:CA:8B:6F:8C:AA:96:B7:DC:0D:9B

**Authority Info Access**  
<http://pki.digitel.es/DIGITELTSQUALIFIEDCATSAG1.crt>  
<http://ocsp.digitel.es>

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.54225.10.1.1  
 CPS pointer: <https://pki.digitel.es/dpc/>  
 Policy OID: 0.4.0.2042.1.2

**Extended Key Usage** id\_kp\_timeStamping

**CRL Distribution Points**  
<http://crl1.pki.digitel.es/DTSQualifiedCATSAG1.crl>  
<http://crl2.pki.digitel.es/DTSQualifiedCATSAG1.crl>

**Subject Key Identifier** 67:25:CC:83:09:F4:50:6C:7A:11:6A:C6:19:9D:5F:D1:5B:A3:6F:AA

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 35:AD:EC:97:9B:5A:AE:56:1E:D4:04:4F:4D:CA:B7:86:BF:B6:51:28:35:96:96:02:55:E1:B0:80:69:39:AF:73

**X509SubjectName**

**Subject C:** ES

**Subject L:** Valladolid

**Subject O:** DIGITEL ON TRUSTED SERVICES SLU

**Subject 2.5.4.97:** *VATES-B47447560*

**Subject OU:** *Digitel Qualified Time Stamp Services*

**Subject SERIAL NUMBER:** *B47447560*

**Subject CN:** *DIGITEL TS QUALIFIED TSU RSA2048 01 G8*

**X509SKI**

**X509 SK I** *ZyXMgwn0UGx6EWrGGZ1f0Vujb6o=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-05-22T00:00:00Z*



**36 - TSP: VIAFIRMA, S.L.****TSP Name**

**Name** [ es ] *VIAFIRMA, S.L.*

**Name** [ en ] *VIAFIRMA, S.L.*

**TSP Trade Name**

**Name** [ en ] *VIAFIRMA*

**Name** [ en ] *VATES-B91052142*

**Name** [ en ] *VIAFIRMA SOCIEDAD LIMITADA*

**PostalAddress**

**Street Address** [ en ] *Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.*

**Locality** [ en ] *Tomares*

**State Or Province** [ en ] *Sevilla*

**Postal Code** [ en ] *41940*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Glorieta Fernando Quiñones, S/N. Edificio CENTRIS, planta baja, módulo 8.*

**Locality** [ es ] *Tomares*

**State Or Province** [ es ] *Sevilla*

**Postal Code** [ es ] *41940*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:psc@viafirma.com*

**URI** [ en ] *https://qtsp.viafirma.com*

**TSP Information URI**

**URI** [ en ] *https://qtsp.viafirma.com*



**Subject O:** VIAFIRMA SOCIEDAD LIMITADA

**Subject C:** ES

**Valid from:** Thu Oct 17 14:35:39 CEST 2019

**Valid to:** Thu Oct 17 14:35:39 CEST 2024

**Public Key:**  
3082 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 D0 61 7F AD 75 24 34 55 0F BB 40 E4 67 CF 33 3A 8E C1 F6 33 F6 E3 5A 88 45 D3 25 E8 03 34 14 91 DC 52 5D D9 86 3E 40 AC 12 5A AC E8 F4 93 A5 64 0E E2 9A 43 C3 70 BF E4 8A 37 1A 94 BF 8A 48 0E 5E 02 23 94 D3 DA 81 E2 57 7C B1 03 05 03 02 0A AE BD F0 10 ED 41 24 E6 3D 2E AC C2 E8 DF 64 39 76 B5 0E D4 SA 96 74 B8 D3 4D FE C3 AD 1F 42 2B AA BE A0 83 63 B1 37 00 33 19 86 F3 F5 CF 03 99 53 8D 76 3F 64 E9 51 E5 EE 7E 5E 12 03 47 F9 6A 25 26 EC 43 7D 5F BB DC 3C 3A B0 B4 09 01 EF 39 5B 0A FC 49 E 5 7B 89 5A D4 93 D3 03 BC 2E 6E CF 09 9B 83 4F 21 91 2F CE 4F F3 41 95 AD 77 BE B3 E6 D9 01 B0 2D BB 8B B0 EB 6E C6 64 1D 77 8F 16 6B 06 CF D5 EF EB 24 6A E2 21 E7 D1 75 B6 FF 92 9E 3F BA 99 A9 54 D4 BF 70 1D 6A DE CE A6 96 61 2C CD ED 62 3F 75 89 E5 FE B5 32 BA 0D EA 23 02 03 01 00 01

**Authority Info Access**  
<http://qtsp.viafirma.com/tsp/subca.crt>  
<http://qtsp.viafirma.com/ocsp>

**Subject Key Identifier**  
4A:55:48:CA:14:B0:D4:A4:39:84:6F:D3:AA:6B:C6:45:B1:ED:1F:C0

**Basic Constraints**  
*isCA: false*

**Authority Key Identifier**  
4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.34253.7.3  
CPS pointer: <http://qtsp.viafirma.com/cps>

**CRL Distribution Points**  
[http://qtsp.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp.viafirma.com/tsp/tsa_subca.crl)  
[http://qtsp1.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp1.viafirma.com/tsp/tsa_subca.crl)

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Key Usage:**  
*digitalSignature - nonRepudiation*

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
84:7E:85:86:E8:42:BD:34:C7:F5:30:8B:9C:28:73:E5:45:BE:79:CA:80:53:7F:E7:BC:6A:2C:A5:C8:26:B0:26

**X509SubjectName**

**Subject 2.5.4.97:** VATES-B91052142

**Subject CN:** VIAFIRMA TSA

**Subject OU:** VIAFIRMA QTSP

**Subject O:** VIAFIRMA SOCIEDAD LIMITADA

**Subject C:** ES

**X509SKI**

**X509 SK I** SIVlyhSw1KQ5hG/TqmvGRbHtH8A=



**Subject 2.5.4.97:** VATES-B91052142

**Subject CN:** VIAFIRMA TSA

**Subject OU:** VIAFIRMA QTSP

**Subject O:** VIAFIRMA SOCIEDAD LIMITADA

**Subject C:** ES

**Valid from:** Wed Sep 28 13:22:57 CEST 2022

**Valid to:** Wed Sep 29 13:22:57 CEST 2027

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009E9801950FBD2C9D64E0E07968AF52C701B7A42C0FF6B3C3CC8EDA5E3C0E8B9506254  
B798271740C7D6A0FA19E46C2F8E438735015432C4AD3A6A79331160289571BB651492D8153F0115DA970642DDDC69174426B57221DAD148EE53AC77DB8D8E4E8  
F7E3F4018CA7D72FE00067902B1AF3C53B5B8E87F230FBE65B1914797FB9FED398E74446932EFA494FAB4F633B84F8F86E8A9C01EC1AFEAD2FDFB95B39FFAB6  
27F624237108C30662B484F997A80510C859DC6F34DCDE363010825DDE979989D7B897924F7B3821997AE39D53EFE14D686FF6326C5C0D25577B25219B124C46  
A13D22E0A6FA0D17EFC803E0FEE3A12A5072BEC1D835FA7D50203010001

**Authority Info Access**  
<http://qtsp.viafirma.com/tsp/subca.crt>  
<http://qtsp.viafirma.com/ocsp>

**Subject Key Identifier**  
F8:1E:F7:90:D9:C2:FE:2C:A7:3E:DC:82:55:0F:49:D4:E2:CD:D1:CD

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.34253.7.3  
CPS pointer: <http://qtsp.viafirma.com/cps>

**CRL Distribution Points**  
[http://qtsp.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp.viafirma.com/tsp/tsa_subca.crl)  
[http://qtsp1.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp1.viafirma.com/tsp/tsa_subca.crl)

**Extended Key Usage**  
id\_kp\_timeStamping

**Key Usage:**  
digitalSignature - nonRepudiation

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
24:9D:7B:F9:C1:6E:BC:DA:81:45:FC:88:5A:15:04:D1:56:F0:A1:88:A2:78:F8:F6:D5:73:D2:CD:71  
:6D:AF:07

**X509SubjectName**

**Subject 2.5.4.97:** VATES-B91052142

**Subject CN:** VIAFIRMA TSA

**Subject OU:** VIAFIRMA QTSP

**Subject O:** VIAFIRMA SOCIEDAD LIMITADA



**Issuer OU:** VIAFIRMA QTSP

**Issuer O:** VIAFIRMA SOCIEDAD LIMITADA

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B91052142

**Subject CN:** VIAFIRMA TSA 003

**Subject OU:** VIAFIRMA QTSP

**Subject O:** VIAFIRMA SOCIEDAD LIMITADA

**Subject C:** ES

**Valid from:** Fri Feb 03 10:47:04 CET 2023

**Valid to:** Fri Feb 04 10:47:04 CET 2028

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100A570F1EFC2D88B4F28FA20B703D25C8B8E5EEF40DB9C3BE1B8E7D6E9A77FB301E5960  
SF8927E884F907A5BF13786A1E8D64FBEF8216886C988DA815FB95D7457C459645827628FA7C4753C68FE8C4077F84DE537324D5A435936EC1658FD22ED0AFA8A40  
C534FF1D197069A3AE12AE8DDB908EAS85D6E8D0E.CB.EA.1D35F5E0FE.C48A.7F626161C47E.EF76.C70A.220B.E857C9EC.67C0.F733.5A.5717.AF67.D909E.56C2.40BB.9679.8F.E4.78.  
D06F.10662E.DC.B48A.9F1101.08.C0.96.D0.43.B0.4C.FC.83.9B.CC.EF.06.4F.B7.37.C2.9D.03.4A.98.82.BC.AE.00.FC.4D.98.95.DE.27.3F.9B.C4.90.8B.D8.61.F5.22.A1.B1.CB.D4.92.85.EF.8C.E0.B6.AA.F6.DF.22  
D8.E9.8A.8E.06.98.32.0D.96.BC.FC.0C.8B19.46.E5.A3.67.80.76.B0.86.57.9C.3D.DC.A7.C1.83.88.0D.10.A7.0B.26.16.D4.4C.46.D5.6D.8F.9F.37.2D.F7.0F.EC.BA.E0.A5.56.F9.AD.D5.4D.89.4F.6F.F7.4D.9C.C3.B9.4  
5.BB.AE.1D.74.9E.A9.F5.6A.AF.40.59.41.54.64.B8.66.BA.27.DC.77.EA.2A.57.37.0C.24.01.D9.DF.11.55.34.E5.AD.FF.4F.23.00.B1.84.71.1C.SD.B7.F9.8B.68.69.19.7B.8E.AD.7E.9C.8D.36.A3.A1.0E.E2.3A.72.A  
3.D9.49.9C.2D.0A.A2.87.1E.11.C0.33.A7.50.19.D6.D0.94.1C.05.9C.C9.0C.EF.0A.EE.7C.04.F1.55.B9.4B.B8.AF.31.05.E5.18.95.5A.64.C5.8E.6B.0C.C4.AA.FF.6C.77.8D.0D.4D.5A.4C.D3.0D.57.F0.FE.23.45.D2.B4.85.  
6A.48.D7.D0.C5.16.9C.F9.85.88.C6.BF.9E.B3.7A.BB.08.13.2D.9A.09.C2.DD.09.C9.B3.E5.C5.62.8E.E9.45.6D.A4.B8.9E.02.1C.34.BA.0F.1F.AC.D6.D6.EE.CD.E1.A8.B7.6C.2F.F6.94.F1.D7.54.6B.E7.72.B0.4E.18.AE.  
BD.D7.39.A0.01.9F.1E.93.AD.E1.8B.3D.2E.DA.7A.C2.74.D3.94.A2.F2.4B.80.09.02.03.01.00.01

**Authority Info Access**  
<http://qtsp.viafirma.com/tsp/subca.crt>  
<http://qtsp.viafirma.com/ocsp>

**Subject Key Identifier**  
3D:E9:46:3F:C9:A6:E6:C6:5D:0A:F5:95:85:3D:11:D5:2A:7F:13:C2

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
4A:C8:02:04:18:43:C2:BD:7F:03:90:B8:8F:F7:13:C8:DC:BE:BE:26

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.34253.7.3  
CPS pointer: <http://qtsp.viafirma.com/cps>

**CRL Distribution Points**  
[http://qtsp.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp.viafirma.com/tsp/tsa_subca.crl)  
[http://qtsp1.viafirma.com/tsp/tsa\\_subca.crl](http://qtsp1.viafirma.com/tsp/tsa_subca.crl)

**Extended Key Usage**  
id\_kp\_timeStamping

**Key Usage:**  
digitalSignature - nonRepudiation

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
1A:2B:FC:30:34:EE:CF:4C:E1:71:DF:3A:D6:A1:5C:D4:49:2D:51:EB:31:40:DF:51:9E:38:5C:18:D  
B:D0:7F:55

X509SubjectName

**Subject 2.5.4.97:** *VATES-B91052142*

**Subject CN:** *VIAFIRMA TSA 003*

**Subject OU:** *VIAFIRMA QTSP*

**Subject O:** *VIAFIRMA SOCIEDAD LIMITADA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *PelGP8mm5sZdCvWVhT0R1Sp/E8I=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-03-28T00:00:00Z*



**37 - TSP: VALIDATED ID, S.L****TSP Name**

**Name** [ es ] *VALIDATED ID, S.L*

**Name** [ en ] *VALIDATED ID, S.L*

**TSP Trade Name**

**Name** [ en ] *VALIDATED ID SL*

**Name** [ en ] *VATES-B65750721*

**Name** [ en ] *Validated ID SL*

**PostalAddress**

**Street Address** [ en ] *C/ Sepúlveda, 143 pl. 4ª - 2º*

**Locality** [ en ] *BARCELONA*

**State Or Province** [ en ] *BARCELONA*

**Postal Code** [ en ] *08011*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ Sepúlveda, 143 pl. 4ª - 2º*

**Locality** [ es ] *BARCELONA*

**State Or Province** [ es ] *BARCELONA*

**Postal Code** [ es ] *08011*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:tsp@validatedid.com*

**URI** [ en ] *https://validatedid.com*

**TSP Information URI**

**URI** [ en ] *validatedid.com*



**Subject OU:** *VALIDATED ID TSP*

**Subject O:** *VALIDATED ID SL*

**Subject L:** *BARCELONA*

**Subject C:** *ES*

**Valid from:** *Tue Nov 26 18:45:11 CET 2019*

**Valid to:** *Fri Nov 26 18:45:11 CET 2027*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100CAF1D8EA3C9570238D8D19AE2F1D2AE935E446ADADA4625E3B2E2D6F4056B74230687  
D1130A83D4C9053096271581759E04E760D2F922DA8F81D35D8432AD0D1E2B84AE68496DCD29432AD6B7BA86AC464F916D03AB14EFC1E0993D1A2627B9AD2F  
7D3E2B155B1903F1D8B39C4226642771251202EDDFB5347A7CF00455E952BAD3E1568A3B5F5C448EF99A0782B26B4E89FAF7BC894758385FE355C4009E23C2DC891C  
69A3D4C0162AB2EF45E7BEAF94469534765E7A8ED329BD436C34CC36F3A8ABF9ED95C00254BBFAA4C356A321CF0A7DF8BD7CA777CD053170C15DCE5F7D.EB  
DC52531584B2AB8B17E42CFD990149CD9D30DE85F6F9121D72D94B1B0203010001

**Authority Info Access**  
*http://ocsp1.uanataca.com/public/pki/ocsp/*  
*http://ocsp2.uanataca.com/public/pki/ocsp/*

**Subject Key Identifier**  
*E8:51:4E:DD:BC:CC:78:9C:11:37:26:F3:CA:D8:98:E1:B8:58:9E:97*

**Basic Constraints**  
*isCA: false*

**Authority Key Identifier**  
*7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.2.5*  
*CPS text: [Certificado de sello de tiempo electrónico.]*  
*CPS pointer: https://www.uanataca.com/public/cps/*  
*Policy OID: 0.4.0.2042.1.2*

**CRL Distribution Points**  
*http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl*  
*http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl*

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Subject Alternative Name**  
*tsp@validatedid.net*

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*E3:00:17:A1:84:38:64:F7:C5:AE:60:4C:E2:12:61:39:C2:11:B4:D2:FE:F8:3E:F1:3E:DE:8F:72:57:B  
6:57:B3*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B65750721*

**Subject CN:** *VALIDATED ID QUALIFIED TSU01*

**Subject OU:** *VALIDATED ID TSP*

**Subject O:** *VALIDATED ID SL*

**Subject L:** *BARCELONA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *6FFO3bzMeJwRNybytiY4bhYnpc=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2020-04-28T00:00:00Z*

## 37.2 - Service (granted): Qualified Certificates issued by Validated ID Subordinate CA 01

**Service Type Identifier** *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[en] Qualified Certificates issued by Validated ID Subordinate CA 01*

**Name** *[es] Certificados Cualificados emitidos por Validated ID Subordinate CA 01*

**Service digital identities**

**Certificate fields details**

**Version:** *3*

**Serial Number:** *2673564476656545333*



**Issuer Alternative Name** *tsp@validatedid.com*

**Subject Alternative Name** *tsp@validatedid.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <https://www.validatedid.com/tsp>*  
*CPS text: [Validated ID Subordinate CA Certificate - <https://www.validatedid.com>]*

**CRL Distribution Points**  
*[http://crl1.validatedid.com/tsp/crl/arl\\_validatedid.crl](http://crl1.validatedid.com/tsp/crl/arl_validatedid.crl)*  
*[http://crl2.validatedid.com/tsp/crl/arl\\_validatedid.crl](http://crl2.validatedid.com/tsp/crl/arl_validatedid.crl)*

**Subject Key Identifier** *26:4E:8E:6F:4A:52:54:00:83:28:70:CF:F1:88:B0:51:25:39:55:57*

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A8:3D:44:88:25:5C:46:9F:66:26:E3:71:1C:69:22:9B:DC:8A:DA:56:7C:F2:9B:2E:A6:5F:AD:19:29:28:31:C2*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Barcelona*

**Subject O:** *Validated ID SL*

**Subject OU:** *TSP - Validated ID*

**Subject CN:** *Validated ID Subordinate CA 01*

**Subject 2.5.4.97:** *VATES-B65750721*

**X509SKI**

**X509 SK I** *Jk6Ob0pSVACDKHDP8YiwUSU5VVc=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-05-31T00:00:00Z*

**37.2.1 - Extension (not critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 37.2.2 - Extension (not critical): additionalServiceInformation

#### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

### 37.2.3 - Extension (not critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description [ en ] undefined.  
[ es ] undefined.

#### Criteria list assert=atLeastOne

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.1.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.2.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.3.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.4.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.5.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.6.3>

Policy Identifier:

Identifier [ OIDsURN ] <urn:oid:1.3.6.1.4.1.54932.2.8.3>

### 37.3 - Service (granted): Qualified timestamps issued by Validated ID Qualified TSU02

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>





**Subject CN:** *Validated ID Qualified TSU02*

**Subject 2.5.4.97:** *VATES-B65750721*

**Valid from:** *Thu Oct 28 14:25:11 CEST 2021*

**Valid to:** *Wed Oct 28 13:25:11 CET 2026*

**Public Key:**  
30820122300D06092A864886F70D010105000382010F003082010A0282010100F0AA265FC20F8BE1415C5AAB3863698B4C4C18F4963FF948B035D4EFECDFDA8ABB03  
4E161054CC1D461FDB9BEAE7023B0D3974BE9563421C43F820D68A207C71A6B60882A45F34106B E936ED2BDD5651AA6FE3C5127ADC8A90FDA78CEA295FC3910DB  
73528E155FDF945F95A34822A6D210309210D29FB9CD3751B15C0D46019CFF99B498003FB563C4038D6417D123332D8A9321D9BA5A8E7CC EE4238FC E6E2E72ADE3  
AEE32C404E50D76F1494C68950747B923188BE47A910C7784654EE1280BF3D5B868214AE C20B7B69B41838B4972FBBC0B108B79B68FC15E8F7EDA2FF1E0B22499  
EB58678CBC2B1220582405692821382D10FD1C9761058981FC CD0203010001

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Authority Info Access**  
[https://www.validatedid.com/tsp/tsp\\_certificates/validatedid\\_ca.crt](https://www.validatedid.com/tsp/tsp_certificates/validatedid_ca.crt)  
<http://ocsp1.validatedid.com/tsp/ocsp/>  
<http://ocsp2.validatedid.com/tsp/ocsp/>

**Subject Key Identifier** *59:D3:96:B6:97:10:95:1C:40:4A:F3:26:F1:C1:11:C8:F2:CA:1F:C6*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier** *26:4E:8E:6F:4A:52:54:00:83:28:70:CF:F1:88:B0:51:25:39:55:57*

**Issuer Alternative Name** *tsp@validatedid.com*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.3*  
*Policy OID: 1.3.6.1.4.1.54932.3.10*  
*CPS pointer: https://www.validatedid.com/tsp*  
*CPS text: [Qualified time stamp certificate]*

**CRL Distribution Points**  
<http://crl1.validatedid.com/tsp/crl/validatedid.crl>  
<http://crl2.validatedid.com/tsp/crl/validatedid.crl>

**Extended Key Usage** *id\_kp\_timeStamping*

**Subject Alternative Name** *tsp@validatedid.com*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *E8:68:AE:7E:58:0C:5F:6A:C7:78:D9:FE:50:AC:5E:A7:AA:A1:93:B4:29:BC:46:67:44:73:2D:F7:6  
D:0D:00:B6*

**X509SubjectName**

**Subject C:** *ES*

**Subject L:** *Barcelona*

**Subject O:** *Validated ID SL*

**Subject OU:** *TSP - Validated ID*

**Subject CN:** *Validated ID Qualified TSU02*

**Subject 2.5.4.97:** *VATES-B65750721*

**X509SKI**

**X509 SK I** *WdOWtpcQIRxASvMm8cERyPLKH8Y=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-05-31T00:00:00Z*

**38 - TSP: ENTRUST EU SL****TSP Name**

<b>Name</b>	[ en ]	<i>ENTRUST EU SL</i>
<b>Name</b>	[ es ]	<i>Entrust Datacard Europe S.L.U.</i>

**TSP Trade Name**

<b>Name</b>	[ en ]	<i>VATES-B81188047</i>
<b>Name</b>	[ en ]	<i>Entrust Datacard Europe S.L.</i>
<b>Name</b>	[ es ]	<i>Entrust Datacard Europe S.L.</i>
<b>Name</b>	[ en ]	<i>Entrust Datacard Europe, S.L.</i>
<b>Name</b>	[ es ]	<i>Entrust Datacard Europe S.L.U.</i>
<b>Name</b>	[ en ]	<i>Entrust Datacard Europe S.L.U.</i>
<b>Name</b>	[ en ]	<i>Entrust EU, S.L.</i>
<b>Name</b>	[ en ]	<i>Entrust EU</i>

**PostalAddress**

<b>Street Address</b>	[ en ]	<i>P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ</i>
<b>Locality</b>	[ en ]	<i>Pozuelo de Alarcón</i>
<b>State Or Province</b>	[ en ]	<i>Madrid</i>
<b>Postal Code</b>	[ en ]	<i>28233</i>
<b>Country Name</b>	[ en ]	<i>ES</i>

**PostalAddress**

<b>Street Address</b>	[ es ]	<i>P.E. La Finca. Paseo del Club Deportivo, 1 Bloque 3 BJ</i>
<b>Locality</b>	[ es ]	<i>Pozuelo de Alarcón</i>
<b>State Or Province</b>	[ es ]	<i>Madrid</i>
<b>Postal Code</b>	[ es ]	<i>28233</i>
<b>Country Name</b>	[ es ]	<i>ES</i>



**Issuer OU:** (c) 2009 Entrust, Inc. - for authorized use only

**Issuer OU:** See [www.entrust.net/legal-terms](http://www.entrust.net/legal-terms)

**Issuer O:** Entrust, Inc.

**Issuer C:** US

**Subject C:** ES

**Subject O:** Entrust Datacard Europe S.L.

**Subject 2.5.4.97:** VATES-B81188047

**Subject CN:** Entrust Certification Authority - QTSP1

**Valid from:** Fri Jul 26 20:31:45 CEST 2019

**Valid to:** Tue Nov 26 20:01:45 CET 2030

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100DC EE40BEE E3742945E371F20E0215FE92680553C3E00528EAC E6AC4A79DB720CD4A20  
28154D0B094320E F74C B74A 80800A AF521C BA438E4985121216EF18532B9E5D F317A1A6DF F762CA1C B7C2888132E08C607A2D48E950A932ED76B9DBE91033EDC777  
8B409AD6AE75952ED978D2C19C053988DEB0264F0FB3DE88AE74450800B23449B4CB21C42FDD83E9A5BEF89A8C76AC57F31A1CFE9B300A C44E5D5B39E9FCBF1079  
7D5B42D6E2779A08983C211659EFA49280BEBC72117E655A5F31E7B053E1F498855E623F5FC563DCBB63405E994FF16799E24C98626D0BDE271F6E3419DE6B88F859  
0B0099A5410CED6115EE E0F4A25667DE29E5DBD6FA23B2B4A50203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: <http://www.entrust.net/rpa>*

**Authority Info Access** *<http://ocsp.entrust.net>*

**CRL Distribution Points** *<http://crl.entrust.net/g2ca.crl>*

**Subject Key Identifier** *1C:AD:3F:9C:D7:2D:22:19:A1:9C:4B:E9:DA:F1:2A:33:F7:FB:BA:0D*

**Authority Key Identifier** *6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *68:1E:BC:18:22:B0:79:B9:7E:04:04:E4:68:7D:9B:6C:0C:08:92:C8:20:F5:57:38:A2:82:AA:E6:25:2  
9:BD:D8*

**X509SubjectName**

**Subject C:** ES

**Subject O:** Entrust Datacard Europe S.L.

**Subject 2.5.4.97:** VATES-B81188047

**Subject CN:** Entrust Certification Authority - QTSP1

## X509SKI

**X509 SK I** HK0/nNctIhmhnEvp2vEqM/t7ug0=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2020-07-28T00:00:00Z

### 38.1.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

### 38.2 - Service (granted): Qualified Certificates issued by “Entrust Certification Authority - ES QSig1”

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [en] Qualified Certificates issued by “Entrust Certification Authority - ES QSig1”

**Name** [es] Certificados cualificados emitidos por “Entrust Certification Authority - ES QSig1”

#### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 91144490788361283369824551057333035359



**Thumbprint algorithm:** SHA-256

**Thumbprint:** B2:87:4B:58:8A:94:03:47:98:31:9D:5D:32:9D:B2:65:F8:3A:47:F3:15:BA:58:31:A4:97:0C:B5:71:66:D5:94

### X509SubjectName

**Subject C:** ES

**Subject O:** Entrust Datacard Europe, S.L.

**Subject 2.5.4.97:** VATES-B81188047

**Subject CN:** Entrust Certification Authority - ES QSig1

### X509SKI

**X509 SK I** WIMiimEwqQ3q1UOX05g7IR4ubQI=

### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

### Status Starting Time

2021-07-01T01:00:00Z

### 38.2.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

### 38.3 - Service (granted): Qualified Certificates issued by “Entrust Certification Authority - ES QSeal1”

#### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### Service Name

**Name** [en] Qualified Certificates issued by “Entrust Certification Authority - ES QSeal1”

**Name** [es] Certificados cualificados emitidos por “Entrust Certification Authority - ES QSeal1”

#### Service digital identities

#### Certificate fields details





**Certificate Policies** Policy OID: 2.5.29.32.0  
 CPS pointer: <http://www.entrust.net/rpa>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 17:01:DE:38:12:4C:44:58:F3:2B:88:AE:7E:62:AC:15:87:6C:42:7A:3A:D3:BB:AE:8F:D1:47:9F:F0:00:30:F3

**X509SubjectName**

**Subject C:** ES

**Subject O:** Entrust Datacard Europe, S.L.

**Subject 2.5.4.97:** VATES-B81188047

**Subject CN:** Entrust Certification Authority - ES QSeal1

**X509SKI**

**X509 SK I** VoAVI5Vxf+ctkNDNBjpPZ2N9PXU=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time** 2021-07-01T01:00:00Z

**38.3.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**38.4 - Service (granted): Qualified Certificates issued by "Entrust Certification Authority - ES QSig2"****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
 [es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by "Entrust Certification Authority - ES QSig2"



**Authority Info Access** *http://ocsp.entrust.net*

**CRL Distribution Points** *http://crl.entrust.net/dsr1.crl*

**Extended Key Usage** *Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: https://www.entrust.net/rpa*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *46:71:FD:EA:D3:C5:B3:2D:83:4B:36:59:1D:41:49:6F:CB:8A:0D:B7:D4:F9:F4:CB:9D:34:EA:BE:09:47:EE:87*

**X509SubjectName**

**Subject CN:** *Entrust Certification Authority - ES QSig2*

**Subject 2.5.4.97:** *VATES-B81188047*

**Subject O:** *Entrust EU, S.L.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *9VYNadfaasnYyaIjbnS+24DGFwA=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2022-07-21T00:00:00Z*

**38.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**38.4.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne**



**Subject C:** ES

**Valid from:** Tue Nov 16 01:00:00 CET 2021

**Valid to:** Sat Dec 29 01:00:00 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C3FBDS89DA7E6AFC56E9325546FAAA7F6C2F08DB9FE3853F5F64B653E7EC2369B08A6AF8277CF046AFFE05865AAD1414685FBFBDB400F4A31A90BD23437ADE8EF38EBE12D2B48997B2C078DCCAT803D0D5E76F6312344AA7ED8543EE140DDF91E1E7E7FA8812EB71733EFA04A7C45A2D2B733BA6FAB59EF57DF7F35F37E159C192FC2260AC851B2EBF2CB9C6EFA15C80A9E78798AEA9C1017E7E7D8FA4CB19FDB6939D9C0C2F882A363CD27DD116737E6DEE144751DC5AA9A92E6B8B8DAFBCBE6F16DE40B05410957C316C3C99A58CA1031B56700B7C67482C0A8F21C1FE6CB8DA9053608B330273012BD913274745E7E9475C1DECS998F02301C96DF1CDA DC1D5AAC0BB7E2807AE1A8D39D54EE954F5C94B7037AD88035C19AF4977F96A45255BF19A897989E9943AB97E1104C702910EB160F1FE2D88CDFD06DA814B23E724E60A84423464DF071B90D5254B23119E7781E1EA68D92B2E4687B6DEDC3A83556334B369601C14D0B837AEF3F3043C6CE2099B2A1E01084C39F816B84599D4B7F57E7216C119B60E6CA7EC4D04583E092A0216BF49A01448D94A512E2C6F15BE02FE02F48A14C782823B95754B8722570F062F848DDFBEF7AA6692992F5981E2F9527E95C2F1DC7EA122763EBECF9F12B31AD157F1861AF0D34708092F1934A4E40C1E55A01ECEED1192F630B0AA9690EC18552AA753E72ACAAAF1C988F5DD0203010001

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 36:18:25:6E:D9:5D:F7:10:05:7C:27:2E:B8:EC:FA:41:4A:60:ED:1F

**Authority Key Identifier** A6:65:41:81:F2:5B:87:05:6A:DD:FD:8A:54:4E:8F:98:7B:DC:23:B8

**Authority Info Access** <http://ocsp.entrust.net>

**CRL Distribution Points** <http://crl.entrust.net/dsr1.crl>

**Extended Key Usage** Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.12

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.entrust.net/rpa>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 8C:31:D9:37:51:28:D4:B1:07:F0:76:78:EE:BF:FF:2C:CA:26:A4:CA:BB:46:2F:25:7F:31:A3:6F:E7:BC:E1:04

**X509SubjectName**

**Subject CN:** Entrust Certification Authority - ES QSeal2

**Subject 2.5.4.97:** VATES-B81188047

**Subject O:** Entrust EU, S.L.

**Subject C:** ES

**X509SKI**

**X509 SK I** Nhg1btld9xAffCcuuOz6QUpg7R8=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2022-07-21T00:00:00Z



**Subject CN:** *Entrust Certification Authority - ES QWAC2*

**Subject 2.5.4.97:** *VATES-B81188047*

**Subject O:** *Entrust EU, S.L.*

**Subject C:** *ES*

**Valid from:** *Tue Nov 16 01:00:00 CET 2021*

**Valid to:** *Sun Dec 01 01:00:00 CET 2030*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C6B2298DF6DA088269EEA1444B8B865A46BBE41D689B838DD602947EFBD A6F06DE  
29012F54B428805008A7B91897D4E4E4B47064F3176C055821F9DDCDA1496704E22764E0A75FBC5E670B8603FE3508F6BF0402D271FD CD738D2063FE0E DD E1  
18279CE7F969B73259FB1A2164C1D5FD91FA3BA31A61A019C95D0A81CB54E5F6C47D276959F9C72DD7704A9CF4B2CB41AFAD0618F83E5D280961DE71F260643E  
05A3ED0E7C63A079B37844E2DCD4D2D19AF05F27AD8A5B7FE439187558EA370E465C9482A89BE86F90A0E DD6D75F2C69AD620F7F30A432BE4D492E30B3694F9  
F324770DE49F707A C9C587566F672A41A07F7379F71D5C211706950203010001

**Basic Constraints** *IsCA: true - Path length: 0*

**Subject Key Identifier** *41:CF:AE:2B:1D:63:3B:CB:4C:F5:90:44:79:B6:5A:24:89:DF:92:9C*

**Authority Key Identifier** *6A:72:26:7A:D0:1E:EF:7D:E7:3B:69:51:D4:6C:8D:9F:90:12:66:AB*

**Authority Info Access** *http://ocsp.entrust.net*

**CRL Distribution Points** *http://crl.entrust.net/g2ca.crl*

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: https://www.entrust.net/rpa*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *C9:7F:2F:6E:6A:8A:DB:6E:CF:E4:97:8F:08:CA:8F:6F:01:23:A9:47:84:52:2B:61:0A:DF:6A:B5:14  
:39:FC:62*

**X509SubjectName**

**Subject CN:** *Entrust Certification Authority - ES QWAC2*

**Subject 2.5.4.97:** *VATES-B81188047*

**Subject O:** *Entrust EU, S.L.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Qc+uKxIjO8tM9ZBEebZaJInfkpw=*





**Issuer C:** US

**Subject CN:** Entrust Certification Authority - ES QTS1

**Subject 2.5.4.97:** VATES-B81188047

**Subject O:** Entrust EU, S.L.

**Subject C:** ES

**Valid from:** Mon Oct 03 17:12:28 CEST 2022

**Valid to:** Sat Dec 29 01:00:00 CET 2040

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C507DF10A18332E94B62121052355905C13E4B4FAE7770CD A28003C0DFCFDA662F693  
29551F0D3C11B3E5B12E554893DAF4F010E0B1DCD2670383081C8D8665C7DB49B1457EB61B3CB42A15A146FE6C68D4A598730545B06E12184C9F7488815E3B54  
0B979367C5814B0229DDDCD22082C0BFAD07FC18D879110C3E9EF130E0DD02B444DC66849A0AE9323E6ED35B5E8B C680B09C3D68B9B96095BE22D45C6F9664F44B  
F1DE685BD227DCFA2FBDAD0C11894134A1F4C4E2811517A071134E5B97176E C62608F315C20A5FA2C884760BCA4CDE096D02815481ECB5C7AA751E C98F7EADFF96B8  
D6594EAE46DE0F717B39DBDA95E24BDD20EC14B87FBED2CE88968B5B9BCD6742287C93E55896F3173C6C9E31AEC237D03979FB03F1ED347A005418F8124P6203  
C6FA3FC93455AEB4938FDD6A1D82AE28DD5CA53F24AC8A8E11E789CD3B5421A2FDBD1CD086F75AD14F4E432F1A6B37C618C98E1B8237DCD6D8A221DEE471490  
05D17B2BA88F3CAE0A4B88E0DFC747F658F1619B76F20DD897C35E4B548237593C57689FA7601BF0349DF6B8884A3E0CF626C8EFA7B33634B4A38E31E6BE9F8  
302F2D252913B0C0344F69ED77E88C363A2AA073FD246F1F0F3F5F0A87C3375125F324AC4AFB2C4D75CEB76AFAD989455B9D4A6663AEBD8BB A71C50F382D5E3A  
D6EC56D560A3DF9129E5A9D2849EC465FEC6135C0F92D0203010001

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 69:63:82:CA:C2:F1:11:9A:71:43:32:85:8B:AE:37:CA:96:76:BE:80

**Authority Key Identifier** A6:65:41:81:F2:5B:87:05:6A:DD:FD:8A:54:4E:8F:98:7B:DC:23:B8

**Authority Info Access** <http://ocsp.entrust.net>

**CRL Distribution Points** <http://crl.entrust.net/dsr1.crl>

**Extended Key Usage** id\_kp\_timeStamping

**Certificate Policies** Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.entrust.net/tpa>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 25:3F:46:3F:B1:9E:06:D1:88:A1:F8:1A:B6:A3:CA:78:C9:35:2B:08:DC:94:DD:74:CF:05:33:68:09:36:38:12

**X509SubjectName**

**Subject CN:** Entrust Certification Authority - ES QTS1

**Subject 2.5.4.97:** VATES-B81188047

**Subject O:** Entrust EU, S.L.

**Subject C:** ES

**X509SKI****X509 SK I***aWOCysLxEZpxQzKFi643ypZ2voA=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2023-07-04T00:00:00Z***Scheme Service Definition URI****URI***[en]**https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\_Entrust.aspx***URI***[es]**https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/TSU\_Entrust.aspx*

## 39 - TSP: EVICERTIA S.L.U.

### TSP Name

**Name** [ en ] *EVICERTIA S.L.U.*

**Name** [ es ] *EVICERTIA S.L.U.*

### TSP Trade Name

**Name** [ en ] *Evicertia*

**Name** [ es ] *Evicertia*

**Name** [ en ] *VATES-B86021839*

**Name** [ es ] *VATES-B86021839*

**Name** [ en ] *EVIDENCIAS CERTIFICADAS S.L.*

**Name** [ en ] *EVICERTIA, SL*

### PostalAddress

**Street Address** [ es ] *C/Lagasca, 95*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28006*

**Country Name** [ es ] *ES*

### PostalAddress

**Street Address** [ en ] *C/Lagasca, 95*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28006*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *mailto:info@evicertia.com*



**Issuer OU:** TSP-UANATACA

**Issuer O:** UANATACA S.A.

**Issuer L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B86021839

**Subject CN:** EVITSU-QE1A

**Subject OU:** EVICERTIA CLOUD QUALIFIED TSA QE1

**Subject O:** EVIDENCIAS CERTIFICADAS S.L.

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Wed Nov 20 11:28:35 CET 2019

**Valid to:** Sat Nov 20 11:28:35 CET 2027

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100ED46D553E898514D212F861066F33174837D1FA7D487E2A177FE19BCFBAD49387FC4BDAC335B77F8ECE71AC3018A8970B861A94F07C16C8F66445E2F0A0257593DC781F385FBD423BFB7E69D88A84E4890A328A718751095E0E07CE5C26AB059314A715C178FA4E73828AED86AA1C19909827130F11B445E73C8AE03EAABAE4C2B80641AC631B26DD18BBD2B5DB25B07A71159CCD2375C8CCECA90FC141C07DF2C0426B250B88C8DC87B0EC750911894A8CEE30A0C0559DFF2BD9B0DE4B1A9C165995341426650766EFA3765D769F9191D310D2DB9857A88507B2F4F93BC574B4FD8C4A9BBD1505337F8C3C87D5A9068E9DFF1C1ED7E99B4DA21E7BE297EB90203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
44:2C:E2:48:B9:CB:2E:62:B2:B5:92:28:47:9F:34:CA:A6:29:D3:47

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47286.2.5  
CPS text: [Certificado de sello de tiempo electrónico.]  
CPS pointer: <https://www.uanataca.com/public/cps/>  
Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Subject Alternative Name**  
[info@evicertia.com](mailto:info@evicertia.com)

**Key Usage:**  
digitalSignature

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *35:2C:E0:7F:3D:6F:31:AC:2E:48:4F:82:66:BD:4A:6A:1E:ED:1F:B8:AC:E9:7D:39:19:DD:8C:D4:47:D6:D5:DF*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B86021839*

**Subject CN:** *EVITSU-QE1A*

**Subject OU:** *EVICERTIA CLOUD QUALIFIED TSA QE1*

**Subject O:** *EVIDENCIAS CERTIFICADAS S.L.*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *RCziSLnLLmKytZIoR580yqYp00c=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-07-28T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**39.2 - Service (granted): Qualified timestamps issued by EVITSU-QE1B****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*

*[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*

**Service Name**

**Name** *[en] Qualified timestamps issued by EVITSU-QE1B*

**Name** *[es] Sellos de tiempo cualificados emitidos por EVITSU-QE1B*





**Public Key:**

30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:A3:F1:18:95:1B:02:FC:1C:DE:72:6D:BE:83:D8:3D:81:58:AB:B3:0B:8F:14:6D:34:8A:7B:88:CC:C5:2F:79:4A:4D:67:  
 93:AE:7A:55:31:2F:4D:6E:80:91:99:8D:97:DC:13:ED:8C:0D:20:48:13:59:A2:A0:D4:00:1F:B1:06:D8:FE:C6:A6:C2:AE:41:38:0D:00:3C:2B:8F:08:DB:9B:6C:D8:D5:80:3C:02:16:6A:A7:A6:7E:E2:5E:DC:ES:DC:72:D1:5F:3:  
 A:5C:BA:30:03:73:D4:57:7E:12:62:F1:EE:5C:83:D9:EF:8F:02:BB:7C:02:7A:80:0A:0E:4B:C3:C8:0E:43:0B:0D:FA:57:24:CC:30:13:FD:C2:53:29:8C:12:E6:9E:05:31:29:A5:79:F0:0A:7E:ED:4A:B6:9D:F7:16:72:64:7:  
 E:61:11:13:BA:A6:7B:12:8E:34:BD:9C:61:7E:46:89:30:58:63:EA:65:ED:E7:94:00:C6:5D:14:ES:D0:8C:83:F3:DE:07:32:6F:75:13:C1:29:EB:22:DF:3D:B4:AB:98:AB:8F:EB:F1:63:4B:D1:AD:1B:CE:71:3E:D2:2A:CB:06:7E:2:  
 9:CC:2F:66:87:28:05:AF:83:8E:86:12:11:C4:2E:3E:68:06:FE:EC:97:74:B7:3F:C6:DA:AF:47:02:03:01:00:01

**Authority Info Access**

<http://ocsp1.uanataca.com/public/pki/ocsp/>

<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**

26:95:95:24:2F:8A:90:E2:84:E3:F7:6B:E7:43:A3:47:3D:D0:24:DA

**Basic Constraints**

isCA: false

**Authority Key Identifier**

7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.47286.2.5

CPS text: [Certificado de sello de tiempo electrónico.]

CPS pointer: <https://www.uanataca.com/public/cps/>

Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**

<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>

<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>

**Extended Key Usage**

id\_kp\_timeStamping

**Subject Alternative Name**

info@evicertia.com

**Key Usage:**

digitalSignature

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

63:F3:67:59:42:A9:AB:49:5A:AA:5F:46:36:BD:FE:60:EA:7A:98:68:A9:6C:4A:5B:A5:34:2E:D8:F  
 7:26:3B:5E

**X509SubjectName****Subject 2.5.4.97:**

VATES-B86021839

**Subject CN:**

EVITSU-QE1B

**Subject OU:**

EVICERTIA CLOUD QUALIFIED TSA QE1

**Subject O:**

EVIDENCIAS CERTIFICADAS S.L.

**Subject L:**

MADRID

**Subject C:**

ES

**X509SKI****X509 SK I**

JpWVJC+KkOKE4/dr50OjRz3QJNo=



**Issuer OU:** *Certificados Cualificados*

**Issuer O:** *Firmaprofesional S.A.*

**Issuer C:** *ES*

**Subject CN:** *EVICERTIA, SL*

**Subject SERIAL NUMBER:** *B86021839*

**Subject 2.5.4.97:** *VATES-B86021839*

**Subject O:** *EVICERTIA, SL*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**Valid from:** *Thu Apr 29 17:53:37 CEST 2021*

**Valid to:** *Tue Apr 28 17:53:36 CEST 2026*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100C62F0F842EA3F45E9AE4F17E9BEA36BE80CD601A66348D0858DF4742482A805606D7  
A756E1B56F8F2A360439E5285CF09E675F9758F560C5694C9B6BA6CB3F1EB91B7D55A47BA8629626F90E0C8680EBCA878405A856F2B12D927210E46B7AFEE233F3F1  
E2B9198B4654D2514231DF82034F6AA494B4FBF8428981DA10D5989FB6F0B586C0FA1F7502C63C215F4868F9E7039A145625136A8B86F8EBBDB7EC80CF33A0E48601A  
39E96B822D8A104CC4F2FD26EC7C81CC38D353E4E854E0E6BC1250F0EB4699840EE44A4CC5B7C64CACE8B4F48FAE7872C6773136D9462C4E2F320ED6742DF97DD  
3971FC8BD58E58DC7D6D40637644FEBCC8362F3D0D3CCFF10203010001

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *8C:71:CC:93:07:6F:D1:D5:86:68:7D:82:3A:41:D9:4C:02:F8:96:5D*

**Authority Info Access**  
*http://crl.firmaprofesional.com/cualificados.crt*  
*http://ocsp.firmaprofesional.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.13177.10.1.10.2*  
*CPS pointer: http://www.firmaprofesional.com/cps*  
*CPS text: [Éste es un Certificado Corporativo de Sello Empresarial cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona]*  
*Policy OID: 0.4.0.194112.1.1*

**Extended Key Usage** *id\_kp\_clientAuth*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://crl.firmaprofesional.com/cualificados.crl*

**Subject Key Identifier** *7E:2B:34:4C:EE:A3:59:9D:A5:4D:75:C4:0C:4B:48:9A:CB:0B:D4:67*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 73:AE:3B:30:3D:B1:91:7D:16:FE:1D:FF:54:06:C8:E0:E8:3A:7D:D3:CC:9F:A0:39:00:FE:4E:9C:08:D6:28:F4

### X509SubjectName

**Subject CN:** EVICERTIA, SL

**Subject SERIAL NUMBER:** B86021839

**Subject 2.5.4.97:** VATES-B86021839

**Subject O:** EVICERTIA, SL

**Subject ST:** MADRID

**Subject C:** ES

### X509SKI

**X509 SK I** fis0TO6jWZ2ITXXEdeImssL1Gc=

### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

### Status Starting Time

2022-12-15T00:00:00Z

### Scheme Service Definition URI

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

### 39.3.1 - History instance n.1 - Status: granted

#### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

#### Service Name

**Name** [en] Qualified electronic registered delivery service Evicertia QERDS

**Name** [es] Servicio cualificado de entrega electrónica certificada Evicertia QERDS

### Service digital identities

#### X509SubjectName

Subject CN: EVICERTIA, SL

Subject SERIAL NUMBER: B86021839

Subject 2.5.4.97: VATES-B86021839

Subject O: EVICERTIA, SL

Subject ST: MADRID

Subject C: ES

**X509SKI**

X509 SK I *fis0TO6jWZ2ITXXEDEtImssL1Gc=*

Service Status *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

Status Starting Time *2021-11-16T02:00:00Z*

**39.4 - Service (granted): Qualified electronic registered delivery service Evicertia QERDS QE1A**

Service Type Identifier *http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

Service type description *[en] An electronic delivery service providing qualified electronic deliveries.*  
*[es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.*

**Service Name**

Name *[en] Qualified electronic registered delivery service Evicertia QERDS QE1A*

Name *[es] Servicio cualificado de entrega electrónica certificada Evicertia QERDS QE1A*

**Service digital identities****Certificate fields details**

Version: 3

Serial Number: 7685577479348319478





**Issuer O:** UANATACA S.A.

**Issuer L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B86021839

**Subject CN:** EVISEAL-QE1A

**Subject SERIAL NUMBER:** B86021839

**Subject O:** Evicertia S.L.

**Subject C:** ES

**Valid from:** Wed Sep 06 13:10:00 CEST 2023

**Valid to:** Mon Sep 04 13:10:00 CEST 2028

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D3F8110F5520B9209ED60DA75C51E3E38C93CF7D92672F478DC3EEFF82C157EB95AB3765784E621954CC4E4D0413E766326710E8125D7E6220E0DD7C1BBDA61851F075D3CED5792F79AE557FD8D98E27E462998DC287612A651EA8529C2090E02894F0F48A887D6278D4F43BF025A2478E2B0E17A8BAE0DD7F7B7E43832577B751053C3D4544A82A10E08B7AC2E00C62ED0E10B9467E011F52E5E2213739221C7475C081C9691EF35580F38D0E50EBF4F2D13B4916E6C9E6015B0CD6D2A840186C068867ED00A7A9590EB598ED4D2E069A3A13AF87F48F3BCBE5DC9257D69A7B2424D9131EF455B627E9ED2BE03338AB67BC0F92B36CF4F50203010001

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
29:EA:16:7A:9C:85:34:6B:27:75:C8:B6:7D:73:B0:80:55:1F:A4:14

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47286.1.9.1  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Certificado cualificado de Sello Electrónico en software.]  
Policy OID: 0.4.0.194112.1.1

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage**  
*id\_kp\_clientAuth*

**Subject Alternative Name**  
*info@evicertia.com*



**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *10:F9:DF:B5:26:1C:36:CA:10:CF:F6:C5:E0:D8:D9:C5:8C:D1:5E:03:18:2B:E3:66:E5:F8:E2:56:01:D4:B2:C0*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B86021839*

**Subject CN:** *EVISEAL-QE1A*

**Subject SERIAL NUMBER:** *B86021839*

**Subject O:** *Evicertia S.L.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *KeoWepyFNGsndci2fXOwgFUfpBQ=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2023-10-24T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**39.4.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/EDS/Q*

**Service Name**

**Name** *[en] Qualified electronic registered delivery service Evicertia QERDS QE1A*

**Name** *[es] Servicio cualificado de entrega electrónica certificada Evicertia QERDS QE1A*

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** *VATES-B86021839*

**Subject CN:** *EWISEAL-QE1A*

**Subject SERIAL NUMBER:** *B86021839*

**Subject O:** *Evicertia S.L.*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *KeoWepyFNGsndci2fXOwgFUfpBQ=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Status Starting Time** *2022-12-15T00:00:00Z*

**40 - TSP: EAD TRUST European Agency of Digital Trust, S.L.****TSP Name**

**Name** [ en ] *EAD TRUST European Agency of Digital Trust, S.L.*

**Name** [ es ] *EAD TRUST European Agency of Digital Trust, S.L.*

**TSP Trade Name**

**Name** [ en ] *EADTrust*

**Name** [ es ] *EADTrust*

**Name** [ en ] *VATES-B85626240*

**Name** [ es ] *VATES-B85626240*

**Name** [ en ] *European Agency of Digital Trust, S.L.*

**Name** [ es ] *European Agency of Digital Trust, S.L.</i>*

**Name** [ en ] *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Name** [ es ] *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**PostalAddress**

**Street Address** [ en ] *Mentrida, 6 - local*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28043*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Mentrida, 6 - local*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28043*

**Country Name** [ es ] *ES*



**Signature algorithm:** SHA256withRSA

**Issuer 2.5.4.97:** VATES-B85626240

**Issuer C:** ES

**Issuer O:** European Agency of Digital Trust, S.L.

**Issuer CN:** EADTrust RSA 2048 Root CA For Qualified Certificates 2019

**Subject OU:** Natural Person

**Subject 2.5.4.97:** VATES-B85626240

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.

**Subject CN:** EADTrust RSA 2048 SubCA For Qualified Certificates 2019

**Valid from:** Thu Jun 06 12:56:21 CEST 2019

**Valid to:** Sat Jun 02 12:56:21 CEST 2035

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100F133F0C5FCF93452BE662A4BF3A967A568A2D3AE0F878B766E0A AF3F0017075402FCE  
E8B9724488E0D7507634FD907280250E0D3F93CA2E83C99E20D0F8B001C4A3F347E21B4C9C3731A09302C72777168646AE2A8AE0C54F1FD483F3033FA693542E075  
6F8AD560FA293CBABF0449E9FE2D2C25BFC398215B3986009CA20133F9A022DD979254EB60DE2838F4F399F7D6AD124CDD0BB07D6EA2DEAFCE45BA1A6825  
A80654C5B8AF8B060211FC98B18207EFA43502D710D5E67FF53C8129DF8B107A403446BB04BB8BA4149EB8A0DCE05F61896E3CD9780AA2E75B054694C2F902D  
08641814421D13CF62C6643D1FA2CB9EC0DFE0F3BA08002230205010001

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401  
CPS pointer: <http://policy.eadtrust.eu>  
CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

**Basic Constraints**  
IsCA: true - Path length: 0

**Subject Key Identifier**  
6B:DE:93:B2:AA:FB:BA:DA:FE:EF:46:4E:C9:67:DC:3D:FE:7B:A7:75

**Issuer Alternative Name**  
ca@eadtrust.eu

**Subject Alternative Name**  
ca@eadtrust.eu  
<http://www.eadtrust.eu>  
<http://ca.eadtrust.eu>  
<http://policy.eadtrust.eu>

**Authority Key Identifier**  
1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99

**CRL Distribution Points**  
<http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl>

**Authority Info Access**  
<http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt>  
<http://ocsp.eadtrust.eu>

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *82:34:0E:A4:D7:AC:D8:0D:F9:7D:C7:59:8C:94:95:58:8C:C8:87:3E:C9:50:6D:AD:0C:11:EA:11:94:33:39:9D*

**X509SubjectName**

**Subject OU:** *Natural Person*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust RSA 2048 SubCA For Qualified Certificates 2019*

**X509SKI**

**X509 SK I** *a96Tsqr7utr+70ZOyWfcPf57p3U=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**40.2 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Certificates 2019- NP****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*



**Valid to:** Sat Jun 02 12:56:35 CEST 2035

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100BF82E1DEE6560F5432104A634A8B3DD62267975563C06A163C7686F365A1D93CA8447D  
FC8F085F1B534760264A40B03755CE3C2837851AF1E971698F9FB255A4C9F9274D94E35C9C8D7715DD159D0C3E544B23703DA1936414BB9072EFEA8B5F5B2D5D6281  
1586C29495CF98F53D2B01D4A17CEFB5A6E9F9517465640B23B4504CF0509052EFCBC834C848517FC897E3865890BD3442B6DEB7D39681B14C328E4492665D742F7  
2318140ACF4ACEFDA24179FCE5E07A1AC737F0E0698034F7969A52D60AD1530CDE7958C3BF8D8AC47132F8D9D3109DC8C976E3E3E067DF5F286CC32243A82B02  
092CB51ADDE731800E31B2591CABF179738DF6C9904B8CA16929E8C3BB67D534F4C1C097C20552BC3ACB9AB4E5A40E466D0EA2EA3970943BE03407B115749E558  
5065E66C4BBD771BDB9425039C40DBC280BAAC6922A4840175AC0EE9F1D E3E442AF39B2198D50F5D623DC5E6A6A9E656800DA614B63C7475A642489136D016862  
6133EE9C3A552CF8AC2329D6D13ABB01CA3E27A15C151E9C811B1CBC8E5A55D411DE2D78D501F966691050BB4722D87494A8DF4AD5C2FBE21738B52B260731FA  
09159C772C440E035F68B57CDB3086934C38F45EC41F41932A00013F9180C265E94AA191A5261FC347C49D1DEB7D12E053F7602CA45901B C11E8784DA4535C8C1BF  
D57E5A44DA88E0FFB3DEDD5A45CCF49B18E27B50203010001

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401  
CPS pointer: <http://policy.eadtrust.eu>  
CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

**Basic Constraints**  
IsCA: true - Path length: 0

**Subject Key Identifier**  
06:33:DA:2B:CE:E9:81:51:4F:69:DD:CD:C8:AF:DF:2C:2F:3D:BE:5E

**Issuer Alternative Name**  
ca@eadtrust.eu

**Subject Alternative Name**  
ca@eadtrust.eu  
<http://www.eadtrust.eu>  
<http://ca.eadtrust.eu>  
<http://policy.eadtrust.eu>

**Authority Key Identifier**  
E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4

**CRL Distribution Points**  
<http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl>

**Authority Info Access**  
<http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt>  
<http://ocsp.eadtrust.eu>

**Key Usage:**  
digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
04:BF:1D:A6:D0:16:8B:DD:3F:2D:EC:2E:22:C5:0D:55:8B:DE:5C:7C:C9:51:6C:83:CB:63:93:35:2  
A:9F:0F:9C

**X509SubjectName**

**Subject OU:**  
Natural Person

**Subject 2.5.4.97:**  
VATES-B85626240

**Subject C:**  
ES

**Subject O:**  
European Agency of Digital Trust, S.L.

**Subject CN:**  
EADTrust RSA 4096 SubCA For Qualified Certificates 2019

X509SKI



X509 SK I

BjPaK87pgVFPad3NyK/fLC89v14=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2020-10-05T00:00:00Z

**Scheme Service Definition URI****URI**

[en]

<https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**URI**

[es]

<https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>**40.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation****URI**

[en]

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>**40.3 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>**Service type description**

[en]

*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[es]

*Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.***Service Name****Name**

[en]

*Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP***Name**

[es]

*Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Certificates 2019- NP***Service digital identities****Certificate fields details****Version:**

3

**Serial Number:**

5842919634329022553



<b>Certificate Policies</b>	<i>Policy OID: 2.5.29.32.0</i>
	<i>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401</i>
	<i>CPS pointer: http://policy.eadtrust.eu</i>
	<i>CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]</i>
<b>Basic Constraints</b>	<i>IsCA: true - Path length: 0</i>
<b>Subject Key Identifier</b>	<i>EA:99:CF:6B:01:18:F9:81:44:69:FD:C8:9A:68:AD:D5:37:D3:73:98</i>
<b>Issuer Alternative Name</b>	<i>ca@eadtrust.eu</i>
<b>Subject Alternative Name</b>	<i>ca@eadtrust.eu</i>
	<i>http://www.eadtrust.eu</i>
	<i>http://ca.eadtrust.eu</i>
	<i>http://policy.eadtrust.eu</i>
<b>Authority Key Identifier</b>	<i>06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB</i>
<b>CRL Distribution Points</b>	<i>http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl</i>
<b>Authority Info Access</b>	<i>http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt</i>
	<i>http://ocsp.eadtrust.eu</i>
<b>Key Usage:</b>	<i>digitalSignature - keyCertSign - cRLSign</i>
<b>Thumbprint algorithm:</b>	<i>SHA-256</i>
<b>Thumbprint:</b>	<i>20:02:B8:D5:AF:02:C5:A9:61:E1:0A:4D:A3:C2:7F:63:F3:5D:7F:7A:AD:94:15:99:DA:36:D5:2E:03:B7:A8:9D</i>
<b>X509SubjectName</b>	
<b>Subject OU:</b>	<i>Natural Person</i>
<b>Subject 2.5.4.97:</b>	<i>VATES-B85626240</i>
<b>Subject C:</b>	<i>ES</i>
<b>Subject O:</b>	<i>European Agency of Digital Trust, S.L.</i>
<b>Subject CN:</b>	<i>EADTrust RSA 8192 SubCA For Qualified Certificates 2019</i>
<b>X509SKI</b>	
<b>X509 SK I</b>	<i>6pnPawEY+YFEaf3Immit1TfTc5g=</i>
<b>Service Status</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<b>Service status description</b>	<i>[en] undefined.</i>
	<i>[es] undefined.</i>



**Signature algorithm:** *SHA256withECDSA*

**Issuer 2.5.4.97:** *VATES-B85626240*

**Issuer C:** *ES*

**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust ECC 256 Root CA For Qualified Certificates 2019*

**Subject OU:** *Natural Person*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

**Valid from:** *Thu Jun 06 13:23:12 CEST 2019*

**Valid to:** *Sat Jun 02 13:23:12 CEST 2035*

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:8B:E1:40:32:84:BC:E1:94:46:21:9F:0B:85:A0:AE:9B:47:C5:E4:2C:BC:77:68:D6:57:28:42:D1:8E:FC:49:72:5A:86:31:D2:F4:BA:98:86:FD:29:47:3F:15:BE:6C:DD:BB:C5:B8:D6:C3:CB:22:05:3B:43:CC:E6:51:77:C8:E8

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401*  
*CPS pointer: <http://policy.eadtrust.eu>*  
*CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Subject Key Identifier**  
*C3:E2:DB:11:EF:36:3C:6A:80:49:8B:23:46:8D:3B:A7:33:6B:99:0C*

**Issuer Alternative Name**  
*ca@eadtrust.eu*

**Subject Alternative Name**  
*ca@eadtrust.eu*  
*<http://www.eadtrust.eu>*  
*<http://ca.eadtrust.eu>*  
*<http://policy.eadtrust.eu>*

**Authority Key Identifier**  
*01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*

**CRL Distribution Points**  
*<http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl>*

**Authority Info Access**  
*<http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt>*  
*<http://ocsp.eadtrust.eu>*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *E5:F7:80:53:30:0C:16:9D:79:A7:FB:38:73:61:AD:2A:8D:1A:9B:B7:50:B9:18:3C:7B:B1:97:34:D5:42:F0:7C*

**X509SubjectName**

**Subject OU:** *Natural Person*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 256 SubCA For Qualified Certificates 2019*

**X509SKI**

**X509 SK I** *w+LbEe82PGqASYsjRo07pzNrmQw=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**40.5 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Certificates 2019- NP****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*



<b>Certificate Policies</b>	<i>Policy OID: 2.5.29.32.0</i>
	<i>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401</i>
	<i>CPS pointer: http://policy.eadtrust.eu</i>
	<i>CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]</i>
<b>Basic Constraints</b>	<i>IsCA: true - Path length: 0</i>
<b>Subject Key Identifier</b>	<i>8F:BA:E8:66:72:74:22:4C:CC:27:89:48:08:31:73:0B:1E:9B:4B:82</i>
<b>Issuer Alternative Name</b>	<i>ca@eadtrust.eu</i>
<b>Subject Alternative Name</b>	<i>ca@eadtrust.eu</i>
	<i>http://www.eadtrust.eu</i>
	<i>http://ca.eadtrust.eu</i>
	<i>http://policy.eadtrust.eu</i>
<b>Authority Key Identifier</b>	<i>78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01</i>
<b>CRL Distribution Points</b>	<i>http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl</i>
<b>Authority Info Access</b>	<i>http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt</i>
	<i>http://ocsp.eadtrust.eu</i>
<b>Key Usage:</b>	<i>digitalSignature - keyCertSign - cRLSign</i>
<b>Thumbprint algorithm:</b>	<i>SHA-256</i>
<b>Thumbprint:</b>	<i>F8:EA:34:65:13:55:C4:07:C9:03:87:56:08:B0:FF:A1:88:80:5E:93:08:1A:D0:3A:39:B8:22:6D:C3:5E:AD:B4</i>
<b>X509SubjectName</b>	
<b>Subject OU:</b>	<i>Natural Person</i>
<b>Subject 2.5.4.97:</b>	<i>VATES-B85626240</i>
<b>Subject C:</b>	<i>ES</i>
<b>Subject O:</b>	<i>European Agency of Digital Trust, S.L.</i>
<b>Subject CN:</b>	<i>EADTrust ECC 384 SubCA For Qualified Certificates 2019</i>
<b>X509SKI</b>	
<b>X509 SK I</b>	<i>j7roZnJ0IkzMJ4IICDFzCx6bS4I=</i>
<b>Service Status</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<b>Service status description</b>	<i>[en] undefined.</i>
	<i>[es] undefined.</i>



**Status Starting Time** 2020-10-05T00:00:00Z

### Scheme Service Definition URI

**URI** [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 40.5.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 40.6 - Service (granted): Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

### Service Name

**Name** [ en ] *Qualified Certificates issued by EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP*

**Name** [ es ] *Certificados cualificados emitidos por EADTrust RSA 2048 SubCA For Qualified Certificates 2019-LP*

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 8387960186886755879



**Subject Alternative Name**  
*ca@eadtrust.eu*  
*http://www.eadtrust.eu*  
*http://ca.eadtrust.eu*  
*http://policy.eadtrust.eu*

**Authority Key Identifier**  
*1F:D4:6B:B0:63:86:0C:0B:09:8C:42:6E:33:DD:7A:1D:14:31:2B:99*

**CRL Distribution Points**  
*http://crl.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crl*

**Authority Info Access**  
*http://ca.eadtrust.eu/eadtrust-root-rsa2048eadq2019.crt*  
*http://ocsp.eadtrust.eu*

**Key Usage:**  
*digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*29:40:0D:5D:52:0D:A0:85:2E:4D:D5:3A:5B:85:D3:26:8F:9A:3D:CC:60:61:C2:85:47:44:40:CB:85:9E:09:A8*

**X509SubjectName**

**Subject OU:**  
*Legal Person*

**Subject 2.5.4.97:**  
*VATES-B85626240*

**Subject C:**  
*ES*

**Subject O:**  
*European Agency of Digital Trust, S.L.*

**Subject CN:**  
*EADTrust RSA 2048 SubCA For Qualified Certificates 2019*

**X509SKI**

**X509 SK I**  
*+tkKomnL/2iv8pqJ/1aUVBuzmY8=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*



**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust RSA 4096 Root CA For Qualified Certificates 2019*

**Subject OU:** *Legal Person*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

**Valid from:** *Thu Jun 06 12:56:57 CEST 2019*

**Valid to:** *Sat Jun 02 12:56:57 CEST 2035*

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100AB19E29A3D347F60447CA81907516194881FA9792C5040EFF9A8FE4124247718665375D8220876BDD08FB6350DAE094CAE06BF22C7DC7DD32121CF5C0C59545546CD746ED10D1E00C3DA82499AD0C8A7B0C79498ED8ED84986B83F8498A8D565258E9F84712C570079CF50E1E357A30CAE6054DF145C861C9138DE12AEF931DF1F0D1B8213F20E3A867B7ED79FF187B24275594C739EA4394FE7D0A41DEDA724DC542A895F6FF83FA48BBD1FD84DA96D4635CE10AFC7DFF4C03CE54E4C0F7BEC8AB35B40AC539D559D28EC70A61E172371DD4D0A2DE05298E9F53BD8EAD034066A383A0F37766807C145048B7C048BD687C7488B0A8D7CC8C12883D38C886D3027474BF36814EAC09D1714A36BA72573FB43A5A580E247D5A7C1C939C1E66E1924068B57C29E4275449DCA699BE8E7346EBA8A882066D8D3C836D2C6340030115B437680C99B82AD77B50958E05BC653DA0893517315F5A988FEC42CE1006BEEDFFB762C71A1A0EF3953BDC675E117F822FCA9C41230745012F5D0AF27694E851574B47DA9201B245D13B7919218388D5FF1C4E29FB454E8BA18E28AA06B6F92D860B3E2B587AEAD1E8687B1403768CA352203227CECF047B11FC42AD86E4EFD0C5469B6F89FC7BFECE0A33AE64EEC3F1538BCD8142E85877307BD82592075FD29EFD928E804301CF443CC20831A49302BE26EF411D9565359810F70203010001

**Certificate Policies**

*Policy OID: 2.5.29.32.0*

*Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401*

*CPS pointer: <http://policy.eadtrust.eu>*

*CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]*

**Basic Constraints**

*IsCA: true - Path length: 0*

**Subject Key Identifier**

*31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*

**Issuer Alternative Name**

*ca@eadtrust.eu*

**Subject Alternative Name**

*ca@eadtrust.eu*

*<http://www.eadtrust.eu>*

*<http://ca.eadtrust.eu>*

*<http://policy.eadtrust.eu>*

**Authority Key Identifier**

*E3:C2:30:34:47:03:C0:0F:17:B2:63:B0:50:13:E5:14:B1:0C:59:F4*

**CRL Distribution Points**

*<http://crl.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crl>*

**Authority Info Access**

*<http://ca.eadtrust.eu/eadtrust-root-rsa4096eadq2019.crt>*

*<http://ocsp.eadtrust.eu>*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *7F:D0:FF:DF:3A:A0:C9:69:93:DC:6D:1A:DA:D7:79:22:63:81:AC:7B:5C:48:A0:1D:1A:2E:4A:FC:6C:2F:77:7A*

**X509SubjectName**

**Subject OU:** *Legal Person*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

**X509SKI**

**X509 SK I** *MS5X72kv2esv2yA4CeOEpyxJ/0U=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**40.8 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Certificates 2019-LP****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**



**Valid from:** Thu Jun 06 13:23:01 CEST 2019

**Valid to:** Sat Jun 02 13:23:01 CEST 2035

**Public Key:**  
 30820422300D06092A864886F70D010105000382040F003082040A0282040100BD017A9AEAB2223930B9D4265667BA340ADF43AA3275B2C50CF29AD748D92E374B  
 809F75D12DA541B8FC29D8CFD768198C72BB25B103F9BC9F1160A5A9140073EB4D229803107CBE07C24687283EEAB9C5B08C9A92D1F89ED9F3E1889C2917D5F  
 B19E179927A46B0DD1D079752B4CD32B81DBD7781F4159ED0754529AA5C301C57AEF51DE61D2EEB5D2C6929160B9D552B146B7CCB91E0559903BASC1C58C3C59  
 9EC661681435276ED01A4F45DAEFADE762FC2BA9D0532C248A95E3639E4391690D0642D46A5E1C678201478BB06540D86E67CE04BE19B89D9DC9B3E18F18F301CE  
 1C07894DCB138789C3DDDA18CA63829FDF83903E16AD78D3D6C25A3473C877DCA7F51D0A562C4B46E3521235C4D00E2E2E33B3644D45633A130831E3CF75CBFCES  
 D3E9585D231994C8AB1F29289B2476B9F2FC29E028C1CC0C2B2CED83A3328AB1E4FC24DA714FC42E8FCA71664C6021634FE70EB0490A11558D8487D3013350AB0E7B  
 C8E7E7E5D3A3F44B2E915F6ED91C705F535FCFC3546A48C5C8766F0C65C8E80ACD972D7B904943F8239CF2A5544A4808CC2195ED4E93DC6E6EDDA6002C7EB4  
 EC7D9836B2A2BD03996C1F1366D0B03653AD2B4BF66F3957533CF2C5F998759CD9F0844C5EFBA D94C180569D8A803760D6D426E1638E6936BBEB985F40224000  
 A6C49C3AD2F8286DC8E9788FBE763C39FE01F6B129B8C76F13D9940A975D5E4A8A4C2D2D107203A3DFD99A6BEFF1FAF66CB7261D7854A48781C041C30366A71  
 D99BD8D250D0A0BDC8A4482AD0FC711E09103F645C6D1B8C6912CDC63BB081E09CF4E86FD7E4DDA3B9A5A2B35B8F9DE15BA3742D28C464E8992686D38459C7  
 D7DA4F0460A6E85E74F42EE2ADDA07A4D013447A7A7103E103C463DB997144C324E0FEF07C0A0F37AD0985FF10632EB2C44680AF024C6E4DE08F09BDC417  
 BBF4C63AD71184A05E4B6AE2E501B56D07794B01AE063F4FC9A528807DBF39712D3EC07703E3C3F2A08B1010779838EB887BCC901E0FEE4496B437D9B1C46AE06  
 A9A79A43A482E159629CA3A176B2E8F4ED0AF36E507B0CE43CA2B42A2F04E7308ECC5448B1E6ACE8E1DEFDEFCF1CF5E1350C8626990CC827985F312E9B5DFF7D  
 E294622891415F801CA2FD729DBF3E8E72E96207A6188CA10D9A1CCED9F9C8C4235C52BFC3E6976D1140B07CEAD41E31C90B382FE12E94D552606498D88  
 E571005B6CFC1F84A63C21BCF91A1B8B0E7E3E7A04DA5A128AFBFB04E029F297589A153E31E419D06341307A1ADBA1C86739A4921D9E7BCABF2C43A0D01537DFB  
 02176129C3C308188CD29AE353CF08CA124324C8FE8482E25A6566C20FF1787F4FE08B59600C55F8078E12006B10F5DF0BC4E17D7C40695519FDAE101199D66F6  
 D40CD4149972249E3B378B4E3A6971130203019001

**Certificate Policies** Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: <http://policy.eadtrust.eu>

CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 8C:48:A3:F4:BF:0A:56:40:CA:CE:93:5D:7A:3D:26:D8:14:94:A6:CF

**Issuer Alternative Name** ca@eadtrust.eu

**Subject Alternative Name** ca@eadtrust.eu

<http://www.eadtrust.eu>

<http://ca.eadtrust.eu>

<http://policy.eadtrust.eu>

**Authority Key Identifier** 06:E6:73:D9:51:39:40:A7:D1:57:8C:36:7F:C7:ED:D0:79:DD:F7:CB

**CRL Distribution Points** <http://crl.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crl>

**Authority Info Access** <http://ca.eadtrust.eu/eadtrust-root-rsa8192eadq2019.crt>

<http://ocsp.eadtrust.eu>

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 22:E4:1B:48:79:FA:A2:11:61:D4:65:02:C7:FC:14:39:E5:49:0E:CC:FF:43:42:1F:6E:9C:08:61:42:70:81:96

## X509SubjectName

**Subject OU:** Legal Person

**Subject 2.5.4.97:** VATES-B85626240

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.



**Subject CN:** EADTrust RSA 8192 SubCA For Qualified Certificates 2019

**X509SKI**

**X509 SK I** jEij9L8KVkDKzpNdej0m2BSUps8=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2020-10-05T00:00:00Z

#### **Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### **40.8.1 - Extension (critical): additionalServiceInformation**

##### **AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### **40.9 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

#### **Service Name**

**Name** [en] Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP

**Name** [es] Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Certificates 2019-LP

#### **Service digital identities**

##### **Certificate fields details**

**Version:** 3

**Serial Number:** 330884354597339267



**Subject Alternative Name**  
*ca@eadtrust.eu*  
*http://www.eadtrust.eu*  
*http://ca.eadtrust.eu*  
*http://policy.eadtrust.eu*

**Authority Key Identifier**  
*01:67:9A:84:C4:99:C6:81:ED:3C:58:04:74:AF:24:A3:D7:5E:41:0D*

**CRL Distribution Points**  
*http://crl.eadtrust.eu/eadtrust-root-ecc256eadq2019.crl*

**Authority Info Access**  
*http://ca.eadtrust.eu/eadtrust-root-ecc256eadq2019.crt*  
*http://ocsp.eadtrust.eu*

**Key Usage:**  
*digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*36:09:93:59:34:06:E5:AA:31:16:63:ED:FF:5A:34:09:A8:DD:1E:30:70:8C:9C:AB:E3:4E:FD:8E:53:92:73:3D*

**X509SubjectName**

**Subject OU:**  
*Legal Person*

**Subject 2.5.4.97:**  
*VATES-B85626240*

**Subject C:**  
*ES*

**Subject O:**  
*European Agency of Digital Trust, S.L.*

**Subject CN:**  
*EADTrust ECC 256 SubCA For Qualified Certificates 2019*

**X509SKI**

**X509 SK I**  
*00xsOr02/nCHI4c67j2Qz8ub9yE=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en]* *undefined.*

*[es]* *undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* *https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es]* *https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*



**Subject 2.5.4.97:** VATES-B85626240

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.

**Subject CN:** EADTrust ECC 384 SubCA For Qualified Certificates 2019

**Valid from:** Thu Jun 06 13:23:16 CEST 2019

**Valid to:** Sat Jun 02 13:23:16 CEST 2035

**Public Key:**  
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:F5:EB:2F:2E:DD:13:FE:73:BD:CB:89:55:48:C7:77:EC:36:AC:6A:62:6B:BB:5E:3D:93:C4:33:50:86:26:D3:87:AE:1F:F8:E7:D0:07:61:E6:98:F7:1A:BC:57:98:85:D9:2C:E8:B9:8F:AA:DF:A4:81:8D:F4:5B:D0:38:DD:F5:52:7E:3C:81:06:A5:43:AC:D9:DA:A8:9C:98:91:F1:C4:7B:8A:BA:94:D6:44:4C:B0:80:65:4B:BA:8A:76:43:A9:66

**Certificate Policies**  
 Policy OID: 2.5.29.32.0  
 Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401  
 CPS pointer: <http://policy.eadtrust.eu>  
 CPS text: [Subordinate Certificate Authority. European Agency of Digital Trust, S.L.]

**Basic Constraints**  
 IsCA: true - Path length: 0

**Subject Key Identifier**  
 5C:19:E2:AB:1D:B6:B8:3D:45:12:91:92:1B:8C:14:71:D8:E8:F5:F6

**Issuer Alternative Name**  
 ca@eadtrust.eu

**Subject Alternative Name**  
 ca@eadtrust.eu  
<http://www.eadtrust.eu>  
<http://ca.eadtrust.eu>  
<http://policy.eadtrust.eu>

**Authority Key Identifier**  
 78:14:FD:EE:D1:09:60:5C:75:A7:67:6E:26:48:81:E4:EA:C4:92:01

**CRL Distribution Points**  
<http://crl.eadtrust.eu/eadtrust-root-ecc384eadq2019.crl>

**Authority Info Access**  
<http://ca.eadtrust.eu/eadtrust-root-ecc384eadq2019.crt>  
<http://ocsp.eadtrust.eu>

**Key Usage:**  
 digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 04:14:B9:54:12:A9:8B:2D:9C:8B:DD:67:16:72:19:9D:7A:9C:E5:B9:7F:69:07:38:01:AD:CB:E0:DE:D9:7B:41

**X509SubjectName**

**Subject OU:** Legal Person

**Subject 2.5.4.97:** VATES-B85626240

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.

**Subject CN:** EADTrust ECC 384 SubCA For Qualified Certificates 2019

**X509SKI**

**X509 SK I** XBniqx22uD1FEpGSG4wUcdjo9fY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2020-10-05T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.10.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**40.11 - Service (granted): Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019

**Name** [en] Certificados cualificados emitidos por EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019

**Service digital identities**



**Authority Info Access** <http://ca.eadtrust.eu/eadtrust-root-rsa4096eadevpsd22019.crt>  
<http://ocsp.eadtrust.eu>

**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *00:9D:BA:D6:86:CE:CD:81:D1:3A:CA:C4:F6:73:DC:BA:5E:EB:78:9E:63:17:3C:DE:13:6C:B2:88:0C:1D:CE:79*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust RSA 4096 SubCA For Qualified Web EV/PSD2 Cert 2019*

**X509SKI**

**X509 SK I** *hM7za6qmVzAn98MSmSDI4JtaHkQ=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.11.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.12 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>



Service type description

[en]

A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.

[es]

Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

Service Name

Name

[en]

Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

Name

[es]

Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

Service digital identities

Certificate fields details

Version:

3

Serial Number:

8543911274838307584

X509 Certificate

-----BEGIN CERTIFICATE-----

MII...-----END CERTIFICATE-----

Signature algorithm:

SHA512withRSA

Issuer C:

ES

Issuer O:

European Agency of Digital Trust, S.L.

Issuer CN:

EADTrust RSA 8192 Root CA For Qualified Web EV/PSD2 Cert 2019

Subject C:

ES

Subject O:

European Agency of Digital Trust, S.L.

Subject CN:

EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

Valid from:

Thu Jun 06 13:49:10 CEST 2019

**Valid to:** Tue Jun 03 13:49:10 CEST 2031

**Public Key:**

```
30820422300D06092A864886F70D010105000382040F003082040A0282040100B122CAB811863EA669166C9E209762E39294A17C52F2291BC672C9B1DE528557644852
C085054E86A4ED5C2B866A8A1677599237EE8445D6425C9635B48942A557071F47E7B6E1504A494F53E7F3634B4201C3E89993F5625335AFAD0A40D5F866D940E134
5F4964AD92D2F5308D01DBBB3F65704EDCBA636E3504FC5D2D70F89879CE221B6DE8753AEA49CC2901292409E0E36481E13A3819FA05B4542121108089E33958A2AC6
D637DA5FB08E2684811EAS39DS77CB6648E9043CD79C3AE7FA8B394A9DC3813E4933909A2B80BC0F2F184C01325D23DD238282CFCA50412999F9467C9EDBE034A
CF3AS1D5D293397928E52C79A2ECF71F94D8E31EBF2D74390732930DC8B80E96A8A27DC683BA50141CED311FCE1683914466EFD00E844B850E9F40274E4042872
04F55EBF457C8DA0430C1FB32FB1E1AC3B6B2750473BFC479BFD4686CC0630C042E8E7647D8F3E773DD4B4E1F1B3AB4D6CC04A434B8E5A856BE0685CC2066D8
7156A106C58BFEAC3FB744EA6FBCD6ABDA79BFE64A9B93A7D24A80DDAE84E8F8FABA3F8DD901CDA614A709309BE72A813F97D939AE2DD4BFB3B0EF25C
8297C51B948E9D72CBF07088F47DD20D9D748366998B5E4BA14023F9E35606C3C642CCA8BD11CE8D85C12DDFDC28D471EC688162918B02137F1102ECBE4B1435
33195A47AKAF8E92EAEFE668A1FD7234F10D41CFF6C9C046B8E520043DCAAE43DA034E33F015050EEF39C9835AF515EC1B539C81D8AC9CD9B996FBA0DD868E12
F06800A11661BE5B0E26B5E42D41D02C12866C34B1D3CD98D6D05F5F82D94D42A5D79B7948664A542E642A7B95D8A6BDC8A9D9BE3612FD49624213FB53710D22A
8BC489D8D17DD6D5660B868852F78CB08965197209DA2C7D441970A0A90C6139E5654E18F9F65DA6E10B1E4971B1B1E2EC5D52269FFDA4ADA8056AA7B729A2
B6D0C68A8FCF1BD70E536BBD6A23B80261A7E01DD16546A8FB90F7E164C0036CF4DAE36AF30B77ACFFBB9C95CF50AE8048B2C2461F449E95868B2D2982F64D42
74D8D7EFCFD2D59D61ADC8E8D9E73A1C32179D51A4AD4219E85C8371370311695A8ACF46AF9F50655694611C8633E615481EB9D926CFB6876DABDB6C7CF
21090024A96EBA3488C107ACCE1C1231153F1066B4D7A926576A98038E87301906841E8B871949B5D44A4C2D0C15FC9140FD7F4C291CCDAE480EBE712C5F637D5
742CE5F342C988CB0BFFAEAI032AFFA7CA9A049EFC55DA9557C7CC8E8E3A66CC8A5CC8558BD877F7B1D20263F0EDEF6F172641617E7F810D34159A5373EC6D70
B82A2395CA6AFAEAB55F78E7E8AA82AE308BFF6C37FDC5C999CF1EDBCAB78CC9F25304C3800283E8FE4ED4866BD02836DEC43D882752AD2E3CDE2DA0D7B9820
3155D65CEEBAF32550E7CC4020C931F8D90205010001
```

**Certificate Policies**

Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: <http://policy.eadtrust.eu>

**Basic Constraints**

IsCA: true - Path length: 0

**Subject Key Identifier**

0E:62:CB:68:7C:BD:63:1B:28:8B:54:21:AE:0F:8D:A4:71:27:22:5E

**Authority Key Identifier**

BA:6A:0E:98:27:36:1C:AA:34:4D:DB:55:F7:DD:B0:73:49:F3:5D:F7

**CRL Distribution Points**

<http://crl.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crl>

**Authority Info Access**

<http://ca.eadtrust.eu/eadtrust-root-rsa8192eadevpsd22019.crt>

<http://ocsp.eadtrust.eu>

**Extended Key Usage**

id\_kp\_serverAuth

**Key Usage:**

digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

51:4A:80:6A:46:D7:B7:97:25:B9:2C:EA:06:85:54:15:D9:24:E7:6D:C5:D5:1E:4E:D5:CA:39:55:CB:6E:C8:5D

**X509SubjectName****Subject C:**

ES

**Subject O:**

European Agency of Digital Trust, S.L.

**Subject CN:**

EADTrust RSA 8192 SubCA For Qualified Web EV/PSD2 Cert 2019

**X509SKI****X509 SK I**

DmLLaHy9Yxsoi1Qhrg+NpHENl4=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en] undefined.

[es] undefined.

**Status Starting Time**

2020-10-05T00:00:00Z

**Scheme Service Definition URI**

URI [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.12.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.13 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

Service type description [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generacion de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

Name [ en ] *Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

Name [ es ] *Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

**Service digital identities****Certificate fields details**

Version: 3

Serial Number: 3612576674077687876

**X509 Certificate**

-----BEGIN CERTIFICATE-----

```
MIIDpDCCA0mgAwIBAgIEM6LrWEZDQEQwCgYIKoZIhIWAQwEAAQwYUxRTBDBgNVBAMPEVBRFRydXN0
IEVDQyAyNTYgUm9vdCB0QSBG63IgtLXVhbGlnaWVkaWZlYyBfV9QU00yIElicnQgMjAxOTVhMC0G
A1U1ECgmRkYyY3BhYyW4gQWdlbmN5Iz9mIHRpZ210YWwvVHJ1c3QsIFMuTC4sCzAUBgNVBAYTAkVT
MFAxDTESMDYwMjE5NDk5NjE5NDk5NjE5NDk5NjE5NDk5NjE5NDk5NjE5NDk5NjE5NDk5NjE5NDk5
QyAyNTYgU3VQU0gRm9yIFZlYXN0IHRpZ210YWwvVHJ1c3QsIFMuTC4sCzAUBgNVBAYTAkVT
JKVlcm9wZWVudFpZdW5jeS0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0y
Bj90MjAxOTVhMC0GAGF0IHRpZ210YWwvVHJ1c3QsIFMuTC4sCzAUBgNVBAYTAkVT
cDStKjRlZGkiC2UyZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0y
OAYNKwYBBAGDQjBBAQDETAAMCUGCCGAAQIIFBwIBBhOdfHRwO8SveC9haWNSlmlVhZHRydXN0LmV1
MBGAIU1deWE9wQIMAYBARKCAQAwDgYDVYRlPAQIBAQAgGMBGAIU1deWE9wQIMAYBARKCAQAwDg
VUEG7NmMDgczAIBgNVHSMGDAWgBTTd81a2q0TXIKTGSngwB1ZkEzBNBgnVHRSEJBEEMKq
OKA-hyxodHRwO8SveC9haWNSlmlVhZHRydXN0LmV1L2VhZHRydXN0LXVhbnQzZWZlZm9udGVudC0y
MjAxOTVhMC0GAGF0IHRpZ210YWwvVHJ1c3QsIFMuTC4sCzAUBgNVBAYTAkVT
ZkZlZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0y
cDovL290c3VudFpZdW5jeS0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0yZm9udGVudC0y
SM49BAMC0kAMEYKCC26IscVSYiSMGZDl0w-4370d86MlgAvvX3yctDv-r6A1bAPPNHzRaILM
LzKpHqgvNFlp1AzzB3y03TE5AZLly
```

-----END CERTIFICATE-----

Signature algorithm: SHA256withECDSA

Issuer C: ES

**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust ECC 256 Root CA For Qualified Web EV/PSD2 Cert 2019*

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

**Valid from:** *Thu Jun 06 13:49:24 CEST 2019*

**Valid to:** *Tue Jun 03 13:49:24 CEST 2031*

**Public Key:**  
30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:2A:03:D0:A5:62:9C:0D:32:13:9F:0F:2B:D8:ED:0E:1A:76:E1:AA:35:EF:B5:C8:FA:E1:0D:D5:E9:3E:3D:86:61:80:36:59:78:3E:53:92:30:EB:18:80:86:51:C8:57:87:0D:B8:53:3F:E9:94:C3:1B:64:D5:55:7F:82:A1:07:35

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401*  
*CPS pointer: <http://policy.eadtrust.eu>*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Subject Key Identifier**  
*09:75:1E:59:AD:00:68:B1:14:92:55:41:06:6F:B3:66:30:39:20:73*

**Authority Key Identifier**  
*D3:77:CD:5A:DA:A3:93:5C:8B:4A:4C:65:D2:9A:0C:01:D5:99:3F:13*

**CRL Distribution Points**  
*<http://crl.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crl>*

**Authority Info Access**  
*<http://ca.eadtrust.eu/eadtrust-root-ecc256eadevpsd22019.crt>*  
*<http://ocsp.eadtrust.eu>*

**Extended Key Usage**  
*id\_kp\_serverAuth*

**Key Usage:**  
*digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*B7:69:11:A3:35:2D:1A:27:B3:C3:55:F0:49:CF:6F:BF:C5:E3:E4:97:5B:FD:BD:BC:1F:A0:41:32:7F:C7:6D:7C*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 256 SubCA For Qualified Web EV/PSD2 Cert 2019*

**X509SKI**

X509 SK I

CXUeWa0AaLEUkIVBBm+zZjA5IHM=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
 [es] undefined.

**Status Starting Time**

2020-10-05T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.13.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.14 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019****Service Type Identifier**<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
 [es] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [en] *Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

**Name** [es] *Certificados cualificados emitidos por EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019*

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 311084161010393909



**X509SubjectName**

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.

**Subject CN:** EADTrust ECC 384 SubCA For Qualified Web EV/PSD2 Cert 2019

**X509SKI**

**X509 SK I** cbtYoDwvViddC3tRSDirYNeqqeM=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time**

2020-10-05T00:00:00Z

**Scheme Service Definition URI**

**URI** [en] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** [es] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.14.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.15 - Service (granted): Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.  
[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.

**Service Name**

**Name** [en] Qualified Certificates issued by EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019

**Name** [es] Certificados cualificados emitidos por EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019

**Service digital identities****Certificate fields details**

<b>Version:</b>	3
<b>Serial Number:</b>	1258060407115912249
<b>X509 Certificate</b>	<pre>-----BEGIN CERTIFICATE----- MIIDDCCA0GqAwIBAgIEEXWHRlglDkwCgYIKoZj0EAWfwYmFsQzBBBGNVBAAMMOA0VBRFRydXN0 IEVDQyAyNTYzLm9ydcBDQSBG65glUXVibGlnaWVklfdiYiBEV9PViBDXU0IDwMTkxLzA1BgNV BAoMJKV1cm9uZWVudFVzZj5cSjBZBEaWdqdGf5FRf5dXN0LjCBITLkwaMQswCOYDVQKGEwFjUzAc Fw0OTzEMDYkMTMNTzIafw0eMTAEMEMAMTMTIEMGIML/EswPwYDQODDhPQUUcsmVzKCBFQ0Mg MjUzIFNlYANBIEZvcjBRdWVsaWZzZzV2IERWU09WIEncQgMjA0TEVMOGAIUECgwwRXVv b3BjYw4gQWdlbmN5IG9mIERzZ20YwugVHJ1c3QsIFMuTC4kCzAJBgNVBAYTAkVMTkFwEwYHKOZi 2jRCAYIKoZj0DAQDQgAFQmaF2YyYjAcaP9MUIFEH2UTDKS16zXoPp-1cAUVayagC9IFB0 2jxcj3X9v5s9V8Uf5SLA70VofBnMjgCAZ0wggGZMEsGAIUdIAREMEfWBgYEVR0gADA4Bg0r BgEEAYNIagEBAYMRMCcwJQYIKwYBBQUHAgEWWGWhdHA6L1y9wb2pY3kuzWfkdHJ1c3QzXUwEgYD VROTj0HfB4pBgEBwIBADA0BjBNVHQBAREBAMCAYYwHQYDVROBBYEFQChgBLfZz0kqH6Av hWfjVAMB8GAIEdlWQYMBsAFLwrx1yap90ubGrU640XAw3yMEsGAIUdHwREMEfWQKArdYg Omb0dHA6L1y9cmuuzWfkdHJ1c3QzXUwEgYDZj0c9cm9vdC1Y2MjNTZlYWRkdj92MjAxOSJ cmwweG9YIKwYBBQUHAgEYBjBMEUCCSgAQUFBACj0bdRw08Y2ZzuzWfkdHJ1c3QzXUwEgYD dHJ1c3Qzcm9vdC1Y2MjNTZlYWRkdj92MjAxOSJmYXN0c3Qzcm9vdC1Y2MjNTZlYWRkdj92MjAxOSJm LmVhZHRydXN0LmV1MB0GA1UdJQQWMBQGCsGAOUFBwMBBgrBgEFBQcDAjAKBggqhYOPQDAgNj ADBGAIEAAsp1y3d0bALK+9bqHdTXznQSSjYmiBQCpv8katsCIQCAlj35pInlyGTWMRoaSNw0 ISAkvhPUopns3pcu8k8g= -----END CERTIFICATE-----</pre>
<b>Signature algorithm:</b>	SHA256withECDSA
<b>Issuer C:</b>	ES
<b>Issuer O:</b>	European Agency of Digital Trust, S.L.
<b>Issuer CN:</b>	EADTrust ECC 256 Root CA For Qualified Web DV/OV Cert 2019
<b>Subject C:</b>	ES
<b>Subject O:</b>	European Agency of Digital Trust, S.L.
<b>Subject CN:</b>	EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019
<b>Valid from:</b>	Thu Jun 06 13:35:52 CEST 2019
<b>Valid to:</b>	Tue Jun 03 13:35:52 CEST 2031
<b>Public Key:</b>	30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:42:6A:8F:D9:82:72:24:00:9A:3E:3F:4C:BB:51:5E:1F:65:13:0C:AE:54:EB:3A:D7:A0:FA:FF:FB:57:00:D1:56:B2:6A:00:BD:24:50:74:D A:0F:F1:7A:3D:D7:F6:DB:F9:ES:CF:55:F2:25:1F:C3:92:C0:EF:45:68:13:B3:4C:8D
<b>Certificate Policies</b>	<p>Policy OID: 2.5.29.32.0</p> <p>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401</p> <p>CPS pointer: <a href="http://policy.eadtrust.eu">http://policy.eadtrust.eu</a></p>
<b>Basic Constraints</b>	IsCA: true - Path length: 0
<b>Subject Key Identifier</b>	E0:9B:82:F0:4B:7F:B6:68:88:EA:9F:B7:A0:2F:FE:15:A5:AC:95:64
<b>Authority Key Identifier</b>	BC:2B:C7:5B:E3:6A:DA:7D:D1:A8:46:AD:47:DE:E3:45:C0:C3:FD:B2
<b>CRL Distribution Points</b>	<a href="http://crl.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crl">http://crl.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crl</a>
<b>Authority Info Access</b>	<p><a href="http://ca.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crt">http://ca.eadtrust.eu/eadtrust-root-ecc256eaddvov2019.crt</a></p> <p><a href="http://ocsp.eadtrust.eu">http://ocsp.eadtrust.eu</a></p>



**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *0E:1F:3A:20:04:0E:D5:B2:72:DC:C9:39:E7:B8:D5:B0:F4:BE:D7:64:C9:5C:E1:6C:B0:A4:7C:A4:56:0A:36:95*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 256 SubCA For Qualified Web DV/OV Cert 2019*

**X509SKI**

**X509 SK I** *4JuC8Et/tmiI6p+3oC/+FaWslWQ=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.15.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**40.16 - Service (granted): Qualified Certificates issued by EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*



**Authority Key Identifier** *1C:94:D8:12:94:49:7F:D7:AD:43:71:BB:2E:B2:BA:33:D2:C0:F4:46*

**CRL Distribution Points** *http://crl.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crl*

**Authority Info Access** *http://ca.eadtrust.eu/eadtrust-root-ecc384eaddvov2019.crt*  
*http://ocsp.eadtrust.eu*

**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *80:AB:1B:AA:C5:CA:A2:36:E8:80:17:92:FF:C8:8D:DC:CE:45:A9:30:FA:30:E5:78:DB:94:4D:51:28:2E:15:70*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust ECC 384 SubCA For Qualified Web DV/OV Cert 2019*

**X509SKI**

**X509 SK I** *Zj/V6yyw0c/kc+YXwGjFc+pv9ko=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.16.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*



**Valid from:** Thu Jun 06 13:24:14 CEST 2019

**Valid to:** Tue Jun 03 13:24:14 CEST 2031

**Public Key:**  
 30820222300D06092A864886F70D01010105000382020F003082020A0282020100B04AEA6054E8ADCACF2CCEB28378C0AF82A1E04328F71C0D3689F6A7386A4115B12965CD93B3CCBB99F2A1E6DE815473C811CB0A25511EF6D362F0222D939E37F221617ABF0BE8B4E285E2F3B2DCE50932886B14E00619FC0E05C86D4A67D8D3D8CD4289560651B6E5CC4B60811AD96092558CE895A3E288EF40CF04C4D9066F3B460214A88B3E1920CF03203A65470447388A65A2B5CC0192E7549A0D0D8864B6D0298DBB45BCE797255FB417FE141EB3C12E44BE92FC50D35915A41A2514BC84D92A0199CDS3D6678C29A8579803EC6BF0CDB78E829CC34B20CFD974C29639B035712E89B0FD2CF8ECBE86FF4E45E8D8258E8E0E14102FD38358B568D411EA4FFB5D8B63DD540CF2CD1A83ED50302C9ABB0D0BDE07D278F4ED22F0F9FB07C8364507BEDE5F2E4ABE77A884D83CCF0CBFBF650D420EFB75D14729BABA4DC72D7C894DA6296709EF17A36BC004A7C21BD1FECD853233BE71D1147F2C8638973353D3E6C8A74BC353DE1EB5D59815345E974DFB30EEFD4DD6EDF48E85F8701D23B8480C9C557248D1FA0274745C54F1F41A0055426AE1DB31FCDD99972615E34EEEAADCEFEF06C8B979E19370F642B4462E5A108C325546C3371660D5D8F36F9120AD8BF67225D1573A65E1953680F767926BC87A2ADBDBFAD84E4F679A1A1B51AC3F5C9975AFD4C4B867A097850796A3D9E7675A04439D5E410205010001

**Certificate Policies** Policy OID: 2.5.29.32.0

Policy OID: 1.3.6.1.4.1.501.2.1.1.1.401

CPS pointer: <http://policy.eadtrust.eu>

**Basic Constraints** IsCA: true - Path length: 0

**Subject Key Identifier** 50:6A:EE:F1:D7:1F:A5:AE:28:0F:A5:B9:00:C0:27:F3:CE:2E:AC:B7

**Authority Key Identifier** B6:C5:79:9E:16:1C:85:D9:52:1D:CB:1C:D2:88:C5:2C:C9:AF:0D:47

**CRL Distribution Points** <http://crl.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crl>

**Authority Info Access** <http://ca.eadtrust.eu/eadtrust-root-rsa4096eaddvov2019.crt>

<http://ocsp.eadtrust.eu>

**Extended Key Usage** id\_kp\_serverAuth

**Key Usage:** digitalSignature - keyCertSign - cRLSign

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 07:2C:23:9E:48:EE:41:17:F2:79:35:1A:1F:39:E2:B2:C8:5A:34:DA:65:52:43:EF:FF:18:D9:9B:CB:10:F9:14

## X509SubjectName

**Subject C:** ES

**Subject O:** European Agency of Digital Trust, S.L.

**Subject CN:** EADTrust RSA 4096 SubCA For Qualified Web DV/OV Cert 2019

## X509SKI

**X509 SKI** UGru8dcfpa4oD6W5AMAn884urLc=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2020-10-05T00:00:00Z

**Scheme Service Definition URI**

URI [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.17.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.18 - Service (granted): Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [ en ] *Qualified Certificates issued by EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

**Name** [ es ] *Certificados cualificados emitidos por EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 2461622916454388023



**CRL Distribution Points** <http://crl.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crl>

**Authority Info Access** <http://ca.eadtrust.eu/eadtrust-root-rsa8192eaddvov2019.crt>  
<http://ocsp.eadtrust.eu>

**Extended Key Usage** *id\_kp\_serverAuth*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A1:46:16:D1:E8:C0:B4:9E:0E:21:CA:E2:B5:42:A8:35:1A:26:74:7D:3A:18:A4:59:99:C3:8B:A1:D0:78:B6:CB*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *European Agency of Digital Trust, S.L.*

**Subject CN:** *EADTrust RSA 8192 SubCA For Qualified Web DV/OV Cert 2019*

**X509SKI**

**X509 SK I** *Uc6GODngV6I1mbGMY1dlisp+exU=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2020-10-05T00:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**40.18.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**40.19 - Service (withdrawn): Qualified timestamps issued by QTSU ALPHA EADTrust**





**Subject CN:** QTSU ALPHA EADTrust

**Valid from:** Fri Oct 18 13:11:27 CEST 2019

**Valid to:** Tue Oct 17 13:11:27 CEST 2023

**Public Key:**  
30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:01:01:00:C4:80:61:83:9E:D6:87:DB:64:BF:35:7E:50:24:63:8E:4F:2B:0F:82:57:B3:36:F4:C8:AB:BC:89:BF:56:48:54:73:4B:22:9C:99:53:6F:CF:FD:18:A3:51:96:C9:09:FB:0E:2E:4D:70:40:89:F0:4B:BC:5F:59:B6:8E:36:CC:5C:80:89:78:18:22:54:DD:B9:CA:DA:CB:A3:8A:37:DE:71:7F:A2:9E:EC:58:BE:ED:2D:0E:AD:C4:53:72:3D:88:48:5D:D8:A6:89:6F:6F:40:51:1C:93:95:AB:7E:10:D3:6F:63:2C:58:25:0B:DB:4D:0F:3A:91:4E:C7:73:2B:DF:28:1F:EB:40:51:78:6A:19:02:BC:FF:63:D1:25:49:4E:86:9A:CE:40:77:93:A7:53:86:40:83:7D:07:23:3E:0D:8B:97:1C:00:FC:30:1F:C1:B5:98:D2:57:E5:53:FF:12:70:A5:1B:9C:2B:7C:45:13:F1:D1:35:00:6A:27:F2:76:FF:10:C9:C3:BC:BB:67:AD:28:07:A7:89:31:2F:12:CF:CC:10:46:34:6D:C5:B1:9F:82:A4:4E:21:EC:85:E7:B2:7F:93:89:10:15:EC:59:4A:9B:0E:B1:E4:ED:6A:25:27:AB:7C:5F:66:88:44:43:83:8C:19:F7:27:06:86:C4:F0:7F:02:03:01:00:01

**Authority Key Identifier** 31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45

**Authority Info Access**  
<http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt>  
<http://ocsp.eadtrust.eu>

**Issuer Alternative Name** ca@eadtrust.eu

**Subject Alternative Name**  
ca@eadtrust.eu  
<https://ca.eadtrust.eu>  
<https://www.eadtrust.eu>  
<https://policy.eadtrust.eu>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421  
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]  
CPS pointer: <http://policy.eadtrust.eu>  
Policy OID: 0.4.0.194112.1.3  
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

**Extended Key Usage** id\_kp\_timeStamping

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15  
id\_etsi\_qcs\_QcSSCD

**CRL Distribution Points** <http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl>

**Subject Key Identifier** E2:60:19:10:A9:F9:70:75:60:4D:EB:35:84:A7:91:F7:28:9B:80:81

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 92:E7:2C:68:F6:B8:4E:8C:71:4F:A6:A0:54:13:C8:D5:0B:8F:1A:97:73:EF:24:0A:17:B3:B0:B5:CA:59:8D:79

**X509SubjectName**

**Subject C:** ES

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU ALPHA EADTrust*

**X509SKI**

**X509 SK I** *4mAZEKn5cHVgTes1hKeR9yibgIE=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2024-01-24T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.19.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service Name**

**Name** *[en] Qualified timestamps issued by QTSU ALPHA EADTrust*

**Name** *[es] Sellos electrónicos cualificados de tiempo emitidos por QTSU ALPHA EADTrust*

**Service digital identities****X509SubjectName**

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU ALPHA EADTrust*



**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust RSA 4096 SubCA For Qualified Certificates 2019*

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU DELTA EADTrust*

**Valid from:** *Wed Nov 06 12:03:26 CET 2019*

**Valid to:** *Sun Nov 05 12:03:26 CET 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100825809008AF0380B6ACD3B824D20B87187014B8320052CE4682DA0228D2F6B85C57  
342DCB4E6E66FBCF5BCD8781DCC950A651BA0DB26EF811E50D6C118A8CF75DACC6C9A93524CB6F67B178A77A33DC230132FC8503DEDE741E8B2AF87E6938A24  
79432568CE72A3B5C2288948A609A3E11492B5A5096CC3B3913412EAS7F53C60282D6B8EE5999080A5B6C3096A627A236A03A845AA645C09B45A48A981CBA4B4B5F  
38CCCE9DEAECAC494C72DF2BDE09B201E5D637663691E575F40E23D6FE814B6A77AB1F49A6C72BA7041D9AE9F2D0D837FBCE37F337FE69A94CB3A50F870FD  
BBE8E8E6935AD78570623DE83211610327422FEBDA2001727D8F12550203010001

**Authority Key Identifier** *31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45*

**Authority Info Access**  
*http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt*  
*http://ocsp.eadtrust.eu*

**Issuer Alternative Name** *ca@eadtrust.eu*

**Subject Alternative Name**  
*ca@eadtrust.eu*  
*http://ca.eadtrust.eu*  
*http://www.eadtrust.eu*  
*http://policy.eadtrust.eu*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*  
*CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]*  
*CPS pointer: http://policy.eadtrust.eu*  
*Policy OID: 0.4.0.194112.1.1*  
*CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

**Subject Key Identifier** *AA:8A:D3:74:92:7B:8F:F8:11:44:C0:EC:91:27:CE:27:8D:15:43:42*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *8F:04:72:62:CF:62:25:7E:BF:C8:85:E6:3F:65:11:12:31:35:13:3D:E2:8D:2A:8C:F1:03:4F:CC:B4:EA:7C:DA*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU DELTA EADTrust*

**X509SKI**

**X509 SK I** *qorTdJJ7j/gRRMDskSfOJ40VQ0I=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2024-01-24T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.20.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service Name**

**Name** *[en] Qualified time stamps issued by QTSU DELTA EADTrust*

**Name** *[es] Sellos electrónicos cualificados de tiempo emitidos por QTSU DELTA EADTrust*

**Service digital identities****X509SubjectName**



**Signature algorithm:** *SHA256withRSA*

**Issuer 2.5.4.97:** *VATES-B85626240*

**Issuer C:** *ES*

**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust RSA 2048 SubCA For Non-Qualified Certificates 2019*

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU EPSILON EADTrust*

**Valid from:** *Wed Nov 06 12:04:13 CET 2019*

**Valid to:** *Sun Nov 05 12:04:13 CET 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D358F88A32AF346BEF68D0730C19146FF955033049D57FC14D3775AB2A AF405E9DE2B  
732C4F81E7DBED9BF3C12FCA3A31E8504A311857F2459F1BB50C152BE1D89A9C8FCD7CDD3DC6FAB4280E7778056886984FC750CD730B35B737AFD7B3E6D117D  
A03FD7E7CF25F2DEA65EE9883603984ED497BCB7B86F65D75EC50A6D6C2018779F104BD4D0C39C0F756FC3B C47E914D9A4E56D8803DE6339A309E638355D18FF0F  
4757E404B5C8C7E7C3DE8F1E425DA09ABF4BFF36C4ACF1337F8B92A1B3015C501334EB132E1065E68521E93C7809E3A83F138A4516C0B381CS875DCB3317EDA0E3  
14D654A0D06A534F2873BCF21B93D1C599D0E53262ECDD0D8CB A70203010001

**Authority Key Identifier** *E7:EB:E9:2F:72:EB:F9:59:BD:7D:50:E9:4E:18:D0:CF:28:59:17:22*

**Authority Info Access**  
*http://ca.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crt*  
*http://ocsp.eadtrust.eu*

**Issuer Alternative Name** *ca@eadtrust.eu*

**Subject Alternative Name**  
*ca@eadtrust.eu*  
*http://ca.eadtrust.eu*  
*http://www.eadtrust.eu*  
*http://policy.eadtrust.eu*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.0.3161*  
*CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]*  
*CPS pointer: http://policy.eadtrust.eu*

**Extended Key Usage** *id\_kp\_timeStamping*

**CRL Distribution Points** *http://crl.eadtrust.eu/eadtrust-subca-rsa2048eadnq2019.crl*

**Subject Key Identifier** *E7:BF:CC:78:34:8F:77:61:9E:4C:5D:61:99:C6:B7:58:33:23:F1:74*



**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *6B:61:40:20:33:60:08:6C:45:F0:73:77:B8:9C:51:35:C3:AB:5A:C2:C0:09:10:D9:20:1C:92:E8:DB:68:3F:61*

**X509SubjectName**

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Entity Seal Certificate*

**Subject CN:** *QTSU EPSILON EADTrust*

**X509SKI**

**X509 SK I** *57/MeDSPd2GeTF1hmca3WDMj8XQ=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2024-01-24T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**40.21.1 - History instance n.1 - Status: granted****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service Name**

**Name** *[en] Qualified time stamps issued by QTSU EPSILON EADTrust*

**Name** *[es] Sellos electrónicos cualificados de tiempo emitidos por QTSU EPSILON EADTrust*

**Service digital identities****X509SubjectName**

**Subject C:** ES

**Subject O:** EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL

**Subject 2.5.4.97:** VATES-B85626240

**Subject OU:** Entity Seal Certificate

**Subject CN:** QTSU EPSILON EADTrust

**X509SKI**

**X509 SK I** 57/MeDSPd2GeTF1hmca3WDMj8XQ=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2020-10-05T00:00:00Z

#### 40.22 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 2048

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo de crear y firmar tokens tiempo sellos calificados.

#### **Service Name**

**Name** [en] Qualified timestamps issued by EADT QTSU 2023 RSA 2048

**Name** [es] Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 RSA 2048

#### Service digital identities

#### **Certificate fields details**

**Version:** 3

**Serial Number:** 1776818162991950082017



**Subject Alternative Name**  
*ca@eadtrust.eu*  
*https://ca.eadtrust.eu*  
*https://www.eadtrust.eu*  
*https://policy.eadtrust.eu*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*  
*CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]*  
  
*CPS pointer: http://policy.eadtrust.eu*  
*Policy OID: 0.4.0.194112.1.1*  
  
*CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*

**Extended Key Usage**  
*id\_kp\_timeStamping*

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points**  
*http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl*

**Subject Key Identifier**  
*A1:2F:86:A4:50:43:86:C6:22:1F:57:A1:63:AB:64:A0:02:F4:3D:05*

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*2B:B1:B5:AA:39:76:B7:70:E8:74:D9:26:3A:39:6B:ED:F7:04:6C:B7:95:54:70:DA:EE:DB:37:B9:9D:82:91:67*

**X509SubjectName**

**Subject C:**  
*ES*

**Subject O:**  
*EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:**  
*VATES-B85626240*

**Subject OU:**  
*Timestamp Certificate*

**Subject CN:**  
*EADT QTSU 2023 RSA 2048*

**X509SKI**

**X509 SK I**  
*oS+GpFBDhsYiH1ehY6tkoAL0PQU=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en]* *undefined.*  
*[es]* *undefined.*

Status Starting Time

2023-02-15T00:00:00Z

40.23 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 3072 ENS alto

Service Type Identifier

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Service type description

[en]

A time-stamping generation service creating and signing qualified time-stamps tokens.

[es]

Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

Service Name

Name

[en]

Qualified timestamps issued by EADT QTSU 2023 RSA 3072 ENS alto

Name

[es]

Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 RSA 3072 ENS alto

Service digital identities

Certificate fields details

Version:

3

Serial Number:

360239224898906147723

X509 Certificate

-----BEGIN CERTIFICATE-----

MIIJzCCBrgeAwIBAgIE4d80mgVWsuLMA0GCCqGSIb3DQEBCwUAMIGXMTUwP2YDVOQDDDFQURU...
-----END CERTIFICATE-----

Signature algorithm:

SHA256withRSA

Issuer OU:

Legal Person

Issuer 2.5.4.97:

VATES-B85626240

Issuer C:

ES

Issuer O:

European Agency of Digital Trust, S.L.

Issuer CN:

EADTrust RSA 4096 SubCA For Qualified Certificates 2019

Subject C:

ES

**Subject O:** EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL

**Subject 2.5.4.97:** VATES-B85626240

**Subject OU:** Timestamp Certificate

**Subject CN:** EADT QTSU 2023 RSA 3072 ENS alto

**Valid from:** Mon Jan 02 19:00:00 CET 2023

**Valid to:** Fri Dec 31 23:59:00 CET 2027

**Public Key:**  
308201A2300D06092A864886F70D01010105000382018F003082018A02820181009CDF5B3C424D59BCB03064D78BD3EA60A8B9E33BE2882B4F399E9655DE36247B5CD  
A1945A5D2AE2AA44D291BF12FCF6A6CC4EER889438CD3B860970C87B8F85EA877889571E0A95CA7842C537713A202208F0AC6A1D1716B8AB25732181DE7309A5A  
D3499D37EFAF2C70EA371B86A54E3925EA167488354F052D47A2F6BE9EA437694B33ED6140DC077E4D971E083005A0FA9FA521E52AD4C57C55F98FD3BAC232180B6  
F7B141A118CB9E44F5CF9FD770FD660E3890D4036242FE0042F4B8388CB3E5317CC77AE6D6E1964CB8C4FA1DFAD2797E9C9E838CB2B5DD96403925267DD7E6990C8  
F2D5CE166FE385AC4EAT2266007A48E74E3E270F66C7E6682E04DBA22B59FB7E267697E26E7CE98B4A8B59883F7BFD3FC306D652007C3045EDCE1D5B61DBBD47  
F2AA0B6B3E5A37FB64864438BD1A1B4C4F73DA7E6FE2E2DCD052B61C9B10012D921DE4E4D70EF6D38E5D2908CB5B6D67300902890D61CA82EC1155487D861FE20  
D5974F7B82097D6B68CF3156307093221BF007708E92DC537190203010001

**Authority Key Identifier** 31:2E:57:EF:69:2F:D9:EB:2F:DB:20:38:09:E3:84:A7:2C:49:FF:45

**Authority Info Access**  
<http://ca.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crt>  
<http://ocsp.eadtrust.eu>

**Issuer Alternative Name** ca@eadtrust.eu

**Subject Alternative Name**  
ca@eadtrust.eu  
<https://ca.eadtrust.eu>  
<https://www.eadtrust.eu>  
<https://policy.eadtrust.eu>

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421  
CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]  
CPS pointer: <http://policy.eadtrust.eu>  
Policy OID: 0.4.0.194112.1.1  
CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]

**Extended Key Usage** id\_kp\_timeStamping

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15

**CRL Distribution Points** <http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl>

**Subject Key Identifier** B4:D9:8A:48:9A:0F:5C:2B:86:CF:95:B6:76:45:8E:BE:02:8B:1A:E8

**Key Usage:** digitalSignature

**Thumbprint algorithm:** SHA-256

**Thumbprint:** 56:CA:F8:F0:7F:F8:F7:AB:8A:B5:C3:C6:37:AB:24:A9:93:C4:14:C4:9F:B7:FA:5B:D8:F2:6B:44:12:7D:A6:92

### X509SubjectName

**Subject C:** ES

**Subject O:** EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL

**Subject 2.5.4.97:** VATES-B85626240

**Subject OU:** Timestamp Certificate

**Subject CN:** EADT QTSU 2023 RSA 3072 ENS alto

### X509SKI

**X509 SK I** tNmKSJoPXCuGz5W2dkWOvgKLgug=

### Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

### Status Starting Time

2023-02-15T00:00:00Z

## 40.24 - Service (granted): Qualified timestamps issued by EADT QTSU 2023 RSA 4096 QSCD ENS alto

### Service Type Identifier

<http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service type description** [en] A time-stamping generation service creating and signing qualified time-stamps tokens.  
[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.

### Service Name

**Name** [en] Qualified timestamps issued by EADT QTSU 2023 RSA 4096 QSCD ENS alto

**Name** [es] Sellos electrónicos cualificados de tiempo emitidos por EADT QTSU 2023 RSA 4096 QSCD ENS alto

### Service digital identities

#### Certificate fields details

**Version:** 3

**Serial Number:** 133785518652922281297





<b>Subject Alternative Name</b>	<i>ca@eadtrust.eu</i> <i>https://ca.eadtrust.eu</i> <i>https://www.eadtrust.eu</i> <i>https://policy.eadtrust.eu</i>
<b>Certificate Policies</b>	<i>Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421</i> <i>CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]</i>  <i>CPS pointer: http://policy.eadtrust.eu</i> <i>Policy OID: 0.4.0.194112.1.3</i>  <i>CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]</i>
<b>Extended Key Usage</b>	<i>id_kp_timeStamping</i>
<b>QCStatements - crit. = false</b>	<i>id_etsi_qcs_QcCompliance</i> <i>id_etsi_qcs_RetentionPeriod: 15</i> <i>id_etsi_qcs_QcSSCD</i>
<b>CRL Distribution Points</b>	<i>http://crl.eadtrust.eu/eadtrust-subca-rsa4096eadlp2019.crl</i>
<b>Subject Key Identifier</b>	<i>DF:4B:77:3C:A1:3C:FC:14:2C:CF:AD:54:34:AB:84:B3:D2:B2:09:76</i>
<b>Key Usage:</b>	<i>digitalSignature</i>
<b>Thumbprint algorithm:</b>	<i>SHA-256</i>
<b>Thumbprint:</b>	<i>77:B8:F4:FA:24:32:0E:AB:C0:FB:D1:4A:F7:B5:5C:C7:89:55:FA:82:EF:94:36:B5:ED:A4:AF:3F:B E:4D:CD:C6</i>
<b>X509SubjectName</b>	
<b>Subject C:</b>	<i>ES</i>
<b>Subject O:</b>	<i>EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL</i>
<b>Subject 2.5.4.97:</b>	<i>VATES-B85626240</i>
<b>Subject OU:</b>	<i>Timestamp Certificate</i>
<b>Subject CN:</b>	<i>EADT QTSU 2023 RSA 4096 QSCD ENS alto</i>
<b>X509SKI</b>	
<b>X509 SK I</b>	<i>30t3PKE8/BQsz61UNKuEs9KyCXY=</i>
<b>Service Status</b>	<i>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</i>
<b>Service status description</b>	<i>[en] undefined.</i> <i>[es] undefined.</i>



**Subject OU:** *Timestamp Certificate*

**Subject CN:** *EADT QTSU 2023 ECC 256 ENS alto*

**Valid from:** *Mon Jan 02 19:00:00 CET 2023*

**Valid to:** *Fri Dec 31 23:59:00 CET 2027*

**Public Key:** *30-59-30-13-06-07-2A-86-48-CE-3D-02-01-06-08-2A-86-48-CE-3D-03-01-07-03-42-00-04-1D-59-6C-0C-70-58-75-9F-2D-A0-F8-E8-4C-09-3C-81-77-38-DD-8A-B5-A4-57-93-20-57-C9-7B-77-6A-DC-D9-BB-81-1D-D1-10-DA-18-7D-24-B0-00-76-A7-BA-1F-AD-26-C6-F9-0B-74-BB-DC-1C-57-97-B5-C2-97-11-A0*

**Authority Key Identifier** *D3:4C:6C:3A:BD:36:FE:70:87:23:87:3A:EE:3D:90:CF:CB:9B:F7:21*

**Authority Info Access** *http://ca.eadtrust.eu/eadtrust-subca-ecc256eadlp2019.crt*  
*http://ocsp.eadtrust.eu*

**Issuer Alternative Name** *ca@eadtrust.eu*

**Subject Alternative Name** *ca@eadtrust.eu*  
*https://ca.eadtrust.eu*  
*https://www.eadtrust.eu*  
*https://policy.eadtrust.eu*

**Certificate Policies** *Policy OID: 1.3.6.1.4.1.501.2.1.1.0.421*  
*CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]*  
*CPS pointer: http://policy.eadtrust.eu*  
*Policy OID: 0.4.0.194112.1.1*  
*CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**CRL Distribution Points** *http://crl.eadtrust.eu/eadtrust-subca-ecc256eadlp2019.crl*

**Subject Key Identifier** *33:10:30:38:C8:64:4A:51:4E:B0:0D:08:E6:01:69:66:73:AA:CC:DD*

**Key Usage:** *digitalSignature*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *03:42:82:8B:B5:28:1C:F3:0B:D9:AF:F5:09:2A:76:1A:8A:FB:E2:1D:37:07:86:6C:28:94:57:19:87:99:2C:48*

**X509SubjectName**

**Subject C:** *ES*



**Signature algorithm:** *SHA384withECDSA*

**Issuer OU:** *Legal Person*

**Issuer 2.5.4.97:** *VATES-B85626240*

**Issuer C:** *ES*

**Issuer O:** *European Agency of Digital Trust, S.L.*

**Issuer CN:** *EADTrust ECC 384 SubCA For Qualified Certificates 2019*

**Subject C:** *ES*

**Subject O:** *EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL*

**Subject 2.5.4.97:** *VATES-B85626240*

**Subject OU:** *Timestamp Certificate*

**Subject CN:** *EADT QTSU 2023 ECC 384 QSCD ENS alto*

**Valid from:** *Mon Jan 02 19:00:00 CET 2023*

**Valid to:** *Fri Dec 31 23:59:00 CET 2027*

**Public Key:**  
30:76:30:10:06:07:2A:86:48:CE:3D:02:01:06:05:2B:81:04:00:22:03:62:00:04:D5:FF:FC:3A:D5:6D:AE:4C:9D:62:00:36:EA:B3:48:A0:4F:86:5C:BE:44:F0:60:68:0D:3D:B2:0E:F3:3A:57:7F:37:66:7A:E5:17:5B:9F:36:F8:B9:D  
2:C4:D4:A3:6C:A8:8E:28:1A:C0:CC:C3:B4:33:2A:4B:57:20:58:ED:FC:AE:D8:46:3D:F1:92:E5:A2:C3:96:18:4F:9B:4C:DC:22:3A:FB:C0:E2:06:C9:B6:4A:58:8B:6B:C0:B9:FE:55:F8:5A

**Authority Key Identifier** *5C:19:E2:AB:1D:B6:B8:3D:45:12:91:92:1B:8C:14:71:D8:E8:F5:F6*

**Authority Info Access**  
*http://ca.eadtrust.eu/eadtrust-subca-ecc384eadlp2019.crt*  
*http://ocsp.eadtrust.eu*

**Issuer Alternative Name** *ca@eadtrust.eu*

**Subject Alternative Name**  
*ca@eadtrust.eu*  
*https://ca.eadtrust.eu*  
*https://www.eadtrust.eu*  
*https://policy.eadtrust.eu*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.501.2.1.1.1.421*  
*CPS text: [European Agency of Digital Trust, S.L. Legal Person Qualified Certificate]*  
  
*CPS pointer: http://policy.eadtrust.eu*  
  
*Policy OID: 0.4.0.194112.1.3*  
*CPS text: [European Telecommunications Standards Institute. eIDAS European Regulation Compliant]*

**Extended Key Usage** *id\_kp\_timeStamping*

**QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15**id\_etsi\_qcs\_QcSSCD***CRL Distribution Points***http://crl.eadtrust.eu/eadtrust-subca-ecc384eadlp2019.crl***Subject Key Identifier***ED:42:4A:85:DC:AF:F7:17:91:DE:8C:E8:C9:9C:4B:5D:9D:64:32:12***Key Usage:***digitalSignature***Thumbprint algorithm:***SHA-256***Thumbprint:***3E:A4:70:EB:D9:06:AB:C6:F0:15:7E:6C:63:06:A2:7D:F6:AB:03:8A:82:63:79:21:11:3A:C6:F1:4A:87:53:CB***X509SubjectName****Subject C:***ES***Subject O:***EAD TRUST EUROPEAN AGENCY OF DIGITAL TRUST SL***Subject 2.5.4.97:***VATES-B85626240***Subject OU:***Timestamp Certificate***Subject CN:***EADT QTSU 2023 ECC 384 QSCD ENS alto***X509SKI****X509 SK I***7UJKhdyv9xeR3ozoyZxLXZ1kMhI=***Service Status***http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2023-02-15T00:00:00Z*

**41 - TSP: Bewor tech, S.L.****TSP Name**

**Name** [ en ] *Bewor tech, S.L.*

**Name** [ es ] *Bewor tech, S.L.*

**TSP Trade Name**

**Name** [ en ] *Bewor tech*

**Name** [ es ] *Bewor tech*

**Name** [ en ] *VATES-B19603968*

**Name** [ es ] *VATES-B19603968*

**PostalAddress**

**Street Address** [ en ] *P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave 7*

**Locality** [ en ] *Granada*

**State Or Province** [ en ] *GRANADA*

**Postal Code** [ en ] *18015*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *P.I. Cortijo del Conde, Calle Pago de Cambea, 14 Nave*

**Locality** [ es ] *Granada*

**State Or Province** [ es ] *Granada*

**Postal Code** [ es ] *18015*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://bewor.com*

**URI** [ es ] *http://bewor.com*

**URI** [ en ] *mailto:info@bewor.com*





**Issuer O:** UANATACA S.A.

**Issuer L:** Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B19603968

**Subject CN:** BEWOR TECH CA1

**Subject OU:** PSC-BEWOR

**Subject O:** Bewor tech SL

**Subject L:** GRANADA

**Subject C:** ES

**Valid from:** Tue May 12 10:46:35 CEST 2020

**Valid to:** Thu May 12 10:46:35 CEST 2033

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A02820201009C53DE96E25C48BC2349FF1B4BCE5F3393E146A454B43A6ED14EB99D9BAECB409AEF94614EA25F7D1C63382925DDE24F13C057DF676E4D6E0D988364737D27653D377459988CFA125D305C609FEDA1DA4C9A73AC873D9C2DB05D0A543A2F7F8D80C2615AA8B9228E27C86F522E85CA590FD2D6E97E53A34A12612301972B25E2714F74E97BECS48C2C9CBF758F7940B8B3BD7CF2CEE0982FCB77E7B72B21E646681E4EF6286B66EFC43DC8205E915EB5A2F07A6246CBBEA7E826DE439D5CDDCD2A0835E5CAE52C50D1BED5296883070426CD5E6E5F982A1189D69589FEF6FF86BA377DB2C4994EB9B10DBA4A4CFC8F42547E11DC1E129847C62B30790C7F28642FA63B259393C919C988F9A71A5CC950E5908693DD10C6825E4CD5898ED52A51B7A692E140CC892113B7DA1445EC415BDF96D194DBD865BC3EA3CBARF7DD37B1DAE5D0BA869B95EA06B14FE1BB60FC05B9BA07C8426FAAABADB379CC5311BB9A48B640A972A7C53BF826B9D7B497298BA9E2FAE2061C7DEB7864919A0857815B2B96CD8074B95AD210C01FA04297DBA12347DB2803A309A3332DB5B3094CC9EBACAE903524260223E16E986035B176030AFD753772C29161068C5F8F2C9F917D30627A4F9A94C89AE2FEB5DC7B0C8E34414640CA56731AA51B9062AA882F7647DD0947B124DE069738116CA2F577D1E31251372DB570D2CCE6D0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
36:02:5A:C1:64:B4:F9:29:F1:03:09:16:94:B3:D9:A6:BD:7A:13:42

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C

**Issuer Alternative Name**  
[info@uanataca.com](mailto:info@uanataca.com)

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://bewor.com/dpc>  
CPS text: [Certificado de la Autoridad de Certificación Subordinada de Bewor tech - <https://bewor.com/proveedor-de-firma>]

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Subject Alternative Name**  
[info@bewor.com](mailto:info@bewor.com)

**Key Usage:**  
keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:** 8A:38:6E:D1:C0:93:26:03:D3:B5:F4:78:9B:7F:CB:33:CF:09:C8:1A:56:DE:97:FC:82:67:47:95:6C:2E:78:6D

## X509SubjectName

**Subject 2.5.4.97:** VATES-B19603968

**Subject CN:** BEWOR TECH CA1

**Subject OU:** PSC-BEWOR

**Subject O:** Bewor tech SL

**Subject L:** GRANADA

**Subject C:** ES

## X509SKI

**X509 SK I** NgJawWS0+SnxAwkWILPZpr16E0I=

## Service Status

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2020-10-23T02:00:00Z

### 41.1.1 - Extension (critical): additionalServiceInformation

#### AdditionalServiceInformation

**URI** [en] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**42 - TSP: SIGNICAT S.L.U.****TSP Name**

**Name** [ en ] *SIGNICAT S.L.U.*

**Name** [ es ] *SIGNICAT S.L.U.*

**TSP Trade Name**

**Name** [ en ] *Electronic Identification S.L.*

**Name** [ es ] *Electronic Identification S.L.*

**Name** [ en ] *VATES-B86681533*

**PostalAddress**

**Street Address** [ en ] *Avenida Ciudad de Barcelona, 81. 4ª Planta.*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28004*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *<https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>*

**URI** [ en ] *<mailto:jorge.guillamet@signicat.com>*

**TSP Information URI**

**URI** [ en ] *<https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>*

**42.1 - Service (granted): Qualified Certificates issued by ELECTRONIC IDENTIFICATION CA1****Service Type Identifier**

*<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**



**Valid from:** Tue Feb 25 11:57:13 CET 2020

**Valid to:** Thu Feb 24 11:57:13 CET 2033

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100C014E4D2C2710125200CEA1F454F91138951C0B48D4AF3CE6A182E8177EE6250C85498  
751E9399B53D9C49CD4B0C50D9DD3C17DA4488B6A2CE2E44E9F0AF036C9346CE7D1D4CA87AA18098DE54AA1CB5B2FD407D96DDE2D87946471F3D5D63F6DDEDCE652  
5080AB319651513FD83F9181861251F1AE1CB1AF40609E15CD1E2F08C1B6582EB1E1F38D1005100B8F44FED0E14D8FF1F85F16FC36BE56401299C015E3B8A4A1E84C8D77  
35DC899A4FB5E2FF4261FD42978F1F36916CF393E3B25FF6C1AA1C9CA1D12187347424DEEB209397314F6D95F9C6C2A270CCFF18DB0DFFFE8115C91BFF57FC856E12C  
1992004751FBAF3642E321FB2D70DD8D8746C3CBF37D2E4E1E3E3FA75C5B3531873483888B46CA7869B66A644759FF880CC35FD4E4C35A55D464E1F5DCB871FAF  
BCEA2E6F98F9AFBA011B9DF0AF1A291087505A8E10C58A241E13E2D5AD7E7E898FBD77801E307C9E9DD44AB0E2D00241085B0770076DD7796E7C29E26C6E9E8F7  
B92F7C8D13084E5CF88A9A70B6565B4970E6447BF68504E4080D40B5E6A24B9C2FCCD1A59BC9DD17164623F578F3A1AE24D28612448FB4C1B2AB85395842EF2D1D  
7874BCECE8DF4653B1D5965F43054A8FBC826337CB792BDECF388D4A4C9AA0E7051B98B0028D3A6EF2DFC4482AE440D4D39399D14C59BAD50E0E2501F5F659  
00F5B1647A0FB0450B4148D51D8FB042A2CB999A390D30203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
85:15:64:CD:9B:07:48:9D:F7:E6:9A:44:07:9C:79:0A:8C:A1:96:3F

**Basic Constraints**  
IsCA: true - Path length: 0

**Authority Key Identifier**  
55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C

**Issuer Alternative Name**  
info@uanataca.com

**Certificate Policies**  
Policy OID: 2.5.29.32.0  
CPS pointer: <https://www.electronicid.eu/certification-practice-statement-cpd/>  
CPS text: [Certificado de la Autoridad de Certificación Subordinada de Electronic Identification. - [www.electronicid.eu](http://www.electronicid.eu)]

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/ar1\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/ar1_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/ar1\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/ar1_uanataca.crl)

**Subject Alternative Name**  
info@electronicid.eu

**Key Usage:**  
keyCertSign - cRLSign

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
EE:DC:F3:16:33:60:9A:CB:49:28:95:FD:55:AA:59:1A:10:9C:44:D3:B0:FC:1D:06:21:E0:FB:41:A2  
:CB:49:2B

**X509SubjectName**

**Subject 2.5.4.97:**  
VATES-B86681533

**Subject CN:**  
ELECTRONIC IDENTIFICATION CA1

**Subject OU:**  
PSC-EID

**Subject O:**  
Electronic Identification S.L.

**Subject L:**  
MADRID

**Subject C:**  
ES

**X509SKI**

**X509 SK I** *hRVkzZsHSJ335ppEB5x5Coyhlj8=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2020-11-18T22:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**42.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[en] http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**42.1.2 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[OIDAsURN] urn:oid:1.3.6.1.4.1.55193.1.1.2*

**Description**

## 43 - TSP: Sectigo (Europe) SL

### TSP Name

**Name** [ en ] *Sectigo (Europe) SL*

**Name** [ es ] *Sectigo (Europe) SL*

### TSP Trade Name

**Name** [ en ] *SECTIGO*

**Name** [ es ] *SECTIGO*

**Name** [ en ] *VATES-B01683580*

### PostalAddress

**Street Address** [ en ] *Rambla Catalunya 86, 3º1*

**Locality** [ en ] *Barcelona*

**State Or Province** [ en ] *Barceona*

**Postal Code** [ en ] *08008*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *https://www.sectigo.com*

**URI** [ en ] *mailto:inigo.barreira@sectigo.com*

### TSP Information URI

**URI** [ en ] *https://www.sectigo.com*

## 43.1 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA E35”

### Service Type Identifier

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

### Service Name





**Certificate Policies** *Policy OID: 2.5.29.32.0*

**CRL Distribution Points** *http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl*

**Authority Info Access** *http://crt.usertrust.com/USERTrustECCAAACA.crt*  
*http://ocsp.usertrust.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *56:2D:6A:5B:4B:06:74:65:FF:D0:FB:FC:9B:B0:57:55:CD:AC:F5:5B:5E:E5:C6:F9:10:B8:B5:3D:B1:28:F5:7A*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Website Authentication CA E35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *ARCwfUxE0qCyYPno2n37iq+er1k=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**43.2 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA R35”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**



**Basic Constraints** *IsCA: true - Path length: 0*

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*

**CRL Distribution Points** *http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl*

**Authority Info Access** *http://crt.usertrust.com/USERTrustRSAAAACA.crt*  
*http://ocsp.usertrust.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *00:23:93:FA:0A:68:25:F7:7E:F6:86:E2:08:62:0B:97:17:77:91:F0:2F:07:DB:25:18:48:0F:BE:37:CE:7B:D8*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Website Authentication CA R35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *6zUIKgY26NYB5WmThNLzLDus3q8=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.2.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

**43.3 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Time Stamping CA R35”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST*

**Service type description** *[en] A time-stamping generation service creating and signing qualified time-stamps tokens.*

*[es] Un servicio de generación de sellado de tiempo crear y firmar tokens tiempo sellos calificados.*



**Extended Key Usage** *id\_kp\_timeStamping*

**Certificate Policies** *Policy OID: 2.5.29.32.0*

**CRL Distribution Points** *http://crl.sectigo.com/SectigoQualifiedTimeStampingRootR45.crl*

**Authority Info Access** *http://crt.sectigo.com/SectigoQualifiedTimeStampingRootR45.crt*  
*http://ocsp.sectigo.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *CD:0A:3E:00:A1:BD:AE:3A:15:9F:A9:E3:D7:0F:8E:66:4F:56:0F:DC:E1:63:57:CB:E4:40:ED:0B:0D:88:24:4F*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Time Stamping CA R35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *YQA/d9n/6jnSkaUcvp01x3hepGc=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**Scheme Service Definition URI**

**URI** *[en] https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**URI** *[es] https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx*

**43.4 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Natural Person CA E35”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** [ en ] *Qualified Certificates issued by "Sectigo Qualified Natural Person CA E35"*

**Name** [ es ] *Certificados cualificados emitidos por "Sectigo Qualified Natural Person CA E35"*

**Service digital identities****Certificate fields details**

**Version:** 3

**Serial Number:** 255804324125549905159335600213648333605

**X509 Certificate**

```
-----BEGIN CERTIFICATE-----
MIIDSzCCAlKgAwIBAgIRAMByHusGrZsHeA+k20j2yUwCgYIKoZlZj0EAWMwXzELMARGA1UEBBMC
RVMAHDAAaBgnVBAoTElNlY3RmZ28gKEVlcm99ZSkgU09wMjAwBgNVBAMTKVNY3RmZ28gUXVhbGlm
aWVkdjE5dHJyYV9wYXN0eS50dHJyYV9wYXN0eS50dHJyYV9wYXN0eS50dHJyYV9wYXN0eS50dHJy
OVowXzELMARGA1UEBBMCRWMAHDAAaBgnVBAoTElNlY3RmZ28gKEVlcm99ZSkgU09wMjAwBgNVBAMT
JlNlY3RmZ28gUXVhbGlmYWkiE5hdHJyYV9wYXN0eS50dHJyYV9wYXN0eS50dHJyYV9wYXN0eS50dHJy
SM49AwEHAQABChB36F7EP=skjmdjD909mHAWSZOASlcs5maYlUNvRCeWZdalmpY73iXQ
Ud2Pg=QgADbW6Tb8DPg=BgjggFvMIlBazABgNVHSMGDAWgBTHAVKc3GY9Axp/QmkDpsle4Q
yzAdBgNVHQ4EFgQUGZAWkVUvEbnWfYUblMhMdsGowDgYDVROPAQHBAQDAgGGMBlGGA1UdEwEB
wQIMAYBANCAGAwHQYDVRRBIBYFAFYIKwYBBQCjHawKCCSsGAQUFBwMEMBEGAlUjIjOjIjOjIjOjIj
VR0gADBQBgNVHR8ESTBIMEWgQ6BBB9odHRwOi8vY3JlLnNY3RmZ28gY29hLnNY3RmZ28gRWFz
aWZpWROyXRlcmFslUGVyc29wIm9ydEU0NSJicm9wYAGCCsGAQUFBwEBBHQwYjBLBggrBgEFBQcw
AoYjIHR5dWw1L2NwKzZzWm0aWdLmNvN09SZWVhWdVXVhbGlmYWkiIm94XlhmZlBicm9vdjY=
b3RFNDUyY3JmZ28gKEVlcm99ZSkgU09wMjAwBgNVBAMTKVNY3RmZ28gUXVhbGlmYWkiE5hdHJyYV9w
AwNnADBkAjAwIQVzmkYP=RFJb4VSeg=UVOjZ24TTCAs3x+syUQ=RKSDo68pE9KD0mCqgVet0psC
MAoBkq=4ob6mPjPDHRUZOHAzSD0AopDEy5yHbBkY9QToOvB5vUSoc5JcFOL++JQ==
-----END CERTIFICATE-----
```

**Signature algorithm:** SHA384withECDSA

**Issuer CN:** Sectigo Qualified Natural Person Root E45

**Issuer O:** Sectigo (Europe) SL

**Issuer C:** ES

**Subject CN:** Sectigo Qualified Natural Person CA E35

**Subject O:** Sectigo (Europe) SL

**Subject C:** ES

**Valid from:** Mon Oct 05 02:00:00 CEST 2020

**Valid to:** Fri Oct 05 01:59:59 CEST 2035

**Public Key:** 30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:2A:86:48:CE:3D:03:01:07:03:42:00:04:28:40:8F:7E:85:93:B1:0F:FA:99:09:99:D8:C3:F5:0F:4C:FC:70:16:F1:93:80:F7:57:1A:E6:60:18:90:83:72:44:20:9E:89:6A:C3:68:B9:85: C9:5E:F7:8B:75:D6:51:DD:8F:83:E4:20:00:36:F2:E9:36:FF:F0:33:EA:F8:11

**Authority Key Identifier** C7:E1:52:9C:DC:66:31:F4:0C:4F:FD:0A:A7:28:3A:6C:D5:EE:10:CB

**Subject Key Identifier** C4:6E:19:01:62:AD:55:4B:C4:84:D5:87:C9:46:CB:30:79:83:68:6A

**Basic Constraints** IsCA: true - Path length: 0

**Extended Key Usage** id\_kp\_clientAuth

**Certificate Policies** Policy OID: 2.5.29.32.0

**CRL Distribution Points** <http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crl>

**Authority Info Access** <http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootE45.crt>  
<http://ocsp.sectigo.com>

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *53:B2:40:05:FD:13:67:1F:54:99:89:C8:C6:69:05:9E:AB:E7:7A:D1:9D:DE:E1:E7:0F:72:C9:FB:B3:C0:D9:F9*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Natural Person CA E35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *xG4ZAWKtVUvEhNWHyUbLMHmDaGo=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2021-05-05T01:00:00Z*

**43.4.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**43.5 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Natural Person CA R35”****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by “Sectigo Qualified Natural Person CA R35”*





**CRL Distribution Points** <http://crl.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crl>

**Authority Info Access** <http://crt.sectigo.com/SectigoQualifiedNaturalPersonRootR45.crt>  
<http://ocsp.sectigo.com>

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *AC:86:68:30:D7:B8:D7:12:73:C7:CD:E0:57:A8:D5:3E:93:4C:4E:6F:16:94:7D:13:8A:12:3C:BE:C8:C6:3B:DE*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Natural Person CA R35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *579kEFIBPKaDCbD8o02jaEBSjQA=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2021-05-05T01:00:00Z*

**43.5.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**43.6 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Legal Person CA E35”****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by “Sectigo Qualified Legal Person CA E35”*



**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *D1:1D:91:67:B7:6C:CF:32:AF:9F:FE:0D:5B:F6:6A:82:BB:56:85:40:AE:39:F5:96:54:41:FB:BD:55:E1:D9:D8*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Legal Person CA E35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *dD9zNWOUlhuO8c13qKgLdXK7FWM=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.6.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**43.7 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Legal Person CA R35”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by “Sectigo Qualified Legal Person CA R35”*

**Name** *[ es ]* *Certificados cualificados emitidos por “Sectigo Qualified Legal Person CA R35”*

**Service digital identities****Certificate fields details**



**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *33:95:96:69:16:F8:D3:9D:CE:B5:F7:5C:FF:8B:8E:F4:ED:CB:36:2B:1C:0C:27:92:4D:A4:2D:07:D  
D:18:F1:59*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Legal Person CA R35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *rO4i+LmL8e5yExqRb6TiTfIU7BQ=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.7.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**43.8 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural E35”****Service Type Identifier**

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural E35”*

**Name** *[ es ]* *Certificados cualificados emitidos por “Sectigo Qualified Website Authentication CA Natural E35”*

**Service digital identities**



**Authority Info Access** <http://crt.usertrust.com/USERTrustECCAAACA.crt>  
<http://ocsp.usertrust.com>

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *A9:84:1D:2E:47:CB:E6:D7:1D:8F:AF:DF:38:38:7F:93:F4:3D:76:D7:92:50:4E:FB:17:A2:10:20:C5:8C:0B:89*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Website Authentication CA Natural E35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *Vy25bdRf++aTI2b1N+s/HmAHHaA=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.8.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication>

**43.9 - Service (granted): Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural R35”****Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>

**Service type description** *[en] A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*  
*[es] Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

**Service Name**

**Name** *[ en ]* *Qualified Certificates issued by “Sectigo Qualified Website Authentication CA Natural R35”*





**Basic Constraints** *IsCA: true - Path length: 0*

**Extended Key Usage** *id\_kp\_serverAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*

**CRL Distribution Points** *http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl*

**Authority Info Access** *http://crt.usertrust.com/USERTrustRSAAAACA.crt*  
*http://ocsp.usertrust.com*

**Key Usage:** *digitalSignature - keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *33:9E:6B:92:BE:54:59:F2:6A:8D:C3:C5:F3:72:09:33:C8:38:E2:36:60:1B:05:00:48:C0:47:A1:23:E6:F8:E7*

**X509SubjectName**

**Subject CN:** *Sectigo Qualified Website Authentication CA Natural R35*

**Subject O:** *Sectigo (Europe) SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *5dbQQcJHwMRygaU+LRlY6VsIKTg=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2021-05-05T01:00:00Z*

**43.9.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication*

## 44 - TSP: Docuten Tech SL

### TSP Name

**Name** [ en ] *Docuten Tech SL*

**Name** [ es ] *Docuten Tech SL*

### TSP Trade Name

**Name** [ en ] *Docuten*

**Name** [ es ] *DOCUTEN TECH SL*

**Name** [ en ] *VATES-B85630978*

### PostalAddress

**Street Address** [ en ] *C/ GAMBRINUS 7,1º D*

**Locality** [ en ] *A CORUÑA*

**Postal Code** [ en ] *15008*

**Country Name** [ en ] *ES*

### ElectronicAddress

**URI** [ en ] *mailto:administracion@docuten.com*

**URI** [ en ] *https://docuten.com/en*

**URI** [ es ] *https://docuten.com/es*

### TSP Information URI

**URI** [ en ] *https://docuten.com/en/pcsc/*

## 44.1 - Service (granted): Certificados cualificados emitidos por “DOCUTEN TECH CA1”

### Service Type Identifier

*http://uri.etsi.org/TrstSvc/Svctype/CA/QC*

**Service type description** [ en ] *A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*

[ es ] *Hay un servicio de generación de certificados crear y firmar certificados reconocidos sobre la base de la identidad y otros atributos verificados por los servicios de registro pertinentes.*

### Service Name



**Valid from:** *Fri Sep 18 10:52:21 CEST 2020*

**Valid to:** *Sun Sep 18 10:52:21 CEST 2033*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100AD19045F2653B1FA3AC9A627B1D428B8FD54F4CS263B10412A35AE061280ECC10  
0B CA DC 50 75 F1 95 BC D4 32 8F E1 F4 41 8D 33 AB BA 98 80 DD B0 E9 DE 69 8D EC 3E A9 4A 04 2F 1B 9D 06 DA E9 9C B5 23 DA 43 56 7F 3E ED 15 16 D8 58 97 FB 9C AB F2 BE 04 FE 8D 6D AC 55 DF D  
F 9F 7B DC 7C FA 94 16 F0 97 3D 37 18 8A 76 75 F1 A0 0D CC EA SE CC 79 7B 4D 92 22 23 93 F8 0F 56 A8 5E 6F 66 3C 14 63 12 F0 5B A0 8D 42 A4 40 CA A2 2B 35 A9 77 03 B5 6B 0D 87 18 D2 03 10 67 5E 93  
B9 A7 B4 A3 8B 6D 46 71 80 03 86 EA 77 3F EC 38 C8 F6 9D 85 FC BE A4 59 E9 12 ED 3C A9 91 9E 73 D1 E7 6C 89 27 A1 E6 D5 E4 CB D3 F4 4A CE E9 C3 4F 03 1F 41 35 94 E0 3D B3 3F 07 DE B6 E2 40 7E D1  
05 F2 4C C7 23 6A 35 52 80 85 1F CD 65 78 17 33 F0 93 7B 06 19 5A EA A3 24 E0 E5 9F BE 91 83 25 73 CB 00 A5 78 D4 F6 D4 46 EF F9 60 A1 28 C4 5E C1 8F 8D A6 A4 71 01 46 0F 0F 25 2F 1E 47 D3 54 2B 9E A  
1 FE F6 C2 11 5A 1B 97 D9 37 E8 F4 32 D5 22 41 29 11 0E 0E 93 EA 0E E3 DD 43 00 20 33 B6 10 2F 3F C5 61 5E B6 F4 8D 11 BE 01 0E 7B B9 EE 76 D8 14 16 E8 2A 39 B0 11 2F BB DB 05 01 B0 F2 E0 04 46 87 0  
A 90 FE AF 11 99 B5 3A 26 3B A3 EB E5 CE DD 0D 78 67 64 16 F8 61 38 ED D3 9C 7D 81 64 A8 63 D2 DF 68 6E 03 02 32 28 A5 E4 ED 50 DC 77 24 EE 7B 42 6A 24 5C 0F 60 30 EF 51 63 0A 88 6A 35 DB 03 ED E  
D 3E E0 B2 7B 1F 3C 6A DC 88 B5 3F 2B 47 6F AB 70 F8 38 16 26 63 A1 E8 12 53 F8 CC 35 EA 48 3C F7 FB 15 00 F0 ED 0A 9D 5E 0A 6E 45 D1 5C 02 17 1E BB 27 A2 3E 78 A0 41 D0 23 5B 08 8F E5 31 F8 ED F  
7 C1 36 80 67 8F 0D BF 36 AF 3F 45 60 69 17 1A 90 68 CD C7 EB 02 03 01 00 01

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Authority Key Identifier**  
*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

**Issuer Alternative Name**  
*info@uanataca.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <https://www.docuten.com/es/psc/cps/>*  
*CPS text: [Subordinate Certification Authority Certificate of / Certificado de la Autoridad de Certificacion Subordinada de / Docuten tech - [www.docuten.com](http://www.docuten.com)]*

**CRL Distribution Points**  
[http://crl1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://crl2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Subject Alternative Name**  
*info@docuten.com*

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*B0:CD:0C:09:3E:A1:D6:52:75:40:14:C6:AF:2E:2B:B2:1B:E1:83:8E:95:8E:90:6B:05:50:5E:CB:AD  
:60:BD:97*

**X509SubjectName**

**Subject 2.5.4.97:**  
*VATES-B85630978*

**Subject CN:**  
*DOCUTEN TECH CA1*

**Subject OU:**  
*TSP-PSC-DOCUTEN*

**Subject O:**  
*Docuten Tech SL*

**Subject L:**  
*A CORUÑA*

**Subject C:**  
*ES*

**X509SKI**

**X509 SK I** *cOMl/c2pcj9RgNYiekdikmYuv1g=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time** *2021-07-01T01:00:00Z*

**44.1.1 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**44.1.2 - Extension (critical): additionalServiceInformation****AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**44.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*  
*[es] undefined.*

**Criteria list assert=atLeastOne****Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.56098.1.1.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.56098.1.2.2.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.56098.1.3.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.56098.1.4.2*

**Policy Identifier:**



**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B85630978

**Subject CN:** DOCUTEN timestamping electronic certificate – TSU01

**Subject OU:** TSP-PSC-DOCUTEN

**Subject O:** DOCUTEN TECH SL

**Subject L:** A CORUÑA

**Subject C:** ES

**Valid from:** Thu Oct 08 12:18:54 CEST 2020

**Valid to:** Sun Oct 08 12:18:54 CEST 2028

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B238B759F0576849E74839816D5DA6750DBE9095FCF2003507B538A2CDEFD117731E4224E6EC4D13E1CA2738521FC5849B7E7E76CC5ACD1C4933274A1B76B58DC91AE273B102AC7CC41C44521F9AF99B95510B8350A56A5966751B91CCDC4C202AD5410B4352C5FB3DF1C9F96E9AF2FA0496E185B1227A6E6B5B65777522CA6577B84DE1A8C434C9290F0C4708D2B5CE3C3B2A042CBB455761DA811FD9414049DFD2C2126106411EB824658867525F7E00C50D4FB60D17A61EF84EB60C18E8AD C7062DC26B4FAA248096DC06A2329C0259128A99F6C7648D342B0178A517281AD19A7BFA82E7BE898A59137278B13740D67A88579580E20AAC593E3BDA3DEC770203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
01:AF:82:55:07:48:16:15:15:00:95:28:30:EA:03:48:68:2B:32:16

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
70:E3:25:FD:CD:A9:72:3F:51:80:D6:22:7A:47:62:92:66:2E:BF:58

**Issuer Alternative Name**  
info@docuten.com

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.56098.2.10  
CPS pointer: <https://www.docuten.com/es/pcsc/cps/>  
CPS text: [Timestamping electronic certificate]  
Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://cr1.uanataca.com/public/pki/crl/docuten.crl>  
<http://cr2.uanataca.com/public/pki/crl/docuten.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Subject Alternative Name**  
info@docuten.com

**Key Usage:**  
digitalSignature

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:** 64:B2:6E:B2:72:6D:47:CA:A4:95:2F:E1:C2:88:E0:59:9E:94:5B:C7:DC:56:03:16:16:85:0B:4A:FB:39:A7:E6

**X509SubjectName**

**Subject 2.5.4.97:** VATES-B85630978

**Subject CN:** DOCUTEN timestamping electronic certificate – TSU01

**Subject OU:** TSP-PSC-DOCUTEN

**Subject O:** DOCUTEN TECH SL

**Subject L:** A CORUÑA

**Subject C:** ES

**X509SKI**

**X509 SK I** Aa+CVQdIFhUVAJUoMOoDSGgrMhY=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2021-07-01T01:00:00Z



**45 - TSP: MAILTECK, S.A.****TSP Name**

**Name** [ es ] *MAILTECK, S.A.*

**Name** [ en ] *MAILTECK, S.A.*

**TSP Trade Name**

**Name** [ en ] *MAILTECK*

**Name** [ en ] *VATES- A31501901*

**Name** [ en ] *Mailteck SA*

**PostalAddress**

**Street Address** [ en ] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

**Locality** [ en ] *Leganés*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28914*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

**Locality** [ es ] *Leganés*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28914*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:infomadrid@mailteck.com*

**URI** [ en ] *https://comunicaciones-legales.mailteck.com/*

**URI** [ es ] *https://comunicaciones-legales.mailteck.com/*

**TSP Information URI**



**Issuer C:** ES

**Subject 2.5.4.97:** VATES-A31501901

**Subject CN:** CertySign

**Subject SERIAL NUMBER:** A31501901

**Subject O:** Mailteck SA

**Subject C:** ES

**Valid from:** Fri Feb 12 14:23:00 CET 2021

**Valid to:** Wed Feb 11 14:23:00 CET 2026

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A02820101009F62BC7D9BC372C3C7C4D4700253499D8C37AE0B0E0E03856AF09DC756AD0E7BE6F3F  
B2F476F082375D476C8E9B6F97E13D17764B499E0E8589894E4EB29CF69F36B794E929783DCE5782B27AF0CBF5A30C1E3D08C5F572DA8922E8FE3A26D84B9B17  
A6201499F266F8AF8009DA33C257D2CE7D100FC68BF0DD59F7F5774B7A789CBF3752C6B7B67864F3563F8E677DB0B6875EEA01CA10E08654150D90463AE3D2679  
209EE45EC3D6443EE40C46F317039AE0BDA3BA9742FC215313A580041B33BE882390F11B214CD445CCA4CE0B0E1926CA3D1C7B400B3B24574EA46DB55AE792E2D  
DE3B785123704CCA2110A8018E2A873EE01BE1B2F9FA3FEAC30203010001

**QCStatements - crit. = false**  
id\_etsi\_qcs\_QcCompliance  
id\_etsi\_qcs\_RetentionPeriod: 15  
id\_etsi\_qcs\_QcSSCD

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
87:DB:A5:98:1F:19:9C:48:9A:F8:02:38:F1:8C:BA:AD:5F:13:16:87

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5

**Certificate Policies**  
Policy OID: 0.4.0.194112.1.3  
Policy OID: 1.3.6.1.4.1.47286.1.9.6  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Qualified certificate for e-seal in Remote QSCD]

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage**  
id\_kp\_clientAuth

**Subject Alternative Name**  
comunicacionescertificadas@mailteck.com

**Key Usage:**  
digitalSignature - nonRepudiation - keyEncipherment

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:** 46:3B:20:D1:F6:C5:71:8A:4E:5D:22:A5:FC:3D:09:DC:83:2E:2A:2C:C7:50:1F:AE:6D:5B:EE:B8:2B:2B:1D:B5

**X509SubjectName**

**Subject 2.5.4.97:** VATES-A31501901

**Subject CN:** CertySign

**Subject SERIAL NUMBER:** A31501901

**Subject O:** Mailteck SA

**Subject C:** ES

**X509SKI**

**X509 SK I** h9ulmB8ZnEia+AI48Yy6rV8TFoc=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time**

2021-09-01T01:00:00Z

**46 - TSP: CUSTOMER COMMUNICATIONS TECKNALIA, S.L.****TSP Name**

**Name** [ es ] *CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*

**Name** [ en ] *CUSTOMER COMMUNICATIONS TECKNALIA, S.L.*

**TSP Trade Name**

**Name** [ en ] *CUSTOMER COMMS*

**Name** [ en ] *VATES-B86414000*

**Name** [ en ] *CUSTOMER COMMUNICATIONS TECKNALIA SL*

**PostalAddress**

**Street Address** [ en ] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

**Locality** [ en ] *Leganés*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28914*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Polígono Industrial La Laguna, Avenida de la Recomba 14*

**Locality** [ es ] *Leganés*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28914*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info@customercomms.com*

**URI** [ en ] *https://www.customercomms.com*

**URI** [ es ] *https://www.customercomms.com*

**URI** [ es ] *mailto:info@customercomms.com*



**Issuer L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Issuer C:** *ES*

**Subject 2.5.4.97:** *VATES-B86414000*

**Subject CN:** *CertySign*

**Subject SERIAL NUMBER:** *B86414000*

**Subject O:** *CUSTOMER COMMUNICATIONS TECKNALIA SL*

**Subject C:** *ES*

**Valid from:** *Fri Feb 12 14:21:00 CET 2021*

**Valid to:** *Wed Feb 11 14:21:00 CET 2026*

**Public Key:** *30820122300D06092A864886F70D01010105000382010F003082010A0282010100BA07785F9DD38A04A0C1849DEC9C90368AE124A2EE2FD09001DD2265E4298CAD4D9A  
F0013756E13202DB992CBA85D50C42EEAAE6E960AE2BFFD72247BA8C9010821FA37999CB920D528017AFAADEDAE8478B854B25FA4DCD9CAE88390159ACF87  
85173AE2F3BAAFC044099C0E127FF88E397F3347EB132AC347D7A3E3DA764FD100E64B6E99596AF6724B7FDFC079A97C5E8F14E818E0F8DD2C3806746D0414F4AEAF  
D3C1F826D1B7FF14793002D84B876734944DBD9C88BAF7597CE5181B8873FA23D1418DC30911B4057726B5648AD0FCADF1DF821DDDA75466AE90BA7D7C9B8C  
E0D2E1DD194522FD9D9F7F3728SD2B4392EEFB164F1653795D7CEF6C90203010001*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Authority Info Access** *[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)*  
*<http://ocsp1.uanataca.com/public/pki/ocsp/>*  
*<http://ocsp2.uanataca.com/public/pki/ocsp/>*

**Subject Key Identifier** *DE:AA:E3:DC:09:D0:D0:F0:A4:9B:80:1A:80:EA:64:26:AF:12:1B:D0*

**Basic Constraints** *IsCA: false*

**Authority Key Identifier** *2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

**Certificate Policies** *Policy OID: 0.4.0.194112.1.3*  
*Policy OID: 1.3.6.1.4.1.47286.1.9.6*  
*CPS pointer: <https://www.uanataca.com/public/cps/>*  
*CPS text: [Qualified certificate for e-seal in Remote QSCD]*

**CRL Distribution Points** *<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>*  
*<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>*

**Extended Key Usage** *id\_kp\_clientAuth*

**Subject Alternative Name** *comunicacionescertificadas@customercomms.com*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *04:2B:A1:E7:60:3B:28:12:F8:C1:25:2B:D1:29:D0:E5:21:F6:A2:A5:28:9A:08:36:89:F3:A5:EF:A5:28:5A:8C*

### **X509SubjectName**

**Subject 2.5.4.97:** *VATES-B86414000*

**Subject CN:** *CertySign*

**Subject SERIAL NUMBER:** *B86414000*

**Subject O:** *CUSTOMER COMMUNICATIONS TECKNALIA SL*

**Subject C:** *ES*

### **X509SKI**

**X509 SK I** *3qrj3AnQ0PCkm4AagOpkJq8SG9A=*

### **Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2021-09-01T01:00:00Z*



**47 - TSP: Iberexaminis Consulting S.L.****TSP Name**

**Name** [ en ] *Iberexaminis Consulting S.L.*

**Name** [ es ] *Iberexaminis Consulting S.L.*

**TSP Trade Name**

**Name** [ en ] *EXAMINIS*

**Name** [ es ] *EXAMINIS*

**Name** [ en ] *VATES-B39877915*

**Name** [ en ] *Iberexaminis Consulting SL*

**PostalAddress**

**Street Address** [ en ] *CALLE JOAQUIN CAYON 14 4ª*

**Locality** [ en ] *TORRELAVEGA*

**State Or Province** [ en ] *CANTABRIA*

**Postal Code** [ en ] *39300*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *CALLE JOAQUIN CAYON 14 4ª*

**Locality** [ es ] *TORRELAVEGA*

**State Or Province** [ es ] *CANTABRIA*

**Postal Code** [ es ] *39300*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info@iberexaminis.com*

**URI** [ en ] *https://www.iberexaminis.com*

**TSP Information URI**



**Subject 2.5.4.97:** VATES-B39877915

**Subject CN:** Examinis TSU01

**Subject OU:** IBEREXAMINIS TSP

**Subject O:** Iberexaminis Consulting SL

**Subject L:** Torrelavega

**Subject C:** ES

**Valid from:** Thu Jan 14 13:18:01 CET 2021

**Valid to:** Sun Jan 14 13:18:01 CET 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100F3E73E081D0932DBF63F438FA1F38F565CE81FA3B340D40E0CF5D0DBB2522C41E57815  
A2A2E1D7D4A29944D0F4687E5AFA953C31FAD20BB09100B60BCBA7752F2457E331E8A84383D7B0719BF89DBE0DF55440E30EEA14125B3AD1DC58F0846BB3E33D24B  
969F403DC4AEF7E054C06B70386FC0782FC72838F7F05A62C98578FFA08FE8F88A0DB39D8B47BF3C9921F262C9B441E0593ECB72C11D121651B2CCF1F56860CB5  
E3470E765F084E4779CBEB62705FC0A4873187D8396B0389861477185C00B1C2B7A529C8440BC630F119E1AB1AC0C3F078ACDECA6578AF741D2A0356D6E935A64995  
07F7A02ABE567F972CC225E4F0AD0DDBF03F446E42764545770203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
79:D2:C4:CF:54:E0:99:39:45:7D:D3:1B:E1:67:DE:6E:16:C2:DC:46

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
7D:57:E7:60:73:CE:07:46:A9:E2:A3:68:F0:E1:11:B2:74:92:73:FD

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.47286.2.5  
CPS text: [Certificado de sello de tiempo electrónico.]  
CPS pointer: <https://www.uanataca.com/public/cps/>  
Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Subject Alternative Name**  
info@iberexaminis.com

**Key Usage:**  
digitalSignature

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**  
54:A9:49:39:DE:E1:89:3D:A5:74:AD:98:DB:46:B4:58:C0:22:82:1B:BE:AA:7A:78:02:47:2F:A3:46  
:75:2A:12

X509SubjectName

**Subject 2.5.4.97:** VATES-B39877915

**Subject CN:** Examinis TSU01

**Subject OU:** IBEREXAMINIS TSP

**Subject O:** Iberexaminis Consulting SL

**Subject L:** Torrelavega

**Subject C:** ES

**X509SKI**

**X509 SK I** edLEz1TgmTIFdMb4WfebhbC3EY=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn>

**Service status description** [en] undefined.

[es] undefined.

**Status Starting Time** 2023-11-08T00:00:00Z

**47.1.1 - History instance n.1 - Status: granted**

**Service Type Identifier** <http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST>

**Service Name**

**Name** [en] Qualified electronic time stamps issued by "Examinis TSU01"

**Name** [es] Sellos electrónicos cualificados de tiempo emitidos por "Examinis TSU01"

**Service digital identities****X509SubjectName**

**Subject 2.5.4.97:** VATES-B39877915

**Subject CN:** Examinis TSU01

**Subject OU:** IBEREXAMINIS TSP

**Subject O:** Iberexaminis Consulting SL

**Subject L:** Torrelavega

**Subject C:** ES

**X509SKI**

**X509 SK I**

*edLEz1TgmTIFfdMb4WfebhbC3EY=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Status Starting Time**

*2021-10-04T01:00:00Z*

**48 - TSP: Lleidanet PKI S.L.****TSP Name**

**Name** [ en ] *Lleidanet PKI S.L.*

**Name** [ es ] *Lleidanet PKI S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B97458996*

**Name** [ en ] *INDENOVA*

**Name** [ en ] *inDenova SL*

**Name** [ en ] *Indenova S.L.*

**Name** [ en ] *Lleidanet PKI*

**PostalAddress**

**Street Address** [ en ] *Carrer dels Traginers, 14 – 2º B*

**Locality** [ en ] *Valencia*

**State Or Province** [ en ] *Valencia*

**Postal Code** [ en ] *46014*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Carrer dels Traginers, 14 - 2ºB*

**Locality** [ es ] *Valencia*

**State Or Province** [ es ] *Valencia*

**Postal Code** [ es ] *46014*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:indenova@indenova.com*

**URI** [ en ] *https://www.indenova.com*



**Issuer O:** *Indenova SL*

**Issuer SERIAL NUMBER:** *B97458996*

**Issuer OU:** *Certification Authority Indenova SL*

**Issuer L:** *Valencia*

**Issuer C:** *ES*

**Subject 2.5.4.13:** *inDenova Subordinate CA 003*

**Subject CN:** *inDenova SUB CA 003*

**Subject O:** *inDenova SL*

**Subject 2.5.4.97:** *VATES-B97458996*

**Subject SERIAL NUMBER:** *B97458996*

**Subject OU:** *Certification Authority inDenova SL*

**Subject T:** *Subordinate Certificate Authority inDenova SL*

**Subject L:** *VALENCIA*

**Subject C:** *ES*

**Valid from:** *Mon May 31 10:32:46 CEST 2021*

**Valid to:** *Fri May 31 10:32:46 CEST 2041*

**Public Key:**  
30820222300D06092A864886F70D010105000382020F003082020A0282020100B72FA317D4C4A2225F21D8C5F1FC009F1658A059E68B1F71D8099A4841CE92CF29ABD  
FCC566E0598E309AD61A95CBB2F46230F79462E5E3C620E6E7042144E9F0F06D1E8D1B23E4B817E32902115BC138257F245DAEBC86B48D83A81157503C918657A94  
B4E4A28256A114BDB8907C8F61B59DFBC9320DF0B52F03F5353544E6167E.E36507E776030A33CF5585448C8B3DEC7695435F36F9F1EA16EA8B6BEA38AD3624D.A70B  
1840A69816FD57A1F60DCA8ADA2F5CA8C4C.F8D25D.A08F5F7D55E7EA4A8038DE6A958F.FE58231C90BE55C831B4D92D38AA3F70F67655AA21668912449112D3571  
86143D5FC0AF6D621BEB8A1D49C99CA78E.E8F8D864AA2AB62C021E7E8D283C1D3CF1F05F3BA71B580DC32A3903F5D0B05E.A9F5E567DE760E195E1E431E1B99E8038  
B9EE7ADB06E91C559A924B59E2F6982E2A4679156770D43A20B679DD7B3158417260850929D7215F785349486BB663C11B423113BE891A72B7371D8ABEAEC8868180  
BA229A85AF79536FB00AC8537DCD11789621451B1A546489BD2232B053BAE9F8BA4B45D3631D14911DC2713A4DD3DBE47406924FD241C3359023E1930D2D6B8CD6  
0163B4D37E7B8901A7294C9878FC0E96F55EC11AB0914D5C70B8E229C40D99188EC56C03010E00AF255E3D4C852E67457388BC793B4C64E0909FB30C4C643041C486F.C4  
2B135A182D50F12C1B349E.DF941CA32096193F0203010001

**Subject Key Identifier** *C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46*

**Authority Key Identifier** *B9:A1:B7:83:14:F5:DA:D8:BC:10:89:01:C0:E2:D2:C5:F7:A0:3F:1B*

**Extended Key Usage** *id\_kp\_clientAuth*

**Certificate Policies** *Policy OID: 2.5.29.32.0*  
*CPS pointer: [http://cps.esigna.es/sub/cps\\_sub003\\_ca.pdf](http://cps.esigna.es/sub/cps_sub003_ca.pdf)*

**Authority Info Access** *[http://certs.esigna.es/root/ca\\_root\\_indenova\\_sl.crt](http://certs.esigna.es/root/ca_root_indenova_sl.crt)*  
*<http://ocsp2.esigna.es>*

**Basic Constraints** *IsCA: true - Path length: 0*



**CRL Distribution Points**  
[http://crl.esigna.es/root/ca\\_root\\_indenova\\_sl.crl](http://crl.esigna.es/root/ca_root_indenova_sl.crl)  
[http://crl1.esigna.es/root/ca\\_root\\_indenova\\_sl.crl](http://crl1.esigna.es/root/ca_root_indenova_sl.crl)

**Key Usage:** *keyCertSign - cRLSign*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *34:52:E9:67:43:44:26:07:F2:1D:85:08:4C:3D:B8:97:E3:75:49:FE:D2:3F:13:5C:DB:D2:02:E6:90:D5:2E:25*

**X509SubjectName**

**Subject 2.5.4.13:** *inDenova Subordinate CA 003*

**Subject CN:** *inDenova SUB CA 003*

**Subject O:** *inDenova SL*

**Subject 2.5.4.97:** *VATES-B97458996*

**Subject SERIAL NUMBER:** *B97458996*

**Subject OU:** *Certification Authority inDenova SL*

**Subject T:** *Subordinate Certificate Authority inDenova SL*

**Subject L:** *VALENCIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *w5x0XdAiqO3y7lC+r6l7aymAbEY=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-12-13T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**48.1.1 - Extension (critical): additionalServiceInformation**

AdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a>
-----	--------	---

48.1.2 - Extension (critical): additionalServiceInformationAdditionalServiceInformation

URI	[ en ]	<a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</a>
-----	--------	---

48.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]

Qualifier type description	[ en ]	undefined.
	[ es ]	undefined.

## Criteria list assert=atLeastOne

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.1
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.2
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.1.3.3
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.1
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.2
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.2.3.3
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.1
------------	-------------	-------------------------------------

## Policy Identifier:

Identifier	[ OIDsURN ]	urn:oid:1.3.6.1.4.1.49959.1.1.3.3.2
------------	-------------	-------------------------------------



**Issuer SERIAL NUMBER:** B97458996

**Issuer OU:** Trusted Timestamp Service inDenova SL

**Issuer T:** Service Timestamping inDenova SL

**Issuer L:** VALENCIA

**Issuer C:** ES

**Subject 2.5.4.13:** inDenova SL Timestamping Certificate 003

**Subject CN:** inDenova TSU 003

**Subject O:** inDenova SL

**Subject 2.5.4.97:** VATES-B97458996

**Subject SERIAL NUMBER:** B97458996

**Subject OU:** Trusted Timestamp Service inDenova SL

**Subject T:** Service Timestamping inDenova SL

**Subject L:** VALENCIA

**Subject C:** ES

**Valid from:** Mon May 31 10:53:49 CEST 2021

**Valid to:** Sat May 31 10:53:49 CEST 2031

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100B6D9EE847B3AD823E8843838D05C02AF8883BEA522CDF48687BF46F3265EFAE3257D657722BDA3FC3A522D659F639746CD1EE8AB0915E722B740CDE1E0C5498E5D0785831F0EADAE06D31E76C5334997413BEAB12A5BFB2991736678835F2A2AC1D0CEC02F5D5803664CCDEDE4173BBE2763E0A2BE372C33380FB20AD722A.CE57086D73493FD1A3BE633337E06D881BD6DC1BFDA023855058FB8355BAB3AD806D5CE8339054756E6EFC0A20C78D204AF281C1D2349F6FC36E01A1C805B2834A1CB8100892122FE0E26CC495038B31CCKE1E869A6C0CF0D4A8B1EB0452ED21D300AB4D2E2C01D079F79469EAD04E2830DAF82C21FDA2F8E9474E531D5B51866F865C4E19F18F8719E94E3CB7026CB84191E3314379ACN1E21E7A39B607E835621E84E805B0A16C16E7978DA256E1743EE7C2C8F8E8A7C3974AD3F1017C64ED8ED3B04A4EPEDECOA95D529FBB017079FFE2F4A6DB6C482153743D69B8168CCCF728C7BFE22A1AA00FE948A2F56E49BD3822D7C6CF79DD9B4B2F30980EC3BF5C7E2F1A583B481DAD509741233483FEA593AE717A7E52A426DA9A1E7E4085C19421C3C217EC6A7588AEAS83407F180C952D388A54343499498F938E9284072C11E44DE80BFE9DCFE8A1D86B24ACDE6A0586BD070DF256FE294F3183B11C49635FEFA35A0F699B64AC522687065894D1192E87C64EEBD3025C94973C6DF90203010001

**Subject Key Identifier** 90:69:12:08:5C:DA:C0:64:CE:86:0D:60:EF:FA:7A:34:75:2C:EB:B8

**Authority Key Identifier** 2B:6E:5E:F1:DA:66:7D:B6:E7:AE:1F:60:6E:9E:DA:3A:3F:B3:EF:B1

**Extended Key Usage** id\_kp\_timeStamping

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.49959.1.1.5  
 CPS pointer: [http://cps.esigna.es/tsa/cps\\_tsa003.pdf](http://cps.esigna.es/tsa/cps_tsa003.pdf)  
 CPS text: [Warranty limitations of this certificate can be found in the CPS]

**Authority Info Access**  
[http://certs.esigna.es/tsa/indenova\\_tsa\\_003.crt](http://certs.esigna.es/tsa/indenova_tsa_003.crt)  
<http://ocsp2.esigna.es>

**Basic Constraints** IsCA: false

**CRL Distribution Points** [http://crl.esigna.es/tsa/indenova\\_tsa\\_003.crl](http://crl.esigna.es/tsa/indenova_tsa_003.crl)  
[http://crl1.esigna.es/tsa/indenova\\_tsa\\_003.crl](http://crl1.esigna.es/tsa/indenova_tsa_003.crl)

**Key Usage:** *digitalSignature - nonRepudiation*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *83:77:19:18:FB:57:38:FC:75:5A:43:90:41:67:C2:21:9D:D9:3A:C4:69:81:7B:14:33:D0:14:9E:65:B0:23:6D*

**X509SubjectName**

**Subject 2.5.4.13:** *inDenova SL Timestamping Certificate 003*

**Subject CN:** *inDenova TSU 003*

**Subject O:** *inDenova SL*

**Subject 2.5.4.97:** *VATES-B97458996*

**Subject SERIAL NUMBER:** *B97458996*

**Subject OU:** *Trusted Timestamp Service inDenova SL*

**Subject T:** *Service Timestamping inDenova SL*

**Subject L:** *VALENCIA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *kGkSCFzawGTOhg1g7/p6NHUs67g=*

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** *[en] undefined.*  
*[es] undefined.*

**Status Starting Time**

*2021-12-13T02:00:00Z*

**Scheme Service Definition URI**

**URI** *[es]* <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

**URI** *[en]* <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>



**Issuer T:** *Subordinate Certificate Authority inDenova SL*

**Issuer L:** *VALENCIA*

**Issuer C:** *ES*

**Subject 2.5.4.97:** *B97458996*

**Subject 2.5.4.13:** *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

**Subject CN:** *(B97458996) Indenova S.L.*

**Subject OU:** *Dirección*

**Subject O:** *Indenova S.L.*

**Subject SERIAL NUMBER:** *44864081M*

**Subject ST:** *VALENCIA*

**Subject L:** *VALENCIA*

**Subject E:** *equipocrypto@indenova.com*

**Subject C:** *ES*

**Valid from:** *Fri Jul 09 11:08:44 CEST 2021*

**Valid to:** *Mon Jul 08 11:18:44 CEST 2024*

**Public Key:** *30820122300D06092A864886F70D01010105000382010F003082010A0282010100A0BA2FCC1CA581CDF400717373680596418C550E7846A1E4193391C74ED854E86FB22831A54B041E0165C82C0C25E0055A12B09003B6D3856B83EE8FC8D56A88CD4CDD2B97942BECDB5918831F6A1FBDD22EBA836EC3F4F15B565CCFE848D8E5925C5DAD7CB1FB675698C152A4074FEAAAB2E2F795AA849F20F2C5A4A9CFE15700B425FCB2DB199B29E36E8818FA39C4ECD0779DB21E62152A91367C658F96D8B878A28B3E3417CF2BA4A2CD14E34A59303DD72265AE408F104AFB98275559C94A9EB747CB7AE3C1A855E6B1E0168AE655C9DBC82942E728AFD530BC431E6BC98C643F47F85DEEDF7A2DEED596885178D384E3C54E451A2199893F9435E0CF8F0203010001*

**Basic Constraints** *isCA: false*

**Extended Key Usage** *Unknown ExtendedKeyUsage OID: 1.3.6.1.4.1.311.10.3.4 - id\_kp\_clientAuth - id\_kp\_smartcardlogon*

**Subject Key Identifier** *56:BF:03:6B:D1:B8:A3:B7:10:98:40:37:51:7F:14:44:A4:5C:18:E9*

**Authority Info Access** *http://ocsp2.esigna.es*  
*http://certs.esigna.es/ca/indenova\_pki\_003.crt*

**Authority Key Identifier** *C3:9C:74:5D:D0:22:A8:ED:F2:EE:50:BE:AF:AD:7B:6B:29:80:6C:46*

**CRL Distribution Points** *http://crl1.esigna.es/sub/indenova\_pki\_003.crl*  
*http://crl.esigna.es/sub/indenova\_pki\_003.crl*

**Certificate Policies***Policy OID: 1.3.6.1.4.1.49959.1.1.3.4.1**CPS pointer: [http://cps.esigna.es/sub/cps\\_sub003\\_ca.pdf](http://cps.esigna.es/sub/cps_sub003_ca.pdf)**CPS text: [Terms of use at CPS [http://cps.esigna.es/sub/cps\\_sub003\\_ca.pdf](http://cps.esigna.es/sub/cps_sub003_ca.pdf)]**Policy OID: 0.4.0.194112.1.1***QCStatements - crit. = false***id\_etsi\_qcs\_QcCompliance**id\_etsi\_qcs\_RetentionPeriod: 15***Key Usage:***digitalSignature - nonRepudiation***Thumbprint algorithm:***SHA-256***Thumbprint:***51:FC:B0:0B:7B:B7:1E:8C:6D:6F:0A:23:24:9E:E0:BF:F3:59:85:C8:C2:AD:7E:8A:B9:8A:D2:DE:  
DA:60:82:99***X509SubjectName****Subject 2.5.4.97:***B97458996***Subject 2.5.4.13:***Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003***Subject CN:***(B97458996) Indenova S.L.***Subject OU:***Dirección***Subject O:***Indenova S.L.***Subject SERIAL NUMBER:***44864081M***Subject ST:***VALENCIA***Subject L:***VALENCIA***Subject E:***equipocrypto@indenova.com***Subject C:***ES***X509SKI****X509 SK I***Vr8Da9G4o7cQmEA3UX8URKRcGOk=***Service Status***<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>***Service status description***[en]**undefined.**[es]**undefined.***Status Starting Time***2023-11-08T00:00:00Z***Scheme Service Definition URI**



URI [ en ] <https://avancedigital.mineco.gob.es/en-us/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

URI [ es ] <https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/SchemeService.aspx>

#### 48.3.1 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

#### 48.3.2 - Extension (critical): additionalServiceInformation

##### AdditionalServiceInformation

URI [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

#### 48.3.3 - History instance n.1 - Status: granted

Service Type Identifier <http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q>

#### Service Name

Name [ es ] *Servicio de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados del proveedor «Indenova S.L.»*

Name [ en ] *Validation service of qualified electronic signatures and qualified electronic seals of the TSP «Indenova S.L.»*

#### Service digital identities

#### X509SubjectName

Subject 2.5.4.97: B97458996

Subject 2.5.4.13: *Certificado de Sello Electrónico Software - Emitido por inDenova SUB CA 003*

Subject CN: *(B97458996) Indenova S.L.*

Subject OU: *Dirección*

Subject O: *Indenova S.L.*

Subject SERIAL NUMBER: 44864081M

Subject ST: VALENCIA

**Subject L:** VALENCIA  
**Subject E:** equipocrypto@indenova.com  
**Subject C:** ES

**X509SKI**

**X509 SK I** Vr8Da9G4o7cQmEA3UX8URKRcGOk=

**Service Status** <http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Status Starting Time** 2021-12-13T02:00:00Z

**48.3.3.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures>

**48.3.3.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** [ en ] <http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals>

**49 - TSP: BTP ONETEC, S.L.****TSP Name**

**Name** [ en ] *BTP ONETEC, S.L.*

**Name** [ es ] *BTP ONETEC, S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B33943564*

**Name** [ es ] *VATES-B33943564*

**Name** [ en ] *BTP ONETEC*

**PostalAddress**

**Street Address** [ en ] *C/ La Mecánica, 305. Polígono Industrial La Peñona*

**Locality** [ en ] *GIJÓN*

**State Or Province** [ en ] *ASTURIAS*

**Postal Code** [ en ] *33211*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ La Mecánica, 305. Polígono Industrial La Peñona*

**Locality** [ es ] *GIJÓN*

**State Or Province** [ es ] *ASTURIAS*

**Postal Code** [ es ] *33211*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:info@btponetec.es*

**URI** [ en ] *https://www.btponetec.es*

**URI** [ es ] *mailto:info@btponetec.es*

**URI** [ es ] *https://www.btponetec.es*



**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B33943564

**Subject CN:** BTP QUALIFIED TSU01

**Subject OU:** BTP TSP

**Subject O:** BTP ONETEC, S.L.

**Subject L:** GIJON

**Subject C:** ES

**Valid from:** Tue Sep 21 18:37:09 CEST 2021

**Valid to:** Fri Sep 21 18:37:09 CEST 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100A53E5821C88F61268B4497E0AD4FA81824B09172D0973A27BE70AC9529C24F822276E9E9AECF233CD1162B7C95E2326C611C88D4859B0E0E0C83F3DA95FF753121B4B2460CCB9CB44B7A9DC7405CB0A85C1CBDC104324F4C2F5DBF218355C24DB412F162B402D4E7E16172D0EB1324F2958E42EDFB299FC7BB8B68E6F72BA5D082BB247DB1AD4EB148ED4EABB139B80A51EB62D69311CDB873FC3123BFBA3B4D31BE2B3F236FED3D002862685662A9C60F35F43A8FFA5B440A669D9788A7503D936AC91D07DDBB91C7D9C34934CAFFD486FFE848B1D18570BA740D53A1962421A4F57A4DC1300D88FA0A102DB64C991D08EB C2B82E0D22E12F0863696890203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
 2C:64:0F:E5:8E:29:B0:8A:5A:2A:73:7D:E4:09:41:A2:C0:62:A8:AB

**Basic Constraints**  
 IsCA: false

**Authority Key Identifier**  
 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

**Issuer Alternative Name**  
 info@uanataca.com

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.47286.2.5  
 CPS pointer: <https://www.uanataca.com/public/cps/>  
 CPS text: [Certificado de sello de tiempo electrónico.]  
 Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://cr1.uanataca.com/public/pki/crl/2021CA1sub.crl>  
<http://cr2.uanataca.com/public/pki/crl/2021CA1sub.crl>

**Extended Key Usage**  
 id\_kp\_timeStamping

**Subject Alternative Name**  
 info@btponetec.es

**Key Usage:**  
 digitalSignature

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:** 09:91:3A:8F:69:B5:42:55:93:4A:40:E1:27:12:AF:D1:D5:B9:9A:95:C0:EC:23:12:7F:3B:32:99:40:29:1A:0D

**X509SubjectName**

**Subject 2.5.4.97:** VATES-B33943564  
**Subject CN:** BTP QUALIFIED TSU01  
**Subject OU:** BTP TSP  
**Subject O:** BTP ONETEC, S.L.  
**Subject L:** GIJON  
**Subject C:** ES

**X509SKI**

**X509 SK I** LGQP5Y4psIpaKnN95AlBosBiqKs=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description** [en] undefined.  
[es] undefined.

**Status Starting Time** 2022-02-08T00:00:00Z

**50 - TSP: AVIVA VOICE SYSTEMS AND SERVICES, S.L.****TSP Name**

**Name** [ es ] AVIVA VOICE SYSTEMS AND SERVICES, S.L.

**Name** [ en ] AVIVA VOICE SYSTEMS AND SERVICES, S.L.

**TSP Trade Name**

**Name** [ en ] VATES-B84216142

**Name** [ en ] Aviva Voice Systems and Services SL

**PostalAddress**

**Street Address** [ en ] C/ Golfo de Salónica 27 Planta 5ª puerta B

**Locality** [ en ] MADRID

**State Or Province** [ en ] MADRID

**Postal Code** [ en ] 28033

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] C/ Golfo de Salónica 27 Planta 5ª puerta B

**Locality** [ es ] MADRID

**State Or Province** [ es ] MADRID

**Postal Code** [ es ] 28033

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ en ] <mailto:info@avivavoice.com>

**URI** [ en ] <http://www.avivavoice.com/>

**URI** [ es ] <http://www.avivavoice.com/>

**URI** [ es ] <mailto:info@avivavoice.com>

**TSP Information URI**





**Subject CN:** AVIVA VOICE QUALIFIED TSU01

**Subject OU:** AVIVA VOICE TSP

**Subject O:** Aviva Voice Systems and Services SL

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Wed Nov 03 17:23:26 CET 2021

**Valid to:** Mon Nov 05 17:23:26 CET 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100A0049603DB2D24165E7CFFE209EF36A2DDC88AB35841482C2521322256C68A0E8347B7  
 C8842618D4538B97083372C5ADFFEA5B4B8E28E0AE861A69CE827E5986B67E372497D0D785931D05CAF1B477FCA95CC493FFC4256A1384408AC9E0D832C21243B  
 7667C7FE671E1D4D8E9C0F37D50E76ACF362A513CB4ACB20643A48AC743C2E725E00F4AB63CD2560929A37D2E0D8FCFF3631DEED6EB9A472BA7D5C1D40A751  
 0B46D49FD31F221CCFE2FB8E8E145A7725695246212D41C24C4077CB99066E56726AC0989003BE5FC06C9F8868F8363463AA60AB54EF534DDABFA58995227317  
 640802AFBD7C3BC736C390997A0AF42B3B679B246E581C514F70203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
 B8:AD:4D:19:60:55:57:7F:D7:C7:95:2A:5B:A5:54:7B:67:4F:E5:5E

**Basic Constraints**  
 IsCA: false

**Authority Key Identifier**  
 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

**Issuer Alternative Name**  
[info@uanataca.com](mailto:info@uanataca.com)

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.47286.2.5  
 CPS pointer: <https://www.uanataca.com/public/cps/>  
 CPS text: [Certificado de sello de tiempo electrónico.]  
 Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>  
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

**Extended Key Usage**  
 id\_kp\_timeStamping

**Subject Alternative Name**  
[info@avivavoice.com](mailto:info@avivavoice.com)

**Key Usage:**  
 digitalSignature

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 95:42:8E:4B:2F:9C:AD:1F:59:44:D7:CA:D8:E7:E7:F9:75:71:84:CE:65:09:86:9D:E8:F8:DE:33:18:  
 D4:26:AE

X509SubjectName

**Subject 2.5.4.97:** *VATES-B84216142*

**Subject CN:** *AVIVA VOICE QUALIFIED TSU01*

**Subject OU:** *AVIVA VOICE TSP*

**Subject O:** *Aviva Voice Systems and Services SL*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *uK1NGWBVV3/Xx5UqW6VUe2dP5V4=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-03-29T00:00:00Z*

**51 - TSP: ASETEC INGENIERIA DE SISTEMAS, S.L.****TSP Name**

**Name** [ es ] *ASETEC INGENIERIA DE SISTEMAS, S.L.*

**Name** [ en ] *ASETEC INGENIERIA DE SISTEMAS, S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B82149139*

**Name** [ en ] *ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK*

**PostalAddress**

**Street Address** [ es ] *Calle Jaenar nº 27*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28043*

**Country Name** [ es ] *ES*

**PostalAddress**

**Street Address** [ en ] *Calle Jaenar nº 27*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28043*

**Country Name** [ en ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:pscc@mensatek.com*

**URI** [ en ] *https://www.mensatek.com*

**URI** [ es ] *https://www.mensatek.com*

**URI** [ es ] *mailto:pscc@mensatek.com*

**TSP Information URI**



**Subject 2.5.4.97:** VATES-B82149139

**Subject CN:** MENSATEK QUALIFIED TSU01

**Subject OU:** MENSATEK TSP

**Subject O:** ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK

**Subject L:** MADRID

**Subject C:** ES

**Valid from:** Tue Sep 21 19:19:13 CEST 2021

**Valid to:** Fri Sep 21 19:19:13 CEST 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100E26E5F7E7E17BDFCC1E3F369C89230D3145DA2F3004DDB10C7DE8C6D4D583A4B391F0BCCE5283AC08A713537319B0D553F6A65E8AB9D57F55694D095AE463F1ACECDDE81AC1FE2D00C84B20DDCC49207FCB422DA9E03B4A4448256B5B637986A7AB4E88B97B8E07C444271209DE179BD483F37594EBB72D7544A05093CD7B8B3850F16CE7D7CA5379799DCDDB93BA1249AD51377B41D7F29E7BF34E7BD158016160EC8400F46A913BD7225932AAF968840B4CBA888E1A3C96F4CC7BA24B903EDE612F1DCA75D459F3F4201FB0C1CF900651A04F7DE0C4DC57B295E36CA69B8AF48D17C4E6EE7BA120D41EBC0033C85B2C52289766076F255B3CD75EF462AD0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
 CC:35:F5:32:59:05:A6:71:E7:48:5A:3C:B6:AB:37:62:AF:75:18:AB

**Basic Constraints**  
 IsCA: false

**Authority Key Identifier**  
 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68

**Issuer Alternative Name**  
 info@uanataca.com

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.47286.2.5  
 CPS pointer: <https://www.uanataca.com/public/cps/>  
 CPS text: [Certificado de sello de tiempo electrónico.]  
 Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>  
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

**Extended Key Usage**  
 id\_kp\_timeStamping

**Subject Alternative Name**  
 tsa@mensatek.com

**Key Usage:**  
 digitalSignature

**Thumbprint algorithm:**  
 SHA-256

**Thumbprint:**  
 EC:C7:39:8F:DF:BC:16:E3:14:45:47:E2:E8:0A:64:F8:1F:9B:F7:50:23:EA:F9:4F:F9:70:B2:B1:E0:6F:16:A8

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B82149139*

**Subject CN:** *MENSATEK QUALIFIED TSU01*

**Subject OU:** *MENSATEK TSP*

**Subject O:** *ASETEC INGENIERIA DE SISTEMAS SL - MENSATEK*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *zDX1MlkFpnHnSFo8tqs3Yq91GKs=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-05-31T00:00:00Z*

**52 - TSP: 3G SOLUCIONES MOVILIDAD, S.L.****TSP Name**

**Name** [ es ] 3G SOLUCIONES MOVILIDAD, S.L.

**Name** [ en ] 3G SOLUCIONES MOVILIDAD, S.L.

**TSP Trade Name**

**Name** [ en ] VATES-B09444431

**Name** [ en ] 3G MOBILE GROUP

**Name** [ en ] 3G SOLUCIONES MOVILIDAD SL

**PostalAddress**

**Street Address** [ en ] Pasaje Gutiérrez, 3, 1º

**Locality** [ en ] Valladolid

**State Or Province** [ en ] Valladolid

**Postal Code** [ en ] 47002

**Country Name** [ en ] ES

**PostalAddress**

**Street Address** [ es ] Pasaje Gutiérrez, 3, 1º

**Locality** [ es ] Valladolid

**State Or Province** [ es ] Valladolid

**Postal Code** [ es ] 47002

**Country Name** [ es ] ES

**ElectronicAddress**

**URI** [ en ] <mailto:soporte@3gmg.com>

**URI** [ en ] <https://www.3gmg.com>

**TSP Information URI**

**URI** [ en ] <https://www.3gmg.com/>





**Subject CN:** 3G QUALIFIED TSU01  
**Subject OU:** 3G TSP  
**Subject O:** 3G SOLUCIONES MOVILIDAD SL  
**Subject L:** VALLADOLID  
**Subject C:** ES  
**Valid from:** Tue Sep 21 18:53:11 CEST 2021  
**Valid to:** Fri Sep 21 18:53:11 CEST 2029  
**Public Key:** 30820122300D06092A864886F70D01010105000382010F003082010A0282010100C051037A CF508CB5F35D476C9F67299FC15350DC68A21A70189B493137F5DDB7A498E3A66406CD122F0C04474F37D88B5E19DB98C6F411A4B68B60F6281D C6DA8036DD09A3B4FC00B951819E891D8EF9AB C0011586DA9138DF73F0F9EE00FB8AD9AE9C4A0034C9181A953F37405E0B B3E767CC209F43F605F066B3BF03649B6507924E6F13940B7660074C04A322ABCF075E6C D38CEC B710AE1BA80B08DB776002311580C2375A5A13889F448059AA9C5E73ED38A2EFDA2D9BFEFED372A36B7D771D6AC152D0B C38C3764E81EFA205BE3B3718EECC662270A1511981E029599AA4A13B2FCF16788B3B09436E99FB26BF9D1B4F940EB68967A0B18BF66DCF97D0203010001  
**Authority Info Access** <http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>  
**Subject Key Identifier** 85:B5:92:7B:68:4C:CB:E1:C2:11:1D:96:40:C3:D1:B6:2F:EC:D5:43  
**Basic Constraints** IsCA: false  
**Authority Key Identifier** 81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68  
**Issuer Alternative Name** info@uanataca.com  
**Certificate Policies** Policy OID: 1.3.6.1.4.1.47286.2.5  
CPS pointer: <https://www.uanataca.com/public/cps/>  
CPS text: [Certificado de sello de tiempo electrónico.]  
Policy OID: 0.4.0.2042.1.2  
**CRL Distribution Points** <http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>  
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>  
**Extended Key Usage** id\_kp\_timeStamping  
**Subject Alternative Name** soporte@3gmg.com  
**Key Usage:** digitalSignature  
**Thumbprint algorithm:** SHA-256  
**Thumbprint:** 07:0E:12:83:52:CC:3F:65:BB:BA:3C:4D:BF:B4:B0:CE:FC:F9:75:1C:3B:FE:EF:15:11:4A:A5:10:13:D3:1D:FA

X509SubjectName

**Subject 2.5.4.97:** *VATES-B09444431*

**Subject CN:** *3G QUALIFIED TSU01*

**Subject OU:** *3G TSP*

**Subject O:** *3G SOLUCIONES MOVILIDAD SL*

**Subject L:** *VALLADOLID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *hbWSe2hMy+HCER2WQMPRti/s1UM=*

**Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time**

*2022-07-26T00:00:00Z*

**53 - TSP: WISE SECURITY GLOBAL S.L.****TSP Name**

**Name** [ en ] *WISE SECURITY GLOBAL S.L.*

**Name** [ es ] *WISE SECURITY GLOBAL S.L.*

**TSP Trade Name**

**Name** [ en ] *WISE SECURITY GLOBAL*

**Name** [ en ] *VATES-B95732087*

**PostalAddress**

**Street Address** [ en ] *Alameda de Recalde, 34, 2º izq*

**Locality** [ en ] *Bilbao*

**State Or Province** [ en ] *Vizcaya*

**Postal Code** [ en ] *48009*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Alameda de Recalde, 34, 2º izq*

**Locality** [ es ] *Bilbao*

**State Or Province** [ es ] *Vizcaya*

**Postal Code** [ es ] *48009*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:administracion@wsg127.com*

**URI** [ en ] *http://wsg127.com*

**TSP Information URI**

**URI** [ en ] *https://erds-mee.com/*



**Issuer L:** MADRID

**Issuer C:** ES

**Subject C:** ES

**Subject O:** WISE SECURITY GLOBAL S.L.

**Subject OU:** TRUST

**Subject 2.5.4.97:** VATES-B95732087

**Subject CN:** WISE - FIRMA Y CUSTODIA DE EVIDENCIAS DE TERCEROS

**Valid from:** Wed Mar 25 14:08:47 CET 2020

**Valid to:** Sun Mar 24 14:08:47 CET 2024

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100B0DD79DB431379A67588396F08FD135B32EB9767FA035780716021A43246AF8493F3E5198180E753A861D03839EDF978E979B72B594E2E26B1BF66F5BEA14FCAD4A991AF885370E57C266FC184901D20AA024969E0E717788449D12B54A1A940820C5C58FA7E203E844E4F10B47D15AF3C0230B55B5204B7B828D62FE6F472CF92FC7E75B37D917E9B00A0E70029209C48A4E6AD82DF065FD3CAD93E16A097EF1C4B73BD2B0C7E0BA4D666C7CEF999BC825B4945A7CC30DE463F892EDFFEF2625CB630F1A6538868614BC262FDFDB1D6755607CB1C2B586879A486A83918B12DF6CA3394266C:D74D0D438C42B559C89BC1C7F2550A762CFBA7209A9F44FB0203010001

**Basic Constraints** IsCA: false

**Extended Key Usage** id\_kp\_clientAuth

**Subject Key Identifier** 51:31:82:76:E1:CE:ED:86:AC:AF:F3:5B:F7:71:8A:F4:C4:DD:A0:C6

**Authority Info Access**  
[http://www.camerfirma.com/certs/ac\\_camerfirma\\_legal\\_persons-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt)  
<http://ocsp.camerfirma.com>

**Authority Key Identifier** C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42

**CRL Distribution Points**  
[http://crl.camerfirma.com/ac\\_camerfirma\\_legal\\_persons-2016.crl](http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl)  
[http://crl1.camerfirma.com/ac\\_camerfirma\\_legal\\_persons-2016.crl](http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl)

**Subject Alternative Name**  
 info@wsg127.com  
 OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO

**Issuer Alternative Name** ca@camerfirma.com

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2  
 CPS pointer: <https://policy.camerfirma.com>  
 CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en <https://policy.camerfirma.com>]  
 Policy OID: 0.4.0.194112.1.1

**QCStatements - crit. = false**  
 id\_etsi\_qcs\_QcCompliance  
 id\_etsi\_qcs\_RetentionPeriod: 15

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *92:77:34:57:D7:E5:13:93:BF:A4:06:B1:81:AF:A1:39:18:62:25:C2:AF:CF:78:23:F8:7B:D3:C9:46:44:10:76*

#### X509SubjectName

**Subject C:** *ES*

**Subject O:** *WISE SECURITY GLOBAL S.L.*

**Subject OU:** *TRUST*

**Subject 2.5.4.97:** *VATES-B95732087*

**Subject CN:** *WISE - FIRMA Y CUSTODIA DE EVIDENCIAS DE TERCEROS*

#### X509SKI

**X509 SK I** *UTGCduHO7Yasr/Nb93GK9MTdoMY=*

#### Service Status

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-09-06T00:00:00Z*

**54 - TSP: COGNICASE MANAGEMENT CONSULTING, S.L.****TSP Name**

**Name** [ en ] *COGNICASE MANAGEMENT CONSULTING, S.L.*

**Name** [ es ] *COGNICASE MANAGEMENT CONSULTING, S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B80440795*

**Name** [ en ] *CMC*

**Name** [ es ] *CMC*

**Name** [ en ] *COGNICASE MANAGEMENT CONSULTING SL*

**Name** [ es ] *COGNICASE MANAGEMENT CONSULTING SL*

**PostalAddress**

**Street Address** [ en ] *Avenida de Manoteras, 10*

**Locality** [ en ] *MADRID*

**State Or Province** [ en ] *MADRID*

**Postal Code** [ en ] *28050*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Avenida de Manoteras, 10*

**Locality** [ es ] *MADRID*

**State Or Province** [ es ] *MADRID*

**Postal Code** [ es ] *28050*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://www.grupocmc.es*

**URI** [ en ] *mailto:psc.es@cgi.com*





**Issuer L:** *Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))*

**Issuer C:** *ES*

**Subject 2.5.4.97:** *VATES-B80440795*

**Subject CN:** *CMC Prestador Servicios Electrónicos Confianza*

**Subject SERIAL NUMBER:** *B80440795*

**Subject O:** *COGNICASE MANAGEMENT CONSULTING SL*

**Subject C:** *ES*

**Valid from:** *Mon Jun 28 15:53:00 CEST 2021*

**Valid to:** *Wed Jun 28 15:53:00 CEST 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100CFCD46694C8E10694BAAAD1C864AA79FDB5A2D0DDBBF0D874AE DC767EA300419A9A  
1A2202CCD34B06BF9385B5D406259DB68F88F3F49FD3E49930FFB453D1767EE3B030CA1F769FD76CEFF31CC7E477418E78D34A1EFD2C87388117E292217509F0DF3785  
7B2D38ED3F4079761580B199285C255B5A5AD6BCEB7116C8E486385094E84B144995B74B3A2A86B1DB7C8254AA88A42F12FC39BED273849B9A10D48407984FB5E  
B8221358A87AD1E1C723440054B3E756583869D791DD61BBB0708B9CE88F3B6C3B0FABF248429E49B8523A67C09E72271C4D46AF821E5E343A6D971581E63E263E  
C1F41C7D71DAC88B048684792E61B74271FB5CBED48703822130203010001

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crl](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crl)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*28:15:B4:76:8C:73:25:4D:C2:A4:9A:0B:30:3C:03:1B:2D:F1:65:7E*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.1.9.5*  
*CPS text: [Certificado cualificado de Sello Electrónico en HSM centralizado.]*  
*CPS pointer: <https://www.uanataca.com/public/cps/>*  
*Policy OID: 0.4.0.194112.1.1*

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage**  
*id\_kp\_clientAuth*

**Subject Alternative Name**  
*info@grupocmc.es*

**Key Usage:**  
*digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *6D:62:6F:7C:1C:5E:9D:8F:66:E8:54:48:92:7B:A6:CA:18:97:7E:8C:6E:7F:B1:25:DE:BF:63:2E:18:D4:12:B6*

### **X509SubjectName**

**Subject 2.5.4.97:** *VATES-B80440795*

**Subject CN:** *CMC Prestador Servicios Electrónicos Confianza*

**Subject SERIAL NUMBER:** *B80440795*

**Subject O:** *COGNICASE MANAGEMENT CONSULTING SL*

**Subject C:** *ES*

### **X509SKI**

**X509 SK I** *KBW0doxzJU3CpJoLMDwDGy3xZX4=*

### **Service Status**

*<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-09-13T00:00:00Z*

**55 - TSP: SERVICIOS DE MAILCERTIFICADO SL****TSP Name**

**Name** [ en ] *SERVICIOS DE MAILCERTIFICADO SL*

**Name** [ es ] *SERVICIOS DE MAILCERTIFICADO SL*

**TSP Trade Name**

**Name** [ en ] *CODICERT*

**Name** [ es ] *CODICERT*

**Name** [ en ] *VATES-B85804532*

**PostalAddress**

**Street Address** [ en ] *Embajadores 181B Local 9*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *MADRID*

**Postal Code** [ en ] *28045*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Embajadores 181B Local 9*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *MADRID*

**Postal Code** [ es ] *28045*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *http://codicert.io*

**URI** [ es ] *http://codicert.io*

**URI** [ en ] *mailto:administracion@codicert.io*

**URI** [ es ] *mailto:administracion@codicert.io*



**Issuer OU:** ANF Autoridad Intermedia de Identidad

**Issuer O:** ANF Autoridad de Certificacion

**Issuer L:** Barcelona (see current address at <http://www.anf.es/es/address-direccion.html> )

**Issuer ST:** Barcelona

**Issuer C:** ES

**Subject 2.5.4.97:** VATES-B85804532

**Subject CN:** CODICERT-SEC

**Subject OU:** Certificado Cualificado de Sello Electronico

**Subject O:** SERVICIOS DE MAILCERTIFICADO SL

**Subject L:** MADRID

**Subject ST:** MADRID

**Subject C:** ES

**Subject SERIAL NUMBER:** B85804532

**Valid from:** Fri Apr 29 14:00:10 CEST 2022

**Valid to:** Wed Apr 29 14:00:10 CEST 2026

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D25B1BFB10E6E154DAFC8F6293190E73F5895AF20EDB70E5964D382C6BAE28AD0F0349223EA23084A3FD355A8E35F9E50E8D7E5A5BE86ECFB2865A8C83B46EEF9CD129C4EABE655CB4182EF2216AD4C86B6D8A040AD6A4CA71A1BC1D09538145297D93CD88175C6E6EDBD184335DD6FDS36A39A49A63D99E653B8F4EFD6720B0B38893BF7E7A38A7C71EC2D4600CF3D0C4BA2379F713E9B38E08E6757732524423C49E622E26F6B0D807043A7F058992916B0245A4005B99458B615431B8570AB4380940F708D7872E515654C85D5DC632584F616387840F2D99A25A781B9B8CD36010B593B6DF61EA220C073D0EA54450A93464746C340C717FE41AA8BCA7127E10205010001

**Authority Key Identifier** 35:2E:2D:E6:29:1C:BF:8B:D9:4A:7C:9E:2B:E0:95:47:D1:C6:4F:3D

**Subject Key Identifier** EF:23:D4:C3:48:B4:60:2D:70:42:E0:4E:1E:25:8E:D7:7C:76:8F:8B

**Subject Alternative Name** no-reply@codicert.net

**Extended Key Usage** id\_kp\_clientAuth

**CRL Distribution Points** [http://www.anf.es/crl/ANF\\_Assured\\_ID\\_CA1\\_SHA256.crl](http://www.anf.es/crl/ANF_Assured_ID_CA1_SHA256.crl)

**Certificate Policies**  
 Policy OID: 1.3.6.1.4.1.18332.25.1.1.1  
 CPS pointer: <https://www.anf.es/documentos>  
 Policy OID: 0.4.0.194112.1.1

**Authority Info Access**  
<http://ocsp.anf.es/spain/AV>  
[http://www.anf.es/es/certificates\\_download/ANF\\_Assured\\_ID\\_CA1\\_SHA256.cer](http://www.anf.es/es/certificates_download/ANF_Assured_ID_CA1_SHA256.cer)

**Basic Constraints** *IsCA: false*

**QCStatements - crit. = false** *id\_etsi\_qcs\_QcCompliance*

**Key Usage:** *digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:** *SHA-256*

**Thumbprint:** *26:60:06:51:7C:8D:5A:21:76:34:2A:C3:6E:60:8A:8B:9E:0B:D0:05:80:AA:20:90:96:D5:19:E8:DB:E4:82:63*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B85804532*

**Subject CN:** *CODICERT-SEC*

**Subject OU:** *Certificado Cualificado de Sello Electronico*

**Subject O:** *SERVICIOS DE MAILCERTIFICADO SL*

**Subject L:** *MADRID*

**Subject ST:** *MADRID*

**Subject C:** *ES*

**Subject SERIAL NUMBER:** *B85804532*

**X509SKI**

**X509 SK I** *7yPUw0i0YC1wQuBOHiWO13x2j4s=*

**Service Status**

*http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-10-10T00:00:00Z*

**56 - TSP: FACTORYNET AUGUSTA, S.L.****TSP Name**

**Name** [ en ] *FACTORYNET AUGUSTA, S.L.*

**Name** [ es ] *FACTORYNET AUGUSTA, S.L.*

**TSP Trade Name**

**Name** [ en ] *FACTORYMAIL*

**Name** [ en ] *VATES- B50980804*

**Name** [ en ] *FACTORYNET AUGUSTA SL*

**PostalAddress**

**Street Address** [ en ] *C/ VELAZQUEZ, 10, 1º A*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28001*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ VELAZQUEZ, 10, 1º A*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28001*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *https://www.factorymail.es*

**URI** [ en ] *mailto:admon@factorymail.es*

**TSP Information URI**

**URI** [ en ] *https://www.factorymail.es/politicas-factorymail*

**56.1 - Service (granted): Servicio cualificado de entrega electrónica certificada emitido para FACTORYNET AUGUSTA S.L.**

**Service Type Identifier**

<http://uri.etsi.org/TrstSvc/Svctype/EDS/Q>

Service type description

[en] An electronic delivery service providing qualified electronic deliveries.  
 [es] Un servicio de entrega electrónica proporcionando entregas electrónicas reconocidas.

**Service Name**

Name

[es] Servicio cualificado de entrega electrónica certificada emitido para FACTORYNET AUGUSTA S.L.

Name

[en] Qualified electronic certified delivery service issued for FACTORYNET AUGUSTA S.L.

**Service digital identities**

**Certificate fields details**

Version:

3

Serial Number:

8760835572502450359

X509 Certificate

```
-----BEGIN CERTIFICATE-----
MIH3jCCBseAwIBAgILZS9uUgdULcwDQYJKoZIhvcNAQELBQAwgbczAIBgNVBAYTAkVMTUQw
QgYDVQIDDCYXJzW3YxbmFgKHNIZSBJdXJzW50GfEZHJic3MeYXQgd3dLnVhbmF0YWNlLnNv
S3N0ZGRZLN0KTEWMBGGA1UEGmVlYXQvR0R0M0g1b7EjLjEwMBGGA1UECwwvVFUQXzIzLnNk
MR0wGAYDVQDDBFVQU5BVEFESDQ0EgMjAxNjE5YmYGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYm
DTIwMTkNAANdewMfoXDTEzMTkNAANdewMfoXDTEzMTkNAANdewMfoXDTEzMTkNAANdewMfo
Q1RFR0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0R0
ZSBkZ2NlbnVudG9zMR0wGAYDVQDDBFVQU5BVEFESDQ0EgMjAxNjE5YmYGA1UEYmVGA1UEYm
A4IBDWAwegEKAAIBAAQDM280M4b1SOP4Lzathow1N-Rb3ODGbkusaY4cWkrcHQ15-RCLPCV
InoWb7mS80SmPKV1Dm2ksof7-GVYQ4uuXNwzAMU1YQA1LmLsqHf0wvcm9772Zb
qhx4d0ISFauzVChqVg56Cw0f80sgDGOXHEGjXRPDW5LsksRv1zBUlnnaHNVc4ibW8iCT
45Eps0UJEMR6gnraUcnznZ91ZPsUBDmHlavH5Z3VQc7axGk8tky8VhHS8+QKRgV5pXPs
SP0yeEhAasSILsdmTIGZL0kroONPwclHb987dGcUp9wzly0V0AgMBAAGgggM0MDDDB8
BgerBGFEB0cBAwRwMG4wCAyGBACORgEEMAsG8GQAJYBAWIBDZAIByEAI5GAQOwNgYGBACORgE
MCwwKHyaalR0cHM6Lj93d3cudWfYXRbY2EuY29lL3BlYm91e3YyYm91e3YyYm91e3YyYm91
CQYHBAQOgGGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1
YXRbY2EuY29lL3BlYm91e3YyYm91e3YyYm91e3YyYm91e3YyYm91e3YyYm91e3YyYm91e3
cn0wNgYIKwYBBQUHMAAGKmb0dHA6Lj9yY3NwMSS1YW5hdGZlYSSp20weHVhMjJL3BraS9y3Nw
LkZ3BgerBGFEB0cBAwRwMG4wCAyGBACORgEEMAsG8GQAJYBAWIBDZAIByEAI5GAQOwNgY
MBOGA1UdDgQWBBSuR-EsGml9UFL0bzZWhRb2tpzAMBgNVHRMBAI8EAAAMBBGA1UdIwQYMBAA
FC1z77Bj#X94MhR49EDECBT03IMRGZBgNVHSAEZeWgY4wCQYHBAQOgGGA1UEYmVGA1UEYm
VGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1
MDOGCsGAOUFBwCMDEMLIF1YWspmlZCBjZXU0aWp2Y2F0ZSBmb3ZlZlZlZlZlZlZlZlZlZl
ZSBRU0NEMjB6bnVHR8EgYcwgYQwKA=odDyGombdHA6Lj9ycmwwLmVhbmF0YWNlLnNvbnB3
WmVscGpl2NysC3Q0TEZdWJcmRpbmFkYS5ScmwwDgYDR0PAQHBAQDAgXgMB0G
A1UdQAwMBQGCsGAOUFBwMCBgerBGFEB0cBAwRwMG4wCAyGBACORgEEMAsG8GQAJYBAWIB
DZAIByEAI5GAQOgGGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1UEYmVGA1
m4cF5JURM5STcT2bXcEATw1CalzHx6dJSD75=SuU2L17nP4nb640jaVdhrTzJ=3kcp
hHdaA6MplD90ep9M3RzdwaEKZLjgS2m8H7gehHblU2S3MaDz20GRn4Y1rscWp0Z=do
ID0M6VcKask8mKkSIXLQV5z2G22YKH07Bh1PwB09uLzGIM7pWwBPM4y
FYQRUXhAQH9E3zak0W7D1u3Hnpg3k6Z7QeYtGrQuC1uUE14clv1DLZ16U131Cs2FPd4
36m48vscEngy9mwF9aAP40KQGIzxubhwE3k8vBVhVJ88mRWSFmz7TuaDpxxyZkKm0G
DEZZV0sgZm8NF=dlRwAdmEg2g1CuU0J_gRc4PR6G21Z7uQhXcv709w0F5KgdF5c
zg2z3Thez93VB6GhR9cp4uZ8JSMjEBS0Xk5LXZ195FHWZGTfWq61g1SzoDqzmdwpx
KHZYUnlLa1OC58eLkZ7lcvEj1zE=HX1RUZAY9CEhbaUZNL9eHC2+CkoQZmYmcwNbkDE
iHlRkImmsdVGRpEccZk3QKz1p=
-----END CERTIFICATE-----
```

Signature algorithm:

SHA256withRSA

Issuer 2.5.4.97:

VATES-A66721499

Issuer CN:

UANATACA CA1 2016

Issuer OU:

TSP-UANATACA

Issuer O:

UANATACA S.A.

Issuer L:

Barcelona (see current address at [www.uanataca.com/address](http://www.uanataca.com/address))

Issuer C:

ES

Subject 2.5.4.97:

VATES-B50980804



**Subject CN:** *Firma de documentos*

**Subject SERIAL NUMBER:** *B50980804*

**Subject O:** *FACTORYNET AUGUSTA SL*

**Subject C:** *ES*

**Valid from:** *Thu Dec 16 09:47:00 CET 2021*

**Valid to:** *Sat Dec 16 09:47:00 CET 2023*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D67CDBCF4CE1B.D5:23:8FE242F36A:2868C3:53:7E:45BDCE94:319BBA:4B:AC:898E:1C:58AA:D  
C1D0FE22E7E4422CF095267A:34321EF799CD8C6D29BF3C:AS490E:ES86:76:C9FC:EF:1:957C:24388A:EF:ES:SD:78:F067:83:14:8D:84:00:D4:99:CB:B2:AC:41:A7E2:70C7FB:67:AF:DE:DF:EF:6  
7:DB:AA:1C:5D:8F:888E:239167BB:354686A56AE7A089C3:FD:1F:8F:C3:AC:8C:31902171:C41A:3C9744:F0:D6:DD:47:AC:92:C46F:D6:DC:C1:50:D3:5A:1C:D5:9E:E2:56:D6:F0:97:13:E3:91:0F:B0:EE:09  
11F31183:A9:EA:AF:15:27:72:76:65:F7:56:4F:B1404399C1:DF:6A:F1:F9:67:95:50:BF:B6:B1:18:A77C:C6:29:32:F1:5B:C8:1D:29:FC:F9:02:91:81:5E:69:5F:F3:E8:48:F3:B2:C0:47:DD:01:A6:92:30:BD:DD:99:3D:46:  
23:62:FA:92:B3:BF:36:D1:56:79:41:DB:7B:DB:11:ED:D4:06:0A:AA:67:F6:FC:F4:CB:46:03:02:03:01:00:01

**QCStatements - crit. = false**  
*id\_etsi\_qcs\_QcCompliance*  
*id\_etsi\_qcs\_RetentionPeriod: 15*  
*id\_etsi\_qcs\_QcSSCD*

**Authority Info Access**  
[http://www.uanataca.com/public/download/tsp\\_certificates/subordinate1.crt](http://www.uanataca.com/public/download/tsp_certificates/subordinate1.crt)  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*AE:47:E1:2C:1B:F9:8B:F5:41:4B:8F:4C:EA:65:68:5F:46:1D:9F:A7*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*2D:71:EF:B0:63:7F:F5:FD:E0:83:22:44:7F:44:10:30:81:4F:4D:E5*

**Certificate Policies**  
*Policy OID: 0.4.0.194112.1.3*  
*Policy OID: 1.3.6.1.4.1.47286.1.9.6*  
*CPS pointer: https://www.uanataca.com/public/cps/*  
*CPS text: [Qualified certificate for e-seal in Remote QSCD]*

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl>  
<http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl>

**Extended Key Usage**  
*id\_kp\_clientAuth*

**Subject Alternative Name**  
*admon@factorymail.es*

**Key Usage:**  
*digitalSignature - nonRepudiation - keyEncipherment*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*14:28:B7:9E:5B:9B:E1:4A:C6:76:1B:36:C3:F5:FF:16:DE:E6:4D:20:BB:83:48:7C:E3:19:C3:B4:47:  
A7:15:E4*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B50980804*

**Subject CN:** *Firma de documentos*

**Subject SERIAL NUMBER:** *B50980804*

**Subject O:** *FACTORYNET AUGUSTA SL*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *rkfhLBv5i/VBS49M6mVoX0Ydn6c=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2022-12-22T00:00:00Z*

**57 - TSP: FULL CERTIFICATE S.L.****TSP Name**

**Name** [ en ] *FULL CERTIFICATE S.L.*

**Name** [ es ] *FULL CERTIFICATE S.L.*

**TSP Trade Name**

**Name** [ en ] *FULL CERTIFICATE, WEVOTE, AVISOS CERTIFICADOS*

**Name** [ es ] *FULL CERTIFICATE, WEVOTE, AVISOS CERTIFICADOS*

**Name** [ en ] *VATES- B87336178*

**Name** [ en ] *FULL CERTIFICATE SL*

**PostalAddress**

**Street Address** [ en ] *BOIX Y MORER 6, 9*

**Locality** [ en ] *Madrid*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28003*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *BOIX Y MORER 6, 9*

**Locality** [ es ] *Madrid*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28003*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *https://www.fullcertificate.com*

**URI** [ en ] *mailto:admin@fullcertificate.com*

**TSP Information URI**



**Issuer OU:** *see current address at <https://www.camerfirma.com/address>*

**Issuer ST:** *MADRID*

**Issuer L:** *MADRID*

**Issuer C:** *ES*

**Subject C:** *ES*

**Subject O:** *FULL CERTIFICATE SL*

**Subject OU:** *DIRECCIÓN*

**Subject OU:** *IT*

**Subject 2.5.4.97:** *VATES-B87336178*

**Subject CN:** *FULL CERTIFICATE*

**Valid from:** *Thu Mar 26 13:31:56 CET 2020*

**Valid to:** *Mon Mar 25 13:31:56 CET 2024*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100DF43023E7122A06D4F5B18023684479D31475E5BBF4167EC7328AF88338FA60A684AD3A3882DFEA260BC48462644B7D65E522D6769BFD366B4C440923C4654B0C24F60D85E39578C8E4AD1230F3078DA448DC117F48303C12AD3E36E4C938E2C79ACD28DDCA650A3FF383ADC39697C2520BEA3BF8365D7BFADDF4E2CDEA681EB7D91A3D3D3904D073102D51B364DB6E1017E6C1098F8795BA6A462F4591CF0C9F60FF0FEAFA54FA9BE8D2DBA31A1EC0331A783D6CD4489A1905EDE3AD0312BA809B0C6B8AE4C3F98DB521BD7649A48DA950FA5E39DCA30F34CAADB3D049A21BA427E264A6676BC14EF455604D795A864F298C575B1A660E304ABFD3D9D0203010001

**Basic Constraints** *IsCA: false*

**Extended Key Usage** *id\_kp\_clientAuth*

**Subject Key Identifier** *7D:DF:5F:7F:C2:E7:DF:49:2A:45:77:EE:5C:3D:E4:44:53:64:22:64*

**Authority Info Access**  
*[http://www.camerfirma.com/certs/ac\\_camerfirma\\_legal\\_persons-2016.crt](http://www.camerfirma.com/certs/ac_camerfirma_legal_persons-2016.crt)*  
*<http://ocsp.camerfirma.com>*

**Authority Key Identifier** *C3:27:85:93:D7:2F:96:C5:1B:AC:76:33:D9:86:A2:4A:7D:68:14:42*

**CRL Distribution Points**  
*[http://crl.camerfirma.com/ac\\_camerfirma\\_legal\\_persons-2016.crl](http://crl.camerfirma.com/ac_camerfirma_legal_persons-2016.crl)*  
*[http://crl1.camerfirma.com/ac\\_camerfirma\\_legal\\_persons-2016.crl](http://crl1.camerfirma.com/ac_camerfirma_legal_persons-2016.crl)*

**Subject Alternative Name**  
*certificate@fullcertificate.com*  
*OID.1.3.6.1.4.1.17326.30.10=CERTIFICADO ELECTRONICO CUALIFICADO DE SELLO ELECTRONICO*

**Issuer Alternative Name** *ca@camerfirma.com*

**Certificate Policies**

Policy OID: 1.3.6.1.4.1.17326.10.16.2.1.2

CPS pointer: <https://policy.camerfirma.com>CPS text: [Certificado cualificado de sello electronico. Consulte las condiciones de uso en <https://policy.camerfirma.com>]

Policy OID: 0.4.0.194112.1.1

**QCStatements - crit. = false**

id\_etsi\_qcs\_QcCompliance

id\_etsi\_qcs\_RetentionPeriod: 15

**Key Usage:**

digitalSignature - nonRepudiation - keyEncipherment

**Thumbprint algorithm:**

SHA-256

**Thumbprint:**

5A:FD:53:AA:CF:4C:A4:0E:E4:03:A0:C2:71:83:7E:A5:3F:30:77:19:12:29:CA:B6:0B:AC:E3:97:AF:5A:41:4E

**X509SubjectName****Subject C:**

ES

**Subject O:**

FULL CERTIFICATE SL

**Subject OU:**

DIRECCIÓN

**Subject OU:**

IT

**Subject 2.5.4.97:**

VATES-B87336178

**Subject CN:**

FULL CERTIFICATE

**X509SKI****X509 SK I**

fd9ff8Ln30kqRXfuXD3kRFNkImQ=

**Service Status**<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-02-15T00:00:00Z

**58 - TSP: DEH NOTIFICACION ELECTRONICA HABILITADA S.L.****TSP Name**

**Name** [ en ] *DEH NOTIFICACION ELECTRONICA HABILITADA S.L.*

**Name** [ es ] *DEH NOTIFICACION ELECTRONICA HABILITADA S.L.*

**TSP Trade Name**

**Name** [ en ] *VATES-B86198306*

**Name** [ en ] *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

**Name** [ en ] *DEH ONLINE*

**PostalAddress**

**Street Address** [ en ] *C/ Sierra de Cazorla, 1, Entreplanta, Oficina H, Edificio Cimaga*

**Locality** [ en ] *Las Matas - Las Rozas*

**State Or Province** [ en ] *Madrid*

**Postal Code** [ en ] *28290*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *C/ Sierra de Cazorla, 1, Entreplanta, Oficina H, Edificio Cimaga*

**Locality** [ es ] *Las Matas - Las Rozas*

**State Or Province** [ es ] *Madrid*

**Postal Code** [ es ] *28290*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *https://www.dehonline.es/*

**URI** [ en ] *mailto:atencionalcliente@dehonline.es*

**TSP Information URI**

**URI** [ en ] *https://www.dehonline.es/*





**Subject OU:** *DEH TSP*

**Subject O:** *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

**Subject L:** *MADRID*

**Subject C:** *ES*

**Valid from:** *Tue Sep 21 18:47:29 CEST 2021*

**Valid to:** *Fri Sep 21 18:47:29 CEST 2029*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100903CABD13EC2F46364EDF1E9CD7E4B3CC2CD0FC4933E4615A6408D0729D3E9DDA4F7  
6C2D36FC1FCAFD4A4E2A127818232CF79F34F863472B632DCEA55BAAE8B03247D58E3BB8FDE97EBF5864B1240A2D4B261F2A2162A803B8E8DE27BD45EEC798104  
955886F317599A1B3AC59401DB4EC5CDA7FD4FE05DFE08C7C8E54797E2E204D7A2DB4C7E55E2E409BAAE7788A206CD47A21C8CDE8F669EA5B47B104C873FE4D61  
CE5A2BF4CC8E15D64B1490B80B7B6CC7541D377780111743EAD889D34CF4D532E30035D81570A2456BC8E50DC1681460EF1F7DE25D6D5C546545BE1C8F8E0DF37C.D1:  
1398BF7A51EE8565DE69AC266B4FE6270A0DC4F71CA8A1BF5F2B92870203010001

**Authority Info Access**  
*http://ocsp1.uanataca.com/public/pki/ocsp/*  
*http://ocsp2.uanataca.com/public/pki/ocsp/*

**Subject Key Identifier**  
*80:C0:E2:57:C7:6B:A2:91:B4:E6:FC:09:36:FE:7A:0F:82:B2:39:1D*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

**Issuer Alternative Name**  
*info@uanataca.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.2.5*  
*CPS pointer: https://www.uanataca.com/public/cps/*  
*CPS text: [Certificado de sello de tiempo electrónico.]*  
  
*Policy OID: 0.4.0.2042.1.2*

**CRL Distribution Points**  
*http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl*  
*http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl*

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Subject Alternative Name**  
*atencionalcliente@dehonline.es*

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*89:BF:44:87:9E:D7:B5:11:8A:90:00:E7:10:98:2E:53:6A:BA:AA:BD:E4:F9:34:AA:DC:67:68:84:C  
2:4E:CD:E0*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B86198306*

**Subject CN:** *DEH QUALIFIED TSU01*

**Subject OU:** *DEH TSP*

**Subject O:** *DEH NOTIFICACIÓN ELECTRÓNICA HABILITADA, S.L.*

**Subject L:** *MADRID*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *gMDiV8dropG05vwJNv56D4KyOR0=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-02-28T00:00:00Z*

**59 - TSP: TECALIS SOTWARE S.L.****TSP Name**

**Name** [ en ] *TECALIS SOTWARE S.L.*

**Name** [ es ] *TECALIS SOTWARE S.L.*

**TSP Trade Name**

**Name** [ en ] *TECALIS*

**Name** [ en ] *VATES-B70186184*

**PostalAddress**

**Street Address** [ en ] *Rúa Oliveira 96 B - Parque empresarial Novo Milladoiro*

**Locality** [ en ] *Milladoiro (Ames)*

**State Or Province** [ en ] *A CORUÑA*

**Postal Code** [ en ] *15895*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Rúa Oliveira 96 B - Parque empresarial Novo Milladoiro*

**Locality** [ es ] *Milladoiro (Ames)*

**State Or Province** [ es ] *A CORUÑA*

**Postal Code** [ es ] *15895*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *https://www.tecalis.com/es*

**URI** [ en ] *mailto:hello@tecalis.com*

**TSP Information URI**

**URI** [ es ] *https://www.tecalis.com/es*

**URI** [ en ] *https://www.tecalis.com*



**Subject OU:** *TECALIS TSP*

**Subject O:** *TECALIS SOFTWARE S.L.*

**Subject L:** *A CORUÑA*

**Subject C:** *ES*

**Valid from:** *Fri May 06 16:26:36 CEST 2022*

**Valid to:** *Mon May 06 16:26:36 CEST 2030*

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D62D345E99F77A80E223E1120BD68695B2D5639650D1B0291A3C3CD4E49FD769CE  
B97DAD2DE70CDE86829C9660B1B887C7CD938DBD1C2F29867DC9A99FC967A5FCD70DBE26709077C1DD984DDDECS47EC2A189C87797CF8FB38ACB68880F60B20  
FF590F67E0DB67488405BEF24A862B991296FF3A191D7B09D7A03ECS3AAS2F9AA0457BE3CA42731A1D63974D3FC2A134FEEDC67519268D4978E81BD757627825C7B  
F745BBCFF68D7BE448E26E3DF09BC7CAB0ECCFD1037B23C4B72AA81070828A4C8FE2B3BA71DB4FA595620F00B16302EFFF72F7DB513194445A23E5575D30CE1433  
C3357C060585F17EF83F3577C12BD80B9D53455EA12E87B8E4D5310203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*3A:B4:DA:09:58:EA:D4:9B:5E:01:48:9C:29:D9:A1:72:41:C5:0B:30*

**Basic Constraints**  
*IsCA: false*

**Authority Key Identifier**  
*81:CF:90:59:34:BB:6A:B7:2D:19:C5:28:F2:8B:5B:CF:CA:FC:15:68*

**Issuer Alternative Name**  
*info@uanataca.com*

**Certificate Policies**  
*Policy OID: 1.3.6.1.4.1.47286.2.5*  
*CPS pointer: <https://www.uanataca.com/public/cps/>*  
*CPS text: [Certificado de sello de tiempo electrónico.]*  
  
*Policy OID: 0.4.0.2042.1.2*

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/2021CA1sub.crl>  
<http://crl2.uanataca.com/public/pki/crl/2021CA1sub.crl>

**Extended Key Usage**  
*id\_kp\_timeStamping*

**Subject Alternative Name**  
*info@tecalis.com*

**Key Usage:**  
*digitalSignature*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*1D:5F:95:13:A7:E4:75:F4:07:E1:46:81:37:B1:58:38:D9:8E:10:28:83:20:E6:58:03:1F:34:A0:4C:A7:  
0D:B7*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-B70186184*

**Subject CN:** *TECALIS QUALIFIED TSU01*

**Subject OU:** *TECALIS TSP*

**Subject O:** *TECALIS SOFTWARE S.L.*

**Subject L:** *A CORUÑA*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *OrTaCVjq1JteAUicKdmhckHFCzA=*

**Service Status** *<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-03-28T00:00:00Z*

**60 - TSP: INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.****TSP Name**

**Name** [ en ] *INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.*

**Name** [ es ] *INSTITUTO PARA LA DINAMIZACION ECONOMICA, S.A.U.*

**TSP Trade Name**

**Name** [ en ] *INDIZE*

**Name** [ en ] *VATES-A18962399*

**Name** [ en ] *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

**PostalAddress**

**Street Address** [ en ] *Camino de la Torrecilla N.º 30, Edificio Educa Edtech, Oficina 11*

**Locality** [ en ] *Maracena*

**State Or Province** [ en ] *GRANADA*

**Postal Code** [ en ] *18200*

**Country Name** [ en ] *ES*

**PostalAddress**

**Street Address** [ es ] *Camino de la Torrecilla N.º 30, Edificio Educa Edtech, Oficina 11*

**Locality** [ es ] *Maracena*

**State Or Province** [ es ] *GRANADA*

**Postal Code** [ es ] *18200*

**Country Name** [ es ] *ES*

**ElectronicAddress**

**URI** [ en ] *mailto:empresa@indize.es*

**URI** [ en ] *https://indize.es/*

**TSP Information URI**

**URI** [ en ] *https://indize.es/*





**Subject CN:** *INDIZE CA Subordinada 01*

**Subject OU:** *TSP - INDIZE*

**Subject O:** *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

**Subject L:** *Granada*

**Subject C:** *ES*

**Valid from:** *Wed Nov 24 13:00:15 CET 2021*

**Valid to:** *Fri Nov 24 13:00:15 CET 2034*

**Public Key:**  
30820222300D06092A864886F70D01010105000382020F003082020A0282020100AD7F79A64047603FDE2A625014B32761D8A0DE6055846A473DA3D515745F736FE87C3  
D0679A3D5D387ABEDCE81B59A1F3742086893C5B8C8BBA4C4B64D70529CA9E07A3C51CCE2E2F505A06B21E3C8345966D3699744D5B0AC9013FA9912E262AE8C30178  
8E43D70B5ED5A6FA24E4752E92DBB9A148DD7E127EDA98A3C6B7ED3776C1333154252F5D13E566E720473FBBE0ED5FC770C8D8A67A67E83319822C53AA2D5  
AD3BAEADA4B67504CA488AFDB7C785FFE1917760FE8AEB21E5DD2172182CE53D9F99874E66141BAF21C052F89365B93E91991E1BA8676975A0C8BFA768B8949D390  
9B1E1F3437DA6EE086C242608C567AC36036D1D05E2A080BC977DCAD016D96A C1B40C03DB589524F3CFC1453D98F9A4B949D3B0916F8EC797C459ABDD4CA2D4B15  
57093AB3253E1AB08CDB1ABBC8CD9FFAD885EBCACD40C92968077A281A1E9EE0EFA5310D68BDEFE6DEE05C3FDDAB8E983D58F3C24FC0D3B368DA212FE27C  
6C1678E1E4E9F34B24E15B50C60F0108C3CDF362AD9A07CA58B1E85EFD20671A0E612B4D50C8D5165173703A85F44C3B04D869245A0346A0499487D5B2A32421277  
92427C4BE78C1470DC72BAE2735B85793759DF29924F8A370747870C30E1D0D6E01A1097441A720DAB95C16A2DABB17E50B4091C13B904C2DD0F30B8EEF0D4B064  
9C5E64B7BB7AB1E2AE8A7FEC8E7789DD421A74FB6488B0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
*E6:33:F2:3A:87:94:F5:B0:36:7C:2E:DE:14:A9:8C:F2:D9:11:7A:F5*

**Basic Constraints**  
*IsCA: true - Path length: 0*

**Authority Key Identifier**  
*55:2C:F1:BC:A1:5E:B9:EE:A0:2F:88:57:10:5B:FC:96:F7:91:9A:2C*

**Issuer Alternative Name**  
*info@uanataca.com*

**Certificate Policies**  
*Policy OID: 2.5.29.32.0*  
*CPS pointer: <https://indize.es/prestador-cualificado-servicios-de-confianza/politicas-practicas>*  
*CPS text: [Certificado de la Autoridad de Certificación Subordinada de INDIZE - <https://indize.es/>]*

**CRL Distribution Points**  
[http://cr1.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://cr1.uanataca.com/public/pki/crl/arl_uanataca.crl)  
[http://cr2.uanataca.com/public/pki/crl/arl\\_uanataca.crl](http://cr2.uanataca.com/public/pki/crl/arl_uanataca.crl)

**Subject Alternative Name**  
*EMPRESA@INDIZE.ES*

**Key Usage:**  
*keyCertSign - cRLSign*

**Thumbprint algorithm:**  
*SHA-256*

**Thumbprint:**  
*41:6D:A0:04:80:EB:C8:14:82:E3:DC:20:3C:BD:D4:3D:69:5F:F1:22:12:7A:DD:98:6F:28:79:B6:29:  
D1:F0:62*

**X509SubjectName**

**Subject 2.5.4.97:** *VATES-A18962399*

**Subject CN:** *INDIZE CA Subordinada 01*

**Subject OU:** *TSP - INDIZE*

**Subject O:** *INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.*

**Subject L:** *Granada*

**Subject C:** *ES*

**X509SKI**

**X509 SK I** *5jPyOoeU9bA2fC7eFKmM8tkRevU=*

**Service Status** *http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted*

**Service status description** *[en] undefined.*

*[es] undefined.*

**Status Starting Time** *2023-03-28T00:00:00Z*

**60.1.1 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures*

**60.1.2 - Extension (critical): additionalServiceInformation**

**AdditionalServiceInformation**

**URI** *[ en ]* *http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals*

**60.1.3 - Extension (critical): Qualifiers [QCQSCDManagedOnBehalf]**

**Qualifier type description** *[en] undefined.*

*[es] undefined.*

**Criteria list assert=atLeastOne**

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.57967.1.1.2*

**Policy Identifier:**

**Identifier** *[ OIDsURN ]* *urn:oid:1.3.6.1.4.1.57967.1.2.2*

**Policy Identifier:**



**Issuer C:** ES

**Subject 2.5.4.97:** VATES-A18962399

**Subject CN:** INDIZE QUALIFIED TSU01

**Subject OU:** TSP - INDIZE

**Subject O:** INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.

**Subject L:** Granada

**Subject C:** ES

**Valid from:** Thu Nov 25 15:26:15 CET 2021

**Valid to:** Tue Nov 27 15:26:15 CET 2029

**Public Key:**  
30820122300D06092A864886F70D01010105000382010F003082010A0282010100D94358146C9EF4044CC0556213AD3A2B77414518940E6DD28D4E1D9812404D8DD6BBF6  
5E289CCFB4B824500D9BDB118CCDCE3999E55CE43E8E2E1C8FE643D8D0043CC76E49B6824624D1E92D039C80819228362FAA42EA20D97FC359296099AF4DCE2F3  
A08A4FD3711ACE7CC1F6A3129621B38FB2F3489B4DD47A8AE2C0F674C88804895EB1B091746B3AF64E581289E89B79EAC8C135140E8AE9A5661A07E30B01D77  
2E63D6DFC073000B5B2FF62598ADB12D9278951BCFB4D3D3AF43FD910DF2B38C60229772D987AD41756CB06A382E20C6C3489D923879A667A6ABAC666CA7B9  
A937588A860DE86C85D3584FFA8B7B24ADBA8546A73F1ED20E157F0203010001

**Authority Info Access**  
<http://ocsp1.uanataca.com/public/pki/ocsp/>  
<http://ocsp2.uanataca.com/public/pki/ocsp/>

**Subject Key Identifier**  
CC:FD:8C:17:F8:29:18:03:9D:E1:83:3F:13:1D:6A:AC:61:7A:2C:2C

**Basic Constraints**  
IsCA: false

**Authority Key Identifier**  
E6:33:F2:3A:87:94:F5:B0:36:7C:2E:DE:14:A9:8C:F2:D9:11:7A:F5

**Issuer Alternative Name**  
EMPRESA@INDIZE.ES

**Certificate Policies**  
Policy OID: 1.3.6.1.4.1.57967.2.2  
CPS text: [Certificado de sello de tiempo electrónico.]  
CPS pointer: <https://indize.es/prestador-cualificado-servicios-de-confianza/politicas-practicas>  
Policy OID: 0.4.0.2042.1.2

**CRL Distribution Points**  
<http://crl1.uanataca.com/public/pki/crl/indize.crl>  
<http://crl2.uanataca.com/public/pki/crl/indize.crl>

**Extended Key Usage**  
id\_kp\_timeStamping

**Subject Alternative Name**  
empresa@indize.es

**Key Usage:**  
digitalSignature

**Thumbprint algorithm:**  
SHA-256

**Thumbprint:**

71:1F:A5:07:FD:AC:69:BB:CC:1B:D1:00:78:C5:1A:AA:F8:C0:8E:FC:58:97:0F:18:8A:06:CF:A8:3D:23:4A:D1

**X509SubjectName****Subject 2.5.4.97:**

VATES-A18962399

**Subject CN:**

INDIZE QUALIFIED TSU01

**Subject OU:**

TSP - INDIZE

**Subject O:**

INSTITUTO PARA LA DINAMIZACION ECONOMICA S.A.

**Subject L:**

Granada

**Subject C:**

ES

**X509SKI****X509 SK I**

zP2MF/gpGAOd4YM/Ex1qrGF6LCw=

**Service Status**

<http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted>

**Service status description**

[en]

undefined.

[es]

undefined.

**Status Starting Time**

2023-03-28T00:00:00Z



**Thumbprint algorithm:**

*SHA-256*

**Thumbprint:**

*18:0C:D5:36:DA:D2:B5:AC:93:32:36:D9:DC:D5:5D:17:AF:CD:99:49:FE:D0:81:89:B8:AE:86:FE:  
7C:2B:C3:A7*