

esFIRMA Qualified Timestamp TSA - QTSU Certificate Profile

Version: 2 (v3)

SerialNumber: Greater than 0 containing 128 bits of output from a CSPRNG

Signature:

algo: 1.2.840.113549.1.1.13 (*sha512WithRSAEncryption(13)*)

params: NULL

Issuer:

2.5.4.6 (*countryName,C*): ES (*type: printableString*)

2.5.4.7 (*localityName,L*): ZARAGOZA (*type: printableString*)

2.5.4.10 (*organizationName*): ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (*type: printableString*)

2.5.4.11 (*organizationalUnitName*): AUTORIDAD DE CERTIFICACION ESFIRMA - AAPP (*type: printableString*)

2.5.4.5 (*serialNumber,SN*): A50878842 (*type: printableString*)

2.5.4.3 (*commonName,CN*): ESFIRMA AC AAPP 2 (*type: printableString*)

Subject:

2.5.4.6 (*countryName,C*): ES (*type: printableString*)

2.5.4.10 (*organizationName*): ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (*type: printableString*)

2.5.4.97 (*organizationIdentifier*): VATES-A50878842 (*type: printableString*)

2.5.4.3 (*commonName,CN*): ESFIRMA TSA - QTSU <ID>(*type: printableString*): ID is a unique TSU Identifier

Validity:

Duration: ~ 5 years

NotBefore: Date on which the certificate validity period begins

NotAfter: Date on which the certificate validity period ends

SubjectPublicKeyInfo:

Algorithm:

algo: 1.2.840.113549.1.1.1 (*RSA*)

params: NULL

PublicKey:

modulus: public key modulus

2.5.29.19 (*Basic constraints*):

Critical

None

2.5.29.35 (*Authority key identifier*)

Identifier: 0xf640efc3a72b4de5bf31e9faeec379791f2a0358 (*b64: 9kDvw6crTeW/Men67sN5eR8qA1g=*)

1.3.6.1.5.5.7.1.1 (*Authority Information Access*):

AccessDescription:

Method: 1.3.6.1.5.5.7.48.2 (*calssuers*)

Location

uri: http://www.esfirma.com/doc-pki/acaapp2.crt (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.1 (*ocsp*)

Location

uri: http://ocsp.esfirma.com/acaapp2/ (*type: IA5String*)

2.5.29.32 (*Certificate policies*)

Policies:

1.3.6.1.4.1.47281.1.5.2 (esFIRMA QTSA Policy)

1.3.6.1.5.5.7.2.1 (CPS)

URI: <https://www.esfirma.com/doc-pki/> (type: IA5String)

0.4.0.194112.1.1 (Qcp-legal)

2.5.29.37 (Extended key usage):

Critical

1.3.6.1.5.5.7.3.8 (timeStamping)

1.3.6.1.5.5.7.1.3 (QcStatements):

1.3.6.1.5.5.7.11.2 (id-qcs-pkixQCSyntax-v2)

keyIdentifier: 0.4.0.194121.1.2 (Id-etsi-qcs-SemanticsId-Legal)

0.4.0.1862.1.1 (QcCompliance)

0.4.0.1862.1.3 (QcRetentionPeriod)

Years: 15 (Oxf)

0.4.0.1862.1.6 (QcType)

0.4.0.1862.1.6.2 (eseal)

2.5.29.31 (Revocation List distribution points):

DistributionPoint

Name

FullName

[0] uri: <http://crls1.esfirma.com/acaapp/acaapp2.crl> (type: IA5String)

DistributionPoint

Name

FullName

[0] uri: <http://crls2.esfirma.com/acaapp/acaapp2.crl> (type: IA5String)

2.5.29.14 (Subject key identifier): 160 bit derived from the public key

2.5.29.16 (Private Key usage Period):

Duration: ~ 2 years

NotBefore: Date on which the certificate validity period begins

NotAfter: Date on which the certificate validity period ends

2.5.29.15 (Key usage):

Critical

1 (ContentCommitment)