esFIRMA Qualified Timestamp Certificate Profile

(esfirma-tsa2.pem)

Version: 2 *(v3)*
SerialNumber: Greater than 0 containing 64 bits of output from a CSPRNG
Signature:
  algo: **1.2.840.113549.1.1.11** *(sha256WithRSAEncryption)*
  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)*
  2.5.4.7 *(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 *(type: printableString)*
  2.5.4.5 *(serialNumber,SN)*: A50878842 *(type: printableString)*
  2.5.4.97 *(organizationIdentifier)*: VATES-A50878842 *(type: printableString)*
  2.5.4.3 *(commonName,CN)*: ESFIRMA TSA 2 *(type: printableString)*
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
    publicExponent: 0x010001
  Key length: 4096 *(0x1000)*
Extensions:
  2.5.29.32 *(Certificate policies)*
    Policies:
      0.4.0.194112.1.1 *(Qcp-legal)*
      1.3.6.1.4.1.47281.1.5.2 *(esFIRMA DPC TSA - MEDIO)*:
        1.3.6.1.5.5.7.2.1 *(CPS)*
          URI: https://www.esfirma.com/doc-pki/ *(type: IA5String)*
        1.3.6.1.5.5.7.2.2 *(User Notice)*
          ExplicitText: Servidor de sellado de tiempo de esFIRMA. Consulte https://www.esfirma.com/doc-pki/ *(type: utf8String)*

2.5.29.14 *(Subject key identifier)*: 160 bit derived from the public key
2.5.29.35 *(Authority key identifier)*
Identifier: 0xf640efc3a72b4de5bf31e9faeec379791f2a0358
2.5.29.19 *(Basic constraints)*
None
2.5.29.15 *(Key usage)*:
Critical
1 *(ContentCommitment)*
2.5.29.37 *(Extended key usage)*:
Critical
1.3.6.1.5.5.7.3.8 *(timeStamping)*
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)*
1.3.6.1.5.5.7.1.1 *(Authority Information Access)*:
AccessDescription:
Method: **1.3.6.1.5.5.7.48.1** *(ocsp)*
Location
uri: http://ocsp1.esfirma.com/acaapp2/ *(type: IA5String)*
AccessDescription:
Method: **1.3.6.1.5.5.7.48.1** *(ocsp)*
Location
uri: http://ocsp2.esfirma.com/acaapp2/ *(type: IA5String)*
AccessDescription:
Method: **1.3.6.1.5.5.7.48.2** *(caIssuers)*
Location
uri: https://www.esfirma.com/doc-pki/acaapp2.crt *(type: IA5String)*
1.3.6.1.5.5.7.1.3 *(QcStatements)*:
0.4.0.1862.1.1 *(QcCompliance)*
0.4.0.1862.1.6 *(QcType)*
0.4.0.1862.1.6.2 *(eseal)*
0.4.0.1862.1.3 *(QcRetentionPeriod)*
Years: 15 *(0xf)*
0.4.0.1862.1.5 *(QcPDS)*:
Location:
lang: en *(type: PrintableString)*
url: https://www.esfirma.com/doc-pki/PDS2/TS2-EN/ *(type: IA5String)*
Location:
lang: es *(type: PrintableString)*

url: https://www.esfirma.com/doc-pki/PDS2/TS2-ES/ *(type: IA5String)*

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)*