

esFIRMA AAPP 2 SUB CA Certificate Profile

Version: 2 (v3)

SerialNumber: Greater than 0 containing 64 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 (*type: printableString*)

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

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

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

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

Validity:

Duration: 13 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

1.3.6.1.5.5.7.1.1 (*Authority Information Access*):

AccessDescription:

Method: 1.3.6.1.5.5.7.48.2 (*caIssuers*)

Location

uri: https://www.esfirma.com/doc-pki/esfirma-acraiz2.crt (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.1 (*ocsp*)

Location

uri: http://ocsp.esfirma.com/acraiz2/ (*type: IA5String*)

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

2.5.29.19 (*Basic constraints*):

Critical

CA: true

pathLenConstraint: 0 (*0x0*)

2.5.29.35 (*Authority key identifier*)

Identifier: 0x8380e5d627bdef30b2ae1d9dcaa8f23214c71332 (*b64: g4Dl1ie97zCyrh2dyqjyMhTHEzI=*)

2.5.29.32 (*Certificate policies*)

Policies

2.5.29.32.0 (*Any Policy*):

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: Autoridad de certificación AAPP 2 de esFirma. Ver <https://www.esfirma.com/doc-pki/> (*type: utf8String*)

2.5.29.31 (*Revocation List distribution points*):

DistributionPoint

Name

FullName

[0] uri: <https://crls1.esfirma.com/acraiz/acraiz2.crl> (*type: IA5String*)

DistributionPoint

Name

FullName

[0] uri: <https://crls2.esfirma.com/acraiz/acraiz2.crl> (*type: IA5String*)

2.5.29.15 (*Key usage*):

Critical

5 (*KeyCertSign*)

6 (*CRLSign*)