

ESFIRMA PROFILE Extended Validation Site Certificate

Version: 2 (v3)

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

Signature:

algo: 1.2.840.113549.1.1.11 (*sha256WithRSAEncryption*)

params: NULL

Issuer:

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

2.5.4.7 (*localityName*): 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*): A50878842 (*type: printableString*)

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

Subject:

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

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

2.5.4.10 (*organizationName*): PRUEBA-TEST (*type: printableString*)

2.5.4.11 (*organizationalUnitName*): SEDE ELECTRONICA (*type: printableString*)

2.5.4.11 (*organizationalUnitName*): PUNTO DE ACCESO GENERAL DE PRUEBAS (*type: printableString*)

2.5.4.5 (*serialNumber*): TEST (*type: printableString*)

2.5.4.15 (*businessCategory*): Government Entity (*type: printableString*)

1.3.6.1.4.1.311.60.2.1.3 (*jurisdictionOfIncorporationCountryName*): ES (*type: printableString*)

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

Validity:

Duration: 1 year 1 month 2 days

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: ...

publicExponent: 01:00:01

Key length: 2048 (*0x800*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

2.16.724.1.3.5.5.2 (*MPR SEDE ELECTRONICA (Nivel Medio/Sustancial)*)

0.4.0.194112.1.4 (*QCP-w: certificate policy for European Union (EU) qualified website authentication certificates*)

1.3.6.1.4.1.47281.1.4.2 (*esFIRMA Sede electrónica AAPP - MEDIO en Software - EV*):

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: Certificado cualificado de sede electrónica de PRUEBA-TEST nivel medio. Consulte <https://www.esfirma.com/doc-pki/> (type: utf8String)

2.23.140.1.1 (Extended Validation (EV) guidelines certificate policy)

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

2.5.29.35 (Authority key identifier)

Identifier: f6:40:ef:c3:a7:2b:4d:e5:bf:31:e9:fa:ee:c3:79:79:

1f:2a:03:58

2.5.29.19 (Basic constraints)

None

2.5.29.15 (Key usage):

Critical

0 (DigitalSignature)

2 (KeyEncipherment)

2.5.29.37 (Extended key usage)

1.3.6.1.5.5.7.3.1 (serverAuth)

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

2.5.29.17 (Subject alternative name)

DNSName: good2.testing.esfirma.com (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)

0.4.0.1862.1.6.3 (web)

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/SE2-MEDIO-SOFT-EN/> *(type: IA5String)***Location:****lang:** es *(type: PrintableString)***url:** <https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-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)***2.23.140.3.1** *(CABForum OrganizationIdentifier):***SchemelIdentifier:** VAT *(type: printableString)***Country:** ES *(type: printableString)***Reference:** TEST *(type: utf8String)*