

ESFIRMA PROFILE Public organization seal HSM certificate

A) Structure when no specific name provided

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,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*): PRUEBA-TEST (*type: printableString*)

2.5.4.11 (*organizationalUnitName*): SELLO ELECTRONICO (*type: printableString*)

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

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

2.5.4.3 (*commonName,CN*): SELLO ELECTRONICO DE PRUEBA-TEST (*type: printableString*)

Validity:

Duration: 2 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: ...

publicExponent: 01:00:01

Key length: 2048 (*0x800*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

2.16.724.1.3.5.6.2 (*MPR SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio, Sustancial)*)

0.4.0.194112.1.1 (*Qcp-legal*)

1.3.6.1.4.1.47281.1.2.4 (*esFIRMA Sello-e AAPP – MEDIO en HSM -DOCUMENTOS*):

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 sello electrónico de PRUEBA-TEST nivel medio. 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: 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*)

1 (*ContentCommitment*)

2 (*KeyEncipherment*)

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*):

rfc822Name: info_sello@pruebas.esfirma.com (*type: IA5String*) (*Optional*)

directoryName:

2.16.724.1.3.5.6.2.1 (*MPR SEAA Medio, Tipo de certificado*): SELLO ELECTRONICO DE NIVEL MEDIO (*type: utf8String*)

2.16.724.1.3.5.6.2.2 (*MPR SEAA Medio, Nombre de la entidad suscriptora*): PRUEBA-TEST (*type: utf8String*)

2.16.724.1.3.5.6.2.3 (*MPR SEAA Medio, NIF entidad suscriptora*): TEST (*type: utf8String*)

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/SO2-MEDIO-HSM-EN/ (*type: IA5String*)

Location:

lang: es (*type: PrintableString*)

url: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-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*)

B) Structure when specific name provided

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,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*): PRUEBA-TEST (*type: printableString*)

2.5.4.11 (*organizationalUnitName*): SELLO ELECTRONICO (*type: printableString*)

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

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

2.5.4.3 (*commonName,CN*): PLATAFORMA GESTIONA PARA AYUNTAMIENTO DE PRUEBAS (*type: printableString*)

Validity:

Duration: 2 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: ...

publicExponent: 01:00:01

Key length: 2048 (*0x800*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

2.16.724.1.3.5.6.2 (MPR SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio,Sustancial))

0.4.0.194112.1.1 (Qcp-legal)

1.3.6.1.4.1.47281.1.2.4 (esFIRMA Sello-e AAPP – MEDIO en HSM -DOCUMENTOS):

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 sello electrónico de PRUEBA-TEST nivel medio. 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: 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)

1 (ContentCommitment)

2 (KeyEncipherment)

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):

rfc822Name: info_sello@pruebas.esfirma.com (type: IA5String) (Optional)

directoryName:

2.16.724.1.3.5.6.2.1 (MPR SEAA Medio, Tipo de certificado): SELLO ELECTRONICO DE NIVEL MEDIO (type: utf8String)

2.16.724.1.3.5.6.2.2 (MPR SEAA Medio, Nombre de la entidad suscriptora): PRUEBA-TEST (type: utf8String)

2.16.724.1.3.5.6.2.3 (MPR SEAA Medio, NIF entidad suscriptora): TEST (type: *utf8String*)

2.16.724.1.3.5.6.2.5 (MPR SEAA Medio, Denominación del sistema): PLATAFORMA GESTIONA PARA AYUNTAMIENTO DE PRUEBAS (type: *utf8String*) (Optional)

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 (Oxf)

0.4.0.1862.1.5 (QcPDS):

Location:

lang: en (type: *PrintableString*)

url: <https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-EN/> (type: *IA5String*)

Location:

lang: es (type: *PrintableString*)

url: <https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-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)