

esFIRMA Electronic Seal Remote Signing Certificate Profile

Country: Any European Union country (*esfirma-sl-hsm-eu.pem*)

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:

2.5.4.3 (*commonName,CN*): ESFIRMA DEV AAPP (*type: utf8String*)

Subject:

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

2.5.4.10 (*organizationName*): TEST (*type: utf8String*)

2.5.4.5 (*serialNumber,SN*): VATEU-000000000 (*type: printableString*)

2.5.4.3 (*commonName,CN*): TEST (*type: utf8String*)

2.5.4.97 (*organizationIdentifier*): VATEU-000000000 (*type: utf8String*)

Validity:

Duration: 1 year 11 months 29 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: public key modulus

publicExponent: 0x010001

Key length: 2048 (*0x800*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

0.4.0.194112.1.1 (*Qcp-legal*)

1.3.6.1.4.1.47281.1.8.4 (*esFIRMA DPC*)

1.3.6.1.5.5.7.2.1 (*CPS*)

URI: <https://www-esfirma.g3stiona.com/doc-pki/> (*type: IA5String*)

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

2.5.29.35 (*Authority key identifier*)

Identifier: 0xf47684706c94969af9d8267494ec2ed9345adb35

2.5.29.19 (*Basic constraints*)

None

2.5.29.15 (*Key usage*):

Critical

1 (*ContentCommitment*)

2.5.29.31 (*Revocation List distribution points*):

DistributionPoint

Name

FullName

[0] uri: <http://crls1-esfirma.g3stiona.com/acaapp/acaapp.crl> (*type: IA5String*)

DistributionPoint

Name

FullName

[0] uri: <http://crls2-esfirma.g3stiona.com/acaapp/acaapp.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.g3stiona.com/acaapp/ (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.1 (*ocsp*)

Location

uri: http://ocsp2-esfirma.g3stiona.com/acaapp/ (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.2 (*caIssuers*)

Location

uri: http://www-esfirma.g3stiona.com/doc-pki/acaapp.crt (*type: IA5String*)

2.5.29.17 (*Subject alternative name*)

rfc822Name: 000000000@test.esfirma.com (*type: IA5String*) (*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 (*0xf*)

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*)

Country: Spain (*Legacy*) (*esfirma-sl-hsm-es-legacy.pem*)

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:

2.5.4.3 (*commonName,CN*): ESFIRMA DEV AAPP (*type: utf8String*)

Subject:

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

2.5.4.10 (*organizationName*): PRUEBA-TEST (*type: utf8String*)

2.5.4.5 (*serialNumber,SN*): VATES-A9999999G (*type: printableString*)

2.5.4.3 (*commonName,CN*): SELLO ELECTRONICO DE PRUEBA-TEST (*type: utf8String*)

2.5.4.97 (*organizationIdentifier*): VATES-A9999999G (*type: utf8String*)

Validity:

Duration: 1 year 11 months 29 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: public key modulus

publicExponent: 0x010001

Key length: 2048 (*0x800*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

0.4.0.194112.1.1 (*Qcp-legal*)

1.3.6.1.4.1.47281.1.8.4 (*esFIRMA DPC*):

1.3.6.1.5.5.7.2.1 (*CPS*)

URI: <https://www-esfirma.g3stiona.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. Consulte <https://www-esfirma.g3stiona.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: 0xf47684706c94969af9d8267494ec2ed9345adb35

2.5.29.19 (*Basic constraints*)

None

2.5.29.15 (*Key usage*):

Critical

1 (*ContentCommitment*)

2.5.29.31 (*Revocation List distribution points*):

DistributionPoint

Name

FullName

[0] uri: http://crls1-esfirma.g3stiona.com/acaapp/acaapp.crl (*type: IA5String*)

DistributionPoint

Name

FullName

[0] uri: http://crls2-esfirma.g3stiona.com/acaapp/acaapp.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.g3stiona.com/acaapp/ (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.1 (*ocsp*)

Location

uri: http://ocsp2-esfirma.g3stiona.com/acaapp/ (*type: IA5String*)

AccessDescription:

Method: 1.3.6.1.5.5.7.48.2 (*calssuers*)

Location

uri: http://www-esfirma.g3stiona.com/doc-pki/acaapp.crt (*type: IA5String*)

2.5.29.17 (*Subject alternative name*)

rfc822Name: a9999999g@test.esfirma.com (*type: IA5String*) (*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 (*0xf*)

0.4.0.1862.1.5 (*QcPDS*):

Location:

lang: en (*type: PrintableString*)

url: https://www-esfirma.g3stiona.com/doc-pki/PDS/SL2-DOCUMENTOS-HSM-EN/ (*type: IA5String*)

Location:

lang: es (*type: PrintableString*)

url: https://www-esfirma.g3stiona.com/doc-pki/PDS/SL2-DOCUMENTOS-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*)