

esFIRMA Public Employee With Pseudonym Remote Signing Certificate Profile

Country: Spain

A) Pseudonym (*esfirma-es-hsm-sign-a-es.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:

2.5.4.6 (*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*): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (*type: printableString*)

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

2.5.4.65 (*pseudonym*): 94784686 (*type: printableString*)

2.5.4.3 (*commonName,CN*): SEUDONIMO - 94784686 - PRUEBA-TEST (*FIRMA*) (*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:

Supported algorithms:

1.2.840.113549.1.1.1 (*RSA 2048 bits*)

1.2.840.10045.3.1.7 (*EC NIST P256*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

2.16.724.1.3.5.4.2 (*MPR CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Medio,Sustancial)*)

0.4.0.194112.1.0 (*Qcp-natural*)

1.3.6.1.4.1.47281.1.3.4 (*esFIRMA Public Employee With Pseudonym Remote Signing HSM 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: Certificado cualificado de firma electrónica de empleado público con seudónimo 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: 0xf640efc3a72b4de5bf31e9faeec379791f2a0358 (*b64: 9kDvw6crTeW/Men67sN5eR8qA1g=*)

2.5.29.19 (*Basic constraints*)

None

2.5.29.15 (*Key usage*):

Critical

0 (*DigitalSignature*)

1 (*ContentCommitment*)

2 (*KeyEncipherment*) when RSA key

4 (KeyAgreement) when EC P256 key

2.5.29.37 (Extended key usage):

1.3.6.1.5.5.7.3.2 (ClientAuth)

1.3.6.1.5.5.7.3.4 (emailProtection)

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: seudonimo@test.esfirma.com (type: IA5String) (Optional)

directoryName:

2.16.724.1.3.5.4.2.1 (MPR CEEPS Medio, Tipo de certificado): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (type: utf8String)

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

2.16.724.1.3.5.4.2.3 (MPR CEEPS Medio, NIF entidad suscriptora): A9999999G (type: utf8String)

2.16.724.1.3.5.4.2.9 (MPR CEEPS Medio, Correo electrónico del firmante): seudonimo@test.esfirma.com (type: IA5String) (Optional)

2.16.724.1.3.5.4.2.12 (MPR CEEPS Medio, Seudónimo): 94784686 (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)

0.4.0.1862.1.6.1 (esign)

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/ES2-MEDIO-HSM-EN/ (type: IA5String)

Location:

lang: es (type: PrintableString)

url: https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/ (type: IA5String)

1.3.6.1.5.5.7.11.2 (id-qcs-pkixQCSyntax-v2)

keyIdentifier: 0.4.0.194121.1.1 (Id-etsi-qcs-SemanticsId-Natural)

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) NIP (*esfirma-es-hsm-sign-b-es.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:

2.5.4.6 (*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*): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (*type: printableString*)

2.5.4.12 (*title,T*): JEFE DE SECCION (*type: printableString*)

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

2.5.4.65 (*pseudonym*): NIP 46789541N (*type: printableString*)

2.5.4.3 (*commonName,CN*): JEFE DE SECCION - NIP 46789541N - PRUEBA-TEST (*FIRMA*) (*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:

Supported algorithms:

1.2.840.113549.1.1.1 (*RSA 2048 bits*)

1.2.840.10045.3.1.7 (*EC NIST P256*)

Extensions:

2.5.29.32 (*Certificate policies*)

Policies:

2.16.724.1.3.5.4.2 (*MPR CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (Nivel Medio,Sustancial)*)

0.4.0.194112.1.0 (*Qcp-natural*)

1.3.6.1.4.1.47281.1.3.4 (*esFIRMA Public Employee With Pseudonym Remote Signing HSM 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: Certificado cualificado de firma electrónica de empleado público con seudónimo 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: 0xf640efc3a72b4de5bf31e9faeec379791f2a0358 (*b64: 9kDvw6crTeW/Men67sN5eR8qA1g=*)

2.5.29.19 (*Basic constraints*)

None

2.5.29.15 (*Key usage*):

Critical

0 (*DigitalSignature*)

1 (*ContentCommitment*)

2 (*KeyEncipherment*) when RSA key

4 (*KeyAgreement*) when EC P256 key

2.5.29.37 (*Extended key usage*):

1.3.6.1.5.5.7.3.2 (*ClientAuth*)

1.3.6.1.5.5.7.3.4 (*emailProtection*)

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 (*calssuers*)

Location

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

2.5.29.17 (*Subject alternative name*):

rfc822Name: seudonimo@test.esfirma.com (*type: IA5String*) (*Optional*)

directoryName:

2.16.724.1.3.5.4.2.1 (*MPR CEEPS Medio, Tipo de certificado*): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO (*type: utf8String*)

2.16.724.1.3.5.4.2.2 (*MPR CEEPS Medio, Nombre de la entidad suscriptor*): PRUEBA-TEST (*type: utf8String*)

2.16.724.1.3.5.4.2.3 (*MPR CEEPS Medio, NIF entidad suscriptor*): A9999999G (*type: utf8String*)

2.16.724.1.3.5.4.2.5 (*MPR CEEPS Medio, NRP o NIP del empleado*): 46789541N (*type: utf8String*)

2.16.724.1.3.5.4.2.9 (*MPR CEEPS Medio, Correo electrónico del firmante*): seudonimo@test.esfirma.com (*type: IA5String*) (*Optional*)

2.16.724.1.3.5.4.2.11 (*MPR CEEPS Medio, Puesto o cargo del firmante*): JEFE DE SECCION (*type: utf8String*)

2.16.724.1.3.5.4.2.12 (*MPR CEEPS Medio, Seudónimo*): NIP 46789541N (*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*)

0.4.0.1862.1.6.1 (*esign*)

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/ES2-MEDIO-HSM-EN/> (*type: IA5String*)

Location:

lang: es (*type: PrintableString*)

url: <https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/> (*type: IA5String*)

1.3.6.1.5.5.7.11.2 (*id-qcs-pkixQCSyntax-v2*)

keyIdentifier: **0.4.0.194121.1.1** (*Id-etsi-qcs-SemanticsId-Natural*)

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*)