

## esFIRMA Natural Person With Pseudonym Linked To Entity Remote Signing Certificate Profile

**Country:** Any European Union country (*esfirma-ps-hsm-sign-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:**

**2.5.4.6** (*countryName,C*): EU ISO 3166-1 alpha-2 code (*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*): EU ISO 3166-1 alpha-2 code (*type: printableString*)

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

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

**2.5.4.65** (*pseudonym*): P53UD0 (*type: printableString*)

**2.5.4.3** (*commonName,CN*): P53UD0 - 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:**

**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:**

**0.4.0.194112.1.0** (*Qcp-natural*)

**1.3.6.1.4.1.47281.1.7.4** (*esFIRMA Natural Person With Pseudonym Linked To Entity Remote Signing HSM Policy*)

**1.3.6.1.5.5.7.2.1** (*CPS*)

**URI:** https://www.esfirma.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:** 0xf640efc3a72b4de5bf31e9faeec379791f2a0358 (*b64: 9kDvw6crTeW/Men67sN5eR8qA1g=*)

**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.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)

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 (Oxf)

**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)

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

**keyIdentifier:** 0.4.0.194121.1.4 (Id-etsi-qcs-SemanticsId-Eidas-Legal)

**Country:** Spain (*Legacy*) (*esfirma-ps-hsm-sign-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:**

**2.5.4.6** (*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 PERSONA FÍSICA CON SEUDÓNIMO VINCULADA A ENTIDAD (*type: utf8String*)

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

**2.5.4.65** (*pseudonym*): P53UD0 (*type: printableString*)

**2.5.4.3** (*commonName,CN*): SEUDONIMO - P53UD0 - 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:**

**0.4.0.194112.1.0** (*Qcp-natural*)

**1.3.6.1.4.1.47281.1.7.4** (*esFIRMA Natural Person With Pseudonym Linked To Entity 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 persona física con seudónimo vinculada a entidad 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

1 (ContentCommitment)

**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:**

**1.3.6.1.4.1.47281.0.7.1** (esFIRMA CERTIFICADO PERSONA FÍSICA CON SEUDÓNIMO VINCULADA A ENTIDAD): CERTIFICADO PERSONA FÍSICA CON SEUDÓNIMO VINCULADA A ENTIDAD (type: utf8String)

**1.3.6.1.4.1.47281.0.7.2** (esFIRMA Entity Name): PRUEBA-TEST (type: utf8String)

**1.3.6.1.4.1.47281.0.7.3** (esFIRMA Entity NIF): A9999999G (type: utf8String)

**1.3.6.1.4.1.47281.0.7.9** (esFIRMA Subject Email): seudonimo@test.esfirma.com (type: IA5String)

**1.3.6.1.4.1.47281.0.7.12** (esFIRMA Pseudonym): P53UD0 (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/PS2-FIRMA-HSM-EN/ (type: IA5String)

**Location:**

**lang:** es (type: PrintableString)

**url:** https://www.esfirma.com/doc-pki/PDS2/PS2-FIRMA-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*)

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

**keyIdentifier: 0.4.0.194121.1.4** (*id-etsi-qcs-SemanticsId-Eidas-Legal*)