

## esFIRMA Natural Person With Pseudonym Linked To Entity Smartcard Authentication Certificate Profile

**Country:** Any European Union country (*esfirma-ps-sc-auth-eu-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*): 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 SET 68 (*type: printableString*)

**2.5.4.97** (*organizationIdentifier*): VATES-A0000000A (*type: printableString*)

**2.5.4.65** (*pseudonym*): 00000000 (*type: printableString*)

**2.5.4.3** (*commonName,CN*): 00000000 - TEST SET 68 (*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:**

**0.4.0.2042.1.2** (*NCP+*)

**1.3.6.1.4.1.47281.1.7.5** (*esFIRMA Natural Person With Pseudonym Linked To Entity Smartcard Auth QSCD 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

0 (*DigitalSignature*)

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*)

**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)

**Country:** Spain (*Legacy*) (*esfirma-ps-sc-auth-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*): TEST SET 68 (*type: printableString*)

**2.5.4.11** (*organizationalUnitName*): CERTIFICADO PERSONA FÍSICA CON SEUDÓNIMO VINCULADA A ENTIDAD (*type: utf8String*)

**2.5.4.97** (*organizationIdentifier*): VATES-A0000000A (*type: printableString*)

**2.5.4.65** (*pseudonym*): 00000000 (*type: printableString*)

**2.5.4.3** (*commonName,CN*): SEUDONIMO - 00000000 - TEST SET 68 (*AUTENTICACIÓN*) (*type: utf8String*)

**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:**

**0.4.0.2042.1.2** (*NCP+*)

**1.3.6.1.4.1.47281.1.7.5** (*esFIRMA Natural Person With Pseudonym Linked To Entity Smartcard Auth QSCD 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 autenticación electrónica de persona física con seudónimo vinculada a entidad nivel alto. 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*)

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*)

**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*): TEST SET 68 (*type: utf8String*)

**1.3.6.1.4.1.47281.0.7.3** (*esFIRMA Entity NIF*): A0000000A (*type: utf8String*)

**1.3.6.1.4.1.47281.0.7.12** (*esFIRMA Pseudonym*): 00000000 (*type: utf8String*)