

## esFIRMA Public Employee Remote Signing Certificate Profile

**Country:** Spain (*esfirma-ep-hsm-sign-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*): TEST SET 69 (*type: printableString*)

**2.5.4.11** (*organizationalUnitName*): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (*type: printableString*)

**2.5.4.5** (*serialNumber,SN*): IDCES-99949997R (*type: printableString*)

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

**2.5.4.4** (*surname*): ESPECIMENSIETE ESPECIMENSIETE (*type: printableString*)

**2.5.4.42** (*givenName,GN*): NOMSIETE (*type: printableString*)

**2.5.4.3** (*commonName,CN*): NOMSIETE ESPECIMENSIETE ESPECIMENSIETE - 99949997R (*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:**

**2.16.724.1.3.5.7.2** (*MPR CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO (Nivel Medio,Sustancial)*)

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

**1.3.6.1.4.1.47281.1.1.4** (*esFIRMA Public Employee 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 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://crs1.esfirma.com/acaapp/acaapp2.crl (type: IA5String)

DistributionPoint

Name

FullName

[0] uri: http://crs2.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:** nombre@test.esfirma.com (type: IA5String) (Optional)

**directoryName:**

**2.16.724.1.3.5.7.2.1** (MPR CEEP Medio, Tipo de certificado): CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO (type: utf8String)

**2.16.724.1.3.5.7.2.2** (MPR CEEP Medio, Nombre de la entidad suscriptora): TEST SET 69 (type: utf8String)

**2.16.724.1.3.5.7.2.3** (MPR CEEP Medio, NIF entidad suscriptora): A0000000A (type: utf8String)

**2.16.724.1.3.5.7.2.4** (MPR CEEP Medio, DNI, NIE del firmante): 99949997R (type: utf8String)

**2.16.724.1.3.5.7.2.6** (MPR CEEP Medio, Nombre de pila del firmante): NOMSIETE (type: utf8String)

**2.16.724.1.3.5.7.2.7** (MPR CEEP Medio, Apellido 1 del firmante): ESPECIMENSIETE (type: utf8String)

**2.16.724.1.3.5.7.2.8** (MPR CEEP Medio, Apellido 2 del firmante): ESPECIMENSIETE (type: utf8String) (Optional)

**2.16.724.1.3.5.7.2.9** (MPR CEEP Medio, Correo electrónico del firmante): nombre@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*)

**0.4.0.1862.1.6.1** (*esign*)

**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/EP2-MEDIO-HSM-EN/> (*type: IA5String*)

**Location:**

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

**url:** <https://www.esfirma.com/doc-pki/PDS2/EP2-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*)