**esFIRMA Natural Person Linked To Entity Smartcard Authentication Certificate Profile**

**Country**: Any European Union country *(esfirma-pv-sc-auth-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)*
  **2.5.4.4** *(surname)*: DA CONCEIÇÃO ESPAÑOLA *(type: utf8String)*
  **2.5.4.42** *(givenName,GN)*: BIANCA *(type: utf8String)*
  **2.5.4.5** *(serialNumber,SN)*: IDCEU-999999999 *(type: printableString)*
  **2.5.4.3** *(commonName,CN)*: BIANCA DA CONCEIÇÃO ESPAÑOLA - 999999999 *(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**:
      **0.4.0.2042.1.2** *(NCP+)*
      **1.3.6.1.4.1.47281.1.6.5** *(esFIRMA DPC Persona Física con Pertenencia a Entidad - ALTO en Tarjeta AUTENTICACIÓN)*
        **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
    0 *(DigitalSignature)*
    2 *(KeyEncipherment)*
  **2.5.29.37** *(Extended key usage)*:
    Critical
    **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.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**: bianca@test.esfirma.com *(type: IA5String) (Optional)*

**Country**: Spain *(Legacy) (esfirma-pv-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**:
  **2.5.4.3** *(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)*
  **2.5.4.11** *(organizationalUnitName)*: CERTIFICADO DE PERSONA FÍSICA VINCULADA A ENTIDAD *(type: utf8String)*
  **2.5.4.4** *(surname)*: ESPAÑOLA ESPAÑOLA *(type: utf8String)*
  **2.5.4.42** *(givenName,GN)*: CARMEN *(type: utf8String)*
  **2.5.4.5** *(serialNumber,SN)*: IDCES-99999999R *(type: printableString)*
  **2.5.4.3** *(commonName,CN)*: CARMEN ESPAÑOLA ESPAÑOLA - 99999999R *(AUTENTICACIÓN) (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**:
      **0.4.0.2042.1.2** *(NCP+)*
      **1.3.6.1.4.1.47281.1.6.5** *(esFIRMA DPC Persona Física con Pertenencia a Entidad - ALTO en Tarjeta AUTENTICACIÓN)*:
        **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 autenticación electrónica de persona física vinculada a entidad nivel alto. 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
0 *(DigitalSignature)*
2 *(KeyEncipherment)*
**2.5.29.37** *(Extended key usage)*:
Critical
**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.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**: carmen@test.esfirma.com *(type: IA5String) (Optional)*
**directoryName**:
**1.3.6.1.4.1.47281.0.6.1** *(esFIRMA Literal)*: CERTIFICADO DE PERSONA FÍSICA VINCULADA A ENTIDAD *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.2** *(esFIRMA Nombre de la entidad)*: PRUEBA-TEST *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.3** *(esFIRMA NIF de la entidad)*: A9999999G *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.4** *(esFIRMA NIF de la persona)*: 99999999R *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.6** *(esFIRMA Nombre de la persona)*: CARMEN *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.7** *(esFIRMA Primer apellido de la persona)*: ESPAÑOLA *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.8** *(esFIRMA Segundo apellido de la persona)*: ESPAÑOLA *(type: utf8String)*
**1.3.6.1.4.1.47281.0.6.9** *(esFIRMA Email de la persona)*: carmen@test.esfirma.com *(type: utf8String)*