

## Perfiles de Certificados

### de ANF AC



**Nivel de Seguridad**

*Documento Público*

---

**Aviso Importante**

*Este documento es propiedad de ANF Autoridad de Certificación*

*Está prohibida su reproducción y difusión sin autorización expresa de ANF Autoridad de Certificación*

**2000 – 2025 CC-BY- ND (Creative commons licenses)**

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 932 661 614 (llamadas desde España) Internacional (+34) 933 935 946

[www.anf.es](http://www.anf.es)

# ÍNDICE

|  |           |
|--|-----------|
| <b>1. Introducción.....</b>  | <b>5</b>  |
| 1.1. Visión general .....  | 5         |
| 1.2. Aspectos comunes.....   | 5         |
| 1.3. Nombre del documento e identificación.....  | 5         |
| <b>2. Certificados de firma electrónica.....</b>                                       | <b>7</b>  |
| 2.1. Certificado de Clase 2 de Persona física .....                                    | 7         |
| 2.1.1. Sujeto.....   | 7         |
| 2.1.2. Extensiones.....  | 8         |
| 2.2. Certificado Corporativo de Persona física .....                                   | 9         |
| 2.2.1. Sujeto.....   | 9         |
| 2.2.1. Extensiones.....  | 9         |
| 2.3. Certificados de Representante Legal de Persona Jurídica.....                      | 10        |
| 2.3.1. Sujeto.....   | 10        |
| 2.3.1. Extensiones.....  | 11        |
| 2.4. Certificado de Representante Legal para administradores únicos y solidarios ..... | 12        |
| 2.4.1. Sujeto.....   | 12        |
| 2.4.2. Extensiones.....  | 12        |
| 2.5. Certificado de Representante Legal de Entidad sin Personalidad Jurídica .....     | 14        |
| 2.5.1. Sujeto.....   | 14        |
| 2.5.2. Extensiones.....  | 14        |
| 2.6. Certificado de Empleado Público .....   | 15        |
| 2.6.1. Sujeto.....   | 15        |
| 2.6.2. Extensiones.....  | 16        |
| <b>3. Certificados de sello electrónico.....</b>                                       | <b>18</b> |
| 3.1. Certificado de Sello electrónico (QSealC).....                                    | 18        |
| 3.1.1. Sujeto.....   | 18        |
| 3.1.2. Extensiones.....  | 19        |
| 3.2. Certificados de Sello electrónico para Administración Pública (QSealC APP).....   | 19        |
| 3.2.1. Sujeto.....   | 19        |
| 3.2.2. Extensiones.....  | 20        |

|           |  |           |
|-----------|--|-----------|
| 3.3.      | Certificado de Sello electrónico para PSD2 (QSealC PSD2)   | 21        |
| 3.3.1.    | Sujeto   | 21        |
| 3.3.2.    | Extensiones  | 21        |
| <b>4.</b> | <b>Certificados de autenticación de sitio web SSL</b>  | <b>23</b> |
| 4.1.      | Certificado SSL Organization Validation (SSL OV)   | 23        |
| 4.1.1.    | Sujeto   | 23        |
| 4.1.2.    | Extensiones  | 24        |
| 4.2.      | Certificado SSL SSL Validación Extendida (EV) – Certificado Cualificado de Autenticación de Sitio Web (QWAC) | 24        |
| 4.2.1.    | Sujeto   | 24        |
| 4.2.2.    | Extensiones  | 25        |
| 4.3.      | Certificado Cualificado de Autenticación de Sitio Web para PSD2 (QWAC PSD2)                                  | 25        |
| 4.3.1.    | Sujeto   | 25        |
| 4.3.2.    | Extensiones  | 26        |
| 4.4.      | Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel alto                         | 27        |
| 4.4.1.    | Sujeto   | 27        |
| 4.4.2.    | Extensiones  | 27        |
| 4.5.      | Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel medio                        | 28        |
| 4.5.1.    | Sujeto   | 28        |
| 4.5.2.    | Extensiones  | 28        |
| <b>5.</b> | <b>Certificados de respondedor OCSP</b>  | <b>30</b> |
| 5.1.      | Certificado de Respondedor OCSP  | 30        |
| 5.1.1.    | Sujeto   | 30        |
| 5.1.2.    | Extensiones  | 30        |
| <b>6.</b> | <b>Certificados de TSU</b>   | <b>32</b> |
| 6.1.      | Certificado de TSU   | 32        |
| 6.1.1.    | Sujeto   | 32        |
| 6.1.2.    | Extensiones  | 32        |

# 1. Introducción

## 1.1. Visión general

El presente documento detalla los perfiles de los certificados emitidos por ANF Autoridad de Certificación.

## 1.2. Aspectos comunes

Todos los certificados emitidos por ANF AC son de conformidad con el estándar X.509 versión 3.

Tal y como indica ETSI EN 319 412-2, el tamaño de los campos *givenName*, *surname*, *pseudonym*, *commonName*, *organizationName* y *organizationUnitName* pueden ser más largos que el límite establecido en IETF RFC 5280.

Dentro de los certificados, además de los campos estandarizados, se incluyen un conjunto de OIDs propietarios de ANF AC (1.3.6.1.4.1.18332.x.x) que aportan información relativa al suscriptor, u otra información de interés. La relación completa de códigos OID y la información asociada a los mismos puede ser consultada en la Sección “Campos Propietarios ANF AC” de la Declaración de Prácticas de Certificación de ANF AC.

Los campos con OID 1.3.6.1.4.1.18838.1.1 son propiedad de la Agencia Estatal de Administración Tributaria (AEAT). Los campos con OID 2.16.724.1.3.5.x.x, son requeridos e identificados en el Esquema de Identificación y Firma Electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.

Todos los literales se introducen en mayúsculas y sin tildes, con las excepciones del correo electrónico que estarán en minúsculas. No se incluye más de un espacio entre cadenas alfanuméricas, ni al principio ni final de cadenas alfanuméricas.

Se admite la inclusión de abreviaturas en base a una simplificación, siempre que no supongan dificultad en la interpretación de la información.

## 1.3. Nombre del documento e identificación

|                             |                                    |                             |            |
|-----------------------------|------------------------------------|-----------------------------|------------|
| <b>Nombre del documento</b> | Perfiles de Certificados de ANF AC |                             |            |
| <b>Versión</b>              | 1.2                                |                             |            |
| <b>OID</b>                  | 1.3.6.1.4.1.18332.3.1.1            |                             |            |
| <b>Fecha de aprobación</b>  | 16/01/2025                         | <b>Fecha de publicación</b> | 16/01/2025 |

### 1.3.1. Revisiones

| <b>Versión</b> | <b>Cambios</b>  | <b>Aprobación</b> | <b>Publicación</b> |
|----------------|---|-------------------|--------------------|
| 1.2            | Revisión periódica.<br>Mayor explicación en campo “Description” de los perfiles de Representación.<br>Retirada mención (FIRMA) campos OU de certificados de Persona Física y Representación | 16/01/2025        | 16/01/2025         |
| 1.1            | Retirada de la extensión AIA en los certificados de Responder OCSP  | 17/12/2024        | 17/12/2024         |

|      |   |            |            |
|------|---|------------|------------|
| 1.0. | Unificación de los documentos: <ul style="list-style-type: none"><li>• Perfiles de Certificados de Firma electrónica de ANF AC (OID 1.3.6.1.4.1.18332.3.1.1) – v.1.5</li><li>• Perfiles de Certificados de Sello electrónico de ANF AC (OID 1.3.6.1.4.1.18332.3.2.1) – v.2.4</li><li>• Perfiles de Certificados Autenticación de sitio Web SSL (OID 1.3.6.1.4.1.18332.3.3.1) – v.2.7.</li><li>• Perfiles de Certificados OCSP de ANF AC (OID 1.3.6.1.4.1.18332.24.1) – v.1.0.</li><li>• Perfiles de Certificados TSU de ANF AC (OID 1.3.6.1.4.1.18332.1.9.1.2.1) – v.1.2.</li></ul> | 21/10/2024 | 21/10/2024 |
|------|---|------------|------------|

## 2. Certificados de firma electrónica

En el presente apartado expone los perfiles de los diferentes tipos de certificados cualificados de firma electrónica emitidos por ANF Autoridad de Certificación:

- **Certificados de Persona Física**
- **Certificados Corporativos de Persona Física**
- **Certificados de Representación**
  - Certificados de Representante Legal de Persona Jurídica
  - Certificados de Representante Legal para Administradores únicos y solidarios
  - Certificados de Representante Legal de Entidad sin Personalidad Jurídica
- **Certificados de Empleado Público**

Las Políticas de Certificación asociadas estos certificados están publicadas y accesibles en la web de ANF AC: <https://www.anf.es/repositorio-legal/>

Para la elaboración de estos perfiles se ha tenido en cuenta las siguientes disposiciones:

- **Reglamento (UE) 910/2014** del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- **ETSI EN 319 412** Electronic Signatures and Infrastructures (ESI); Certificate Profiles (las 5 partes)
- **IETF RFC 3739**. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- **Política de Firma y de Certificados de la Administración General del Estado**:. Anexo 2: Perfiles de certificados electrónicos

### 2.1. Certificado de Clase 2 de Persona física

#### 2.1.1. Sujeto

| Campo                              | Descripción   |
|------------------------------------|---|
| <b>Common Name (CN)</b>            | Nombre, apellidos, guión (-) y DNI/NIE del firmante.  |
| <b>Given name (G)</b>              | Nombre del firmante tal y como aparece en el documento de identidad.                        |
| <b>Surname (SN)</b>                | Apellidos del firmante tal y como aparece en el documento de identidad.                     |
| <b>Email (E) (opcional)</b>        | Correo electrónico del firmante.  |
| <b>Country (C)</b>                 | Código de país de dos dígitos según ISO 3166-1.   |
| <b>Locality Name (L)</b>           | Ciudad del firmante.  |
| <b>State or Province (S)</b>       | Región, comunidad autónoma o provincia del firmante.  |
| <b>Organizational Unit (OU)</b>    | Certificado de Clase 2 de Persona Física  |
| <b>SerialNumber (SERIALNUMBER)</b> | NIF, NIE o número de pasaporte <sup>1</sup> del firmante codificado según ETSI EN 319 412-1 |

<sup>1</sup> Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

## 2.1.2. Extensiones

| Extensión                           | Descripción   |
|-------------------------------------|---|
| <b>Certificate Policies</b>         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.3.4.1.2.22 (Software)</li> <li>• 1.3.6.1.4.1.18332.3.4.1.4.22 (QSCD)</li> <li>• 1.3.6.1.4.1.18332.3.4.1.5.22 (Centralizado)</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.0 (QCP-n)</li> <li>• 0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul>                                  |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | Digital Signature<br>Content Commitment   |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection   |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email del firmante <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>• 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> </ul> |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI<br>CA Issuers - URI  |
| <b>QCStatement</b>                  | Mínimo: <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> En caso de certificado en QSCD o centralizado, también: <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul>   |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.  |
| <b>1.3.6.1.4.1.18332.19.1</b>       | Localizador del Operador OVP que tramitó la solicitud   |

## 2.2. Certificado Corporativo de Persona física

### 2.2.1. Sujeto

| Campo                               | Descripción   |
|-------------------------------------|---|
| <b>Common Name (CN)</b>             | Nombre, apellidos, guión (-) y DNI/NIE del firmante.  |
| <b>Given name (G)</b>               | Nombre del firmante tal y como aparece en el documento de identidad.                                  |
| <b>Surname (SN)</b>                 | Apellidos del firmante tal y como aparece en el documento de identidad.                               |
| <b>Email (E) (opcional)</b>         | Correo electrónico del firmante.  |
| <b>Country (C)</b>                  | Código de país de dos dígitos según ISO 3166-1.   |
| <b>Locality Name (L)</b>            | Ciudad del firmante.  |
| <b>State or Province (S)</b>        | Región, comunidad autónoma o provincia del firmante.  |
| <b>Description (2.5.4.13)</b>       | Cargo del firmante  |
| <b>Organizational Unit (OU)</b>     | Certificado corporativo de Persona Física   |
| <b>SerialNumber (SERIALNUMBER)</b>  | NIF, NIE o número de pasaporte <sup>2</sup> del firmante codificado según ETSI EN 319 412-1           |
| <b>Organization name (O)</b>        | Nombre de la persona jurídica con la que el firmante tiene relación laboral.                          |
| <b>Organization identifier (OI)</b> | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |
| <b>Title (T)</b>                    | Cargo, rol o posición del firmante en la organización.  |

### 2.2.1. Extensiones

| Extensión                       | Descripción  |
|---------------------------------|--|
| <b>Certificate Policies</b>     | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.3.4.1.6.22 (Software)</li> <li>• 1.3.6.1.4.1.18332.3.4.1.7.22 (QSCD)</li> <li>• 1.3.6.1.4.1.18332.3.4.1.8.22 (Centralizado)</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.0 (QCP-n)</li> <li>• 0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul> |
| <b>Basic Constraints</b>        | CA:FALSE   |
| <b>Key Usage</b>                | Digital Signature<br>Content Commitment  |
| <b>Extended Key Usage</b>       | clientAuth<br>emailProtection  |
| <b>Subject Alternative Name</b> | (Opcional) RFC822: email del firmante <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> </ul>  |

<sup>2</sup> Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

|                                     |   |
|-------------------------------------|---|
|                                     | <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>• 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> <li>• 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial del firmante</li> </ul> |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI<br>CA Issuers - URI  |
| <b>QCStatement</b>                  | <p>Mínimo:</p> <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> <p>En caso de certificado en QSCD o centralizado, también:</p> <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul> |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.  |
| <b>1.3.6.1.4.1.18332.19.1</b>       | Localizador del Operador OVP que tramitó la solicitud   |

## 2.3. Certificados de Representante Legal de Persona Jurídica

### 2.3.1. Sujeto

| Campo                           | Descripción  |
|---------------------------------|--|
| <b>Common Name (CN)</b>         | DNI/NIE, Nombre y apellidos del firmante, seguido de (R: NIF de la entidad representada). Ejemplo: <i>00000000T NOMBRE APELLIDO APELLLIDO (R: A00000000)</i> |
| <b>Given name (G)</b>           | Nombre del firmante tal y como aparece en el documento de identidad.   |
| <b>Surname (SN)</b>             | Apellidos del firmante tal y como aparece en el documento de identidad.  |
| <b>Email (E) (opcional)</b>     | Correo electrónico del firmante.   |
| <b>Country (C)</b>              | Código de país de dos dígitos según ISO 3166-1.  |
| <b>Locality Name (L)</b>        | Ciudad del firmante.   |
| <b>State or Province (S)</b>    | Región, comunidad autónoma o provincia del firmante.   |
| <b>Organization name (O)</b>    | Nombre de la persona jurídica sobre la que el firmante tiene suficientes poderes de representación.  |
| <b>Organizational Unit (OU)</b> | Certificado de Representante Legal de Persona Jurídica   |

|                                     |  |
|-------------------------------------|--|
| <b>Title (T)</b>                    | Cargo o posición del firmante en la organización.  |
| <b>Description (2.5.4.13)</b>       | Codificación del documento público que certifica las facultades del firmante o los datos de registro. Registro Público, Datos de Inscripción, Cargo, Notario y Fecha de otorgamiento |
| <b>Organization identifier (OI)</b> | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000)  |
| <b>SerialNumber (SERIALNUMBER)</b>  | NIF, NIE o número de pasaporte <sup>3</sup> del firmante.  |
| <b>1.3.6.1.4.1.18838.1.1</b>        | DNI/NIE del firmante.  |

### 2.3.1. Extensiones

| Extensión                           | Descripción   |
|-------------------------------------|---|
| <b>Certificate Policies</b>         | <p>OID de Política de certificación de ANF AC correspondiente al certificado:</p> <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.2.5.1.3 (Software)</li> <li>1.3.6.1.4.1.18332.2.5.1.10 (QSCD)</li> <li>1.3.6.1.4.1.18332.2.5.1.14 (Centralizado)</li> </ul> <p>OID según Secretaría SGIADSC de Persona Física representante de Persona Jurídica: 2.16.724.1.3.5.8</p> <p>OID de Políticas de certificación europeas (no concurrencia):</p> <ul style="list-style-type: none"> <li>0.4.0.194112.1.0 (QCP-n)</li> <li>0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul>       |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | Digital Signature<br>Content Commitment   |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection   |
| <b>Subject Alternative Name</b>     | <p>(Opcional) RFC822: email del firmante</p> <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> <li>1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> <li>1.3.6.1.4.1.18332.1 Fecha de la identificación inicial del firmante</li> </ul> |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:  |
| <b>QCStatement</b>                  | <p>Mínimo:</p> <ul style="list-style-type: none"> <li>QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> </ul>  |

<sup>3</sup> Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

|                               |   |
|-------------------------------|---|
|                               | <ul style="list-style-type: none"> <li>QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> <p>En caso de certificado en QSCD o centralizado, también:</p> <ul style="list-style-type: none"> <li>QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul> |
| <b>1.3.6.1.4.1.18332.19</b>   | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.  |
| <b>1.3.6.1.4.1.18332.19.1</b> | Localizador del Operador OVP que tramitó la solicitud   |

## 2.4. Certificado de Representante Legal para administradores únicos y solidarios

### 2.4.1. Sujeto

| Campo                               | Descripción  |
|-------------------------------------|--|
| <b>Common Name (CN)</b>             | Nombre y apellidos del firmante.   |
| <b>Given name (G)</b>               | Nombre del firmante tal y como aparece en el documento de identidad.   |
| <b>Surname (SN)</b>                 | Apellidos del firmante tal y como aparece en el documento de identidad.  |
| <b>Email (E) (opcional)</b>         | Correo electrónico del firmante.   |
| <b>Country (C)</b>                  | Código de país de dos dígitos según ISO 3166-1.  |
| <b>Locality Name (L)</b>            | Ciudad del firmante.   |
| <b>State or Province (S)</b>        | Región, comunidad autónoma o provincia del firmante.   |
| <b>Description (2.5.4.13)</b>       | Codificación del documento público que certifica las facultades del firmante o los datos de registro. Registro Público, Datos de Inscripción, Cargo, Notario y Fecha de otorgamiento |
| <b>Organization name (O)</b>        | Nombre de la persona jurídica sobre la que el firmante tiene suficientes poderes de representación.  |
| <b>Organizational Unit (OU)</b>     | Certificado de Representante Legal para administradores únicos y solidarios  |
| <b>Title (T)</b>                    | Cargo o posición del firmante en la organización.  |
| <b>Organization identifier (OI)</b> | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES- B00000000)   |
| <b>SerialNumber (SERIALNUMBER)</b>  | NIF, NIE o número de pasaporte <sup>4</sup> del firmante.  |
| <b>1.3.6.1.4.1.18838.1.1</b>        | DNI/NIE del firmante.  |

### 2.4.2. Extensiones

| Extensión                   | Descripción   |
|-----------------------------|---|
| <b>Certificate Policies</b> | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.2.5.1.9 (Software)</li> </ul> |

<sup>4</sup> Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

|                                     |   |
|-------------------------------------|---|
|                                     | <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.2.5.1.12 (QSCD)</li> <li>• 1.3.6.1.4.1.18332.2.5.1.13 (Centralizado)</li> </ul> <p>OID según Secretaría SGIADSC de Persona Física representante de Persona Jurídica: 2.16.724.1.3.5.8</p> <p>OID de Políticas de certificación europeas (no concurrencia):</p> <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.0 (QCP-n)</li> <li>• 0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul>   |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | Digital Signature<br>Content Commitment   |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection   |
| <b>Subject Alternative Name</b>     | <p>(Opcional) RFC822: email del firmante</p> <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>• 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> <li>• 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial del firmante</li> </ul> |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:  |
| <b>QCStatement</b>                  | <p>Mínimo:</p> <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> <p>En caso de certificado en QSCD o centralizado, también:</p> <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul>   |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.  |
| <b>1.3.6.1.4.1.18332.19.1</b>       | Localizador del Operador OVP que tramitó la solicitud   |

## 2.5. Certificado de Representante Legal de Entidad sin Personalidad Jurídica

### 2.5.1. Sujeto

| Campo                               | Descripción   |
|-------------------------------------|---|
| <b>Common Name (CN)</b>             | Nombre y apellidos del firmante.  |
| <b>Given name (G)</b>               | Nombre del firmante tal y como aparece en el documento de identidad.  |
| <b>Surname (SN)</b>                 | Apellidos del firmante tal y como aparece en el documento de identidad.   |
| <b>Email (E) (opcional)</b>         | Correo electrónico del firmante.  |
| <b>Country (C)</b>                  | Código de país de dos dígitos según ISO 3166-1.   |
| <b>Locality Name (L)</b>            | Ciudad del firmante.  |
| <b>State or Province (S)</b>        | Región, comunidad autónoma o provincia del firmante.  |
| <b>Description (2.5.4.13)</b>       | Codificación del documento público que certifica las facultades del firmante o los datos de registro, si es preceptivo. Cargo. Fecha del Acta de la Junta |
| <b>Organization name (O)</b>        | Nombre de la entidad sin personalidad jurídica sobre la que el firmante tiene suficientes poderes de representación.                                      |
| <b>Organizational Unit (OU)</b>     | Certificado de Representante Legal de Entidad sin personalidad jurídica   |
| <b>Title (T)</b>                    | Cargo o posición del firmante en la organización.   |
| <b>Organization identifier (OI)</b> | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES- B00000000)  |
| <b>SerialNumber (SERIALNUMBER)</b>  | NIF, NIE o número de pasaporte <sup>5</sup> del firmante.   |
| <b>1.3.6.1.4.1.18338.1.1</b>        | DNI/NIE del firmante.   |

### 2.5.2. Extensiones

| Extensión                   | Descripción  |
|-----------------------------|--|
| <b>Certificate Policies</b> | <p>OID de Política de certificación de AN F AC correspondiente al certificado:</p> <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.2.5.1.6 (Software)</li> <li>• 1.3.6.1.4.1.18332.2.5.1.11 (QSCD)</li> <li>• 1.3.6.1.4.1.18332.2.5.1.15 (Centralizado)</li> </ul> <p>OID según Secretaría SGIADSC de Persona Física representante de Persona sin Entidad Jurídica: 2.16.724.1.3.5.9</p> <p>OID de Políticas de certificación europeas (no concurrencia):</p> <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.0 (QCP-n)</li> <li>• 0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul> |
| <b>Basic Constraints</b>    | CA:FALSE   |
| <b>Key Usage</b>            | Digital Signature<br>Content Commitment  |
| <b>Extended Key Usage</b>   | clientAuth   |

<sup>5</sup> Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

|                                     |  |
|-------------------------------------|--|
|                                     | emailProtection  |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email del firmante <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>• 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> <li>• 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial del firmante</li> </ul> |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash  |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash   |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:   |
| <b>QCStatement</b>                  | Mínimo: <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> <p>En caso de certificado en QSCD o centralizado, también:</p> <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul>   |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.   |
| <b>1.3.6.1.4.1.18332.19.1</b>       | Localizador del Operador OVP que tramitó la solicitud  |

## 2.6. Certificado de Empleado Público

### 2.6.1. Sujeto

| Campo                        | Descripción   |
|------------------------------|---|
| <b>Common Name (CN)</b>      | Nombre y apellidos del firmante. + “- DNI “ + NIF del empleado público  |
| <b>Given name (G)</b>        | Nombre del firmante tal y como aparece en el documento de identidad.  |
| <b>Surname (SN)</b>          | Apellidos del firmante tal y como aparece en el documento de identidad. + “ - DNI “ + NIF del empleado público. |
| <b>Email (E) (opcional)</b>  | Correo electrónico del firmante.  |
| <b>Country (C)</b>           | Código de país de dos dígitos según ISO 3166-1.   |
| <b>Locality Name (L)</b>     | Ciudad del firmante.  |
| <b>State or Province (S)</b> | Región, comunidad autónoma o provincia del firmante.  |

|                                    |  |
|------------------------------------|--|
| <b>Organization name (O)</b>       | Denominación de la Administración, organismo o entidad de derecho público a la que se encuentra vinculada el empleado. |
| <b>Organizational Unit (OU)</b>    | Certificado de Empleado Público  |
| <b>Title (T)</b>                   | Cargo o posición del firmante que le vincula con la Administración, organismo o entidad de derecho público.            |
| <b>SerialNumber (SERIALNUMBER)</b> | NIF, NIE   |

## 2.6.2. Extensiones

| Extensión                           | Descripción  |
|-------------------------------------|--|
| <b>Certificate Policies</b>         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.4.1.1.22 (Autenticación nivel alto)</li> <li>1.3.6.1.4.1.18332.4.1.4.22 (Cifrado nivel alto)</li> <li>1.3.6.1.4.1.18332.4.1.3.22 (Firma nivel alto)</li> <li>1.3.6.1.4.1.18332.4.1.2.22 (Nivel medio)</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>0.4.0.194112.1.0 (QCP-n)</li> <li>0.4.0.194112.1.2 (QCP-n-qscd)</li> </ul> |
| <b>Basic Constraints</b>            | CA:FALSE   |
| <b>Key Usage</b>                    | Digital Signature<br>Content Commitment  |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection  |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email del firmante <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad.</li> <li>1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.</li> <li>1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente).</li> <li>1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante</li> </ul>  |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash  |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash   |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:   |
| <b>QCStatement</b>                  | Mínimo: <ul style="list-style-type: none"> <li>QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica)</li> </ul> En caso de certificado en QSCD o centralizado, también:  |

|                               |   |
|-------------------------------|---|
|                               | <ul style="list-style-type: none"><li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li></ul> |
| <b>1.3.6.1.4.1.18332.19</b>   | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.                            |
| <b>1.3.6.1.4.1.18332.19.1</b> | Localizador del Operador OVP que tramitó la solicitud   |

## 3. Certificados de sello electrónico

En el presente apartado expone los perfiles de los diferentes tipos de certificados cualificados de sello electrónico emitidos por ANF Autoridad de Certificación:

- **Certificados de Sello electrónico** (*QSealC*)
- **Certificados de Sello electrónico para Administración Pública** (*QSealC APP*)
- **Certificados de Sello electrónico para PSD2** (*QSealC PSD2*)

Las Políticas de Certificación asociadas estos certificados están publicadas y accesibles en la web de ANF AC: <https://www.anf.es/repositorio-legal/>

Para la elaboración de estos perfiles se ha tenido en cuenta las siguientes disposiciones:

- **Reglamento (UE) 910/2014** del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- **ETSI EN 319 412** Electronic Signatures and Infrastructures (ESI); Certificate Profiles (las 5 partes)
- **ETSI TS 119 495** Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- **IETF RFC 3739**. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- **Política de Firma y de Certificados de la Administración General del Estado**:. Anexo 2: Perfiles de certificados electrónicos

### 3.1. Certificado de Sello electrónico (QSealC)

#### 3.1.1. Sujeto

| Campo   | Descripción   |
|---|---|
| <b>Common Name (CN)</b>                             | Nombre comercial de la persona jurídica.  |
| <b>Email (E)</b> ( <i>opcional</i> )                | Correo electrónico de contacto de la organización.  |
| <b>Country (C)</b>                                  | Código de país de dos dígitos según ISO 3166-1.   |
| <b>Locality Name (L)</b> ( <i>opcional</i> )        | Ciudad del suscriptor.  |
| <b>State or Province (S)</b> ( <i>opcional</i> )    | Región, comunidad autónoma o provincia del suscriptor.  |
| <b>Organization name (O)</b>                        | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.                   |
| <b>Organizational Unit (OU)</b> ( <i>opcional</i> ) | Certificado Cualificado de Sello Electrónico  |
| <b>Organizational Unit (OU)</b> ( <i>opcional</i> ) | Departamento o Unidad dentro de la organización.  |
| <b>Organization identifier (OI)</b>                 | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |

### 3.1.2. Extensiones

| Extensión                           | Descripción  |
|-------------------------------------|--|
| <b>Certificate Policies</b>         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.25.1.1.1 (Software)</li> <li>• 1.3.6.1.4.1.18332.25.1.1.4 (QSCD)</li> <li>• 1.3.6.1.4.1.18332.25.1.1.9 (Centralizado)</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.1 (QCP-I)</li> <li>• 0.4.0.194112.1.3 (QCP-I-qscd)</li> </ul> |
| <b>Basic Constraints</b>            | CA:FALSE   |
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Content Commitment</i><br><i>Key Encipherment</i>   |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection  |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email del contacto <ul style="list-style-type: none"> <li>• 1.3.6.1. 4.1.18332.10.4 - NIF de la entidad</li> </ul>  |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash  |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash   |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | OCSP - URI<br>CA Issuers - URI   |
| <b>QCStatement</b>                  | Mínimo: <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico)</li> </ul> En caso de certificado en QSCD o centralizado, también: <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul>  |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.   |

## 3.2. Certificados de Sello electrónico para Administración Pública (QSealC APP)

### 3.2.1. Sujeto

| Campo                               | Descripción  |
|-------------------------------------|--|
| <b>Common Name (CN)</b>             | Nombre comercial de la persona jurídica.           |
| <b>Email (E) (opcional)</b>         | Correo electrónico de contacto de la organización. |
| <b>Country (C)</b>                  | Código de país de dos dígitos según ISO 3166-1.    |
| <b>Locality Name (L) (opcional)</b> | Ciudad del suscriptor.                             |

|   |   |
|---|---|
| <b>State or Province (S)</b> <i>(opcional)</i>    | Región, comunidad autónoma o provincia del suscriptor.  |
| <b>Organization name (O)</b>                      | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.                   |
| <b>Organizational Unit (OU)</b> <i>(opcional)</i> | Certificado de Sello Electrónico  |
| <b>Organizational Unit (OU)</b> <i>(opcional)</i> | Departamento o Unidad dentro de la organización.  |
| <b>Organization identifier (OI)</b>               | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |

### 3.2.2. Extensiones

| Extensión                           | Descripción   |
|-------------------------------------|---|
| <b>Certificate Policies</b>         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.25.1.1.3 (Software) – nivel medio</li> <li>• 1.3.6.1.4.1.18332.25.1.1.12 (Dis.Claves) – nivel medio</li> <li>• 1.3.6.1.4.1.18332.25.1.1.2 (QSCD) – nivel alto</li> <li>• 1.3.6.1.4.1.18332.25.1.1.11 (Centralizado) – nivel alto</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.1 (QCP-I)</li> <li>• 0.4.0.194112.1.3 (QCP-I-qscd)</li> </ul> OID según SGIADS: <ul style="list-style-type: none"> <li>• 2.16.724.1.3.5.6.1 (nivel alto)</li> <li>• 2.16.724.1.3.5.6.2 (nivel medio)</li> </ul> |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Content Commitment</i><br><i>Key Encipherment</i>  |
| <b>Extended Key Usage</b>           | clientAuth<br>emailProtection   |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email de contacto<br>Directoryname:<br>2.16.724.1.3.5.6.2.1 = "SELLO ELECTRONICO DE NIVEL MEDIO" o "SELLO ELECTRONICO DE NIVEL ALTO"<br>2.16.724.1.3.5.6.1.2 = <O del DN><br>2.16.724.1.3.5.6.1 .3 = <serialNumber del DN><br>(opcional) 2.16.724.1.3.5.6.1 .4 = <NIF/NIE del custodio><br>2.16.724.1.3.5.6.1 .5 = <CN del DN><br>(opcional) 2.16.724.1.3.5.6.1 .6 = <Given name><br>(opcional) 2.16.724.1.3.5.6.1 .7 = <Primer apellido del custodio><br>(opcional) 2.16.724.1.3.5.6.1 .8 = <Segundo apellido del custodio><br>(opcional) 2.16.724.1.3.5.6.1 .9 = <correo electrónico del custodio>   |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:  |
| <b>QCStatement</b>                  | Mínimo:   |

|                             |  |
|-----------------------------|--|
|                             | <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico)</li> </ul> <p>En caso de certificado en QSCD o centralizado, también:</p> <ul style="list-style-type: none"> <li>• QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)</li> </ul> |
| <b>1.3.6.1.4.1.18332.19</b> | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.   |

### 3.3. Certificado de Sello electrónico para PSD2 (QSealC PSD2)

#### 3.3.1. Sujeto

| Campo   | Descripción  |
|---|--|
| <b>Common Name (CN)</b>                           | Nombre comercial de la persona jurídica.   |
| <b>Email (E)</b> <i>(opcional)</i>                | Correo electrónico de contacto de la organización.   |
| <b>Country (C)</b>                                | Código de país de dos dígitos según ISO 3166-1.  |
| <b>Locality Name (L)</b>                          | Ciudad del suscriptor.   |
| <b>State or Province (S)</b>                      | Región, comunidad autónoma o provincia del suscriptor.   |
| <b>Organization name (O)</b>                      | Denominación exacta de la persona jurídica según aparezca en el Registro público de la Autoridad Nacional Competente (NCA) del Estado Miembro de origen o en los registros oficiales de la Autoridad Bancaria Europea (EBA). |
| <b>Organizational Unit (OU)</b> <i>(opcional)</i> | Certificado de Sello Electrónico PSD2  |
| <b>Organizational Unit (OU)</b> <i>(opcional)</i> | Departamento o Unidad dentro de la organización.   |
| <b>Organization identifier (OI)</b>               | Número de autorización PSD2 de la organización, codificado según la especificación técnica ETSI TS 119 495   |
| <b>SerialNumber (SERIALNUMBER)</b>                | NIF de la entidad  |

#### 3.3.2. Extensiones

| Extensión                   | Descripción   |
|-----------------------------|---|
| <b>Certificate Policies</b> | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.25.1.1.5 (Software)</li> </ul> OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.1 (QCP-I)</li> </ul> |
| <b>Basic Constraints</b>    | CA:FALSE  |
| <b>Key Usage</b>            | <i>Digital Signature</i><br><i>Content Commitment</i><br><i>Key Encipherment</i>  |
| <b>Extended Key Usage</b>   | clientAuth  |

|                                     |   |
|-------------------------------------|---|
|                                     | emailProtection   |
| <b>Subject Alternative Name</b>     | (Opcional) RFC822: email del contacto<br>1.3.6.1. 4.1.18332.10.4 - NIF de la entidad  |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | OCSP - URI:<br>CA Issuers - URI:  |
| <b>QCStatement</b>                  | <p>Mínimo:</p> <ul style="list-style-type: none"> <li>• QcCompliance: 0.4.0.1862.1.1 (indica que es un certificado cualificado)</li> <li>• QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico)</li> <li>• PSD2QcStatement: 0.4.0.19495.2 incluyendo: <ul style="list-style-type: none"> <li>• RoIPSD2: <ul style="list-style-type: none"> <li>○ servicio de cuentas (PSP_AS);</li> <li>○ iniciación de pago (PSP_PI);</li> <li>○ información de la cuenta (PSP_AI);</li> <li>○ emisión de instrumentos de pago basados en tarjeta (PSP_IC).</li> </ul> </li> <li>• Nombre de la Autoridad Nacional Competente donde el PSP está registrado. Esta información se proporciona en dos formas: la cadena de nombre completo (<i>NCAName</i>) y un identificador único abreviado (<i>NCAId</i>).</li> </ul> </li> </ul> <p>Conforme a ETSI TS 119 495 clausula 5.1.</p> |
| <b>1.3.6.1.4.1.18332.19</b>         | Localizador de la solicitud del certificado generado al momento de procederse a la identificación.  |

## 4. Certificados de autenticación de sitio web SSL

El presente apartado expone los perfiles de los diferentes tipos de certificados de autenticación de sitio web SSL emitidos por ANF Autoridad de Certificación:

- **Certificados SSL Organization Validation (SSL OV)**
- **Certificado SSL Validación Extendida (EV) – Certificado Cualificado de Autenticación de Sitio Web (QWAC)**
- **Certificado Cualificado de Autenticación de Sitio Web para PSD2 (QWAC PSD2)**
- **Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel alto**
- **Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel medio**

Las Políticas de Certificación asociadas estos certificados están publicadas y accesibles en la web de ANF AC: <https://www.anf.es/repositorio-legal/>

Para la elaboración de estos perfiles se ha tenido en cuenta las siguientes disposiciones:

- **Reglamento (UE) 910/2014** del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- **ETSI EN 319 412** Electronic Signatures and Infrastructures (ESI); Certificate Profiles (partes 1, 4 y 5)
- **ETSI TS 119 495** Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- **IETF RFC 3739**. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- **CA/B Forum Baseline Requirements** for the Issuance and Management of Publicly-Trusted Certificates situados en <https://cabforum.org/baseline-requirements-documents> ,
- **CA/B Forum Guidelines for Extended Validation** Certificates situados en <https://cabforum.org/extended-validation> ,
- **Política de Firma y de Certificados de la Administración General del Estado**:. Anexo 2: Perfiles de certificados electrónicos

### 4.1. Certificado SSL Organization Validation (SSL OV)

#### 4.1.1. Sujeto

| Campo                              | Descripción   |
|------------------------------------|---|
| <b>Organization name (O)</b>       | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil. |
| <b>SerialNumber (SERIALNUMBER)</b> | NIF de la Persona Jurídica  |
| <b>Country (C)</b>                 | Código de país de dos dígitos según ISO 3166-1.                                     |
| <b>State or Province (S)</b>       | Región, comunidad autónoma o provincia del suscriptor.                              |
| <b>Locality Name (L)</b>           | Ciudad del suscriptor.  |

#### 4.1.2. Extensiones

| Extensión                    | Descripción   |
|------------------------------|---|
| Certificate Policies         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.55.1.1.7.322</li> </ul> OID de CAB/Forum: <ul style="list-style-type: none"> <li>2.23.140.1.2.2 (OVCP)</li> </ul>   |
| Basic Constraints            | CA:FALSE  |
| Key Usage                    | Digital Signature<br>Key Encipherment   |
| Extended Key Usage           | clientAuth<br>serverAuth  |
| Subject Alternative Name     | dNSName que contenga Fully-Qualified Domain Name (FQDN) verificado.   |
| Subject Key Identifier       | ID clave pública del certificado obtenido a partir del hash   |
| Authority Key Identifier     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| CRL Distribution Points      | URI de la CRL   |
| Authority Information Access | Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)<br>Access Location 1: <a href="http://ocsp.anf.es/spain/AV">http://ocsp.anf.es/spain/AV</a><br>Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)<br>Access Location 2: <a href="http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer">http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer</a> |

## 4.2. Certificado SSL SSL Validación Extendida (EV) – Certificado Cualificado de Autenticación de Sitio Web (QWAC)

### 4.2.1. Sujeto

| Campo  | Descripción   |
|--|---|
| Organization name (O)                                | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.                   |
| Organization identifier (OI)                         | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |
| SerialNumber (SERIALNUMBER)                          | NIF de la Persona Jurídica  |
| Country (C)  | Código de país de dos dígitos según ISO 3166-1.   |
| State or Province (S)                                | Región, comunidad autónoma o provincia del suscriptor.  |
| Locality Name (L)                                    | Ciudad del suscriptor.  |
| Business Category                                    | · "Private Organization"<br>· "Government Entity"<br>· "Business Entity"<br>· "Non-Commercial Entity" |
| Jurisdiction Of Incorporation Country Name           | Subject Jurisdiction of Incorporation or Registration   |
| Jurisdiction Of Incorporation State Or Province Name | Subject Jurisdiction of Incorporation or Registration (no siempre está presente)                      |

|  |  |
|--|--|
| <b>Jurisdiction Of Incorporation<br/>Locality Name</b> | Subject Jurisdiction of Incorporation or Registration (no siempre está presente) |
|--|--|

#### 4.2.2. Extensiones

| Extensión                           | Descripción   |
|-------------------------------------|---|
| <b>Certificate Policies</b>         | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>1.3.6.1.4.1.18332.55.1.1.2.322</li> </ul> OID de Políticas de certificación europeas: <ul style="list-style-type: none"> <li>0.4.0.194112.1.4 (Qcp-w)</li> </ul> OID de CAB/Forum: <ul style="list-style-type: none"> <li>2.23.140.1.1 (EVCP)</li> </ul>  |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Key Encipherment</i>   |
| <b>Extended Key Usage</b>           | clientAuth<br>serverAuth  |
| <b>Subject Alternative Name</b>     | dNSName que contenga Fully-Qualified Domain Name (FQDN) verificado.   |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)<br>Access Location 1: <a href="http://ocsp.anf.es/spain/AV">http://ocsp.anf.es/spain/AV</a><br>Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)<br>Access Location 2: <a href="http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer">http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer</a> |
| <b>cabfOrganizationIdentifier</b>   | <ul style="list-style-type: none"> <li>3 caracteres, identificador del esquema</li> <li>Código de país de dos dígitos ISO 3166-1</li> <li>Identificador de la organización conforme al esquema</li> </ul>   |
| <b>QCStatement</b>                  | Mínimo:<br>QcCompliance: 0.4.0.1862.1.1<br>QcType: 0.4.0.1862.1.6.3   |

### 4.3. Certificado Cualificado de Autenticación de Sitio Web para PSD2 (QWAC PSD2)

#### 4.3.1. Sujeto

| Campo                        | Descripción  |
|------------------------------|--|
| <b>Organization name (O)</b> | Denominación exacta de la persona jurídica según aparezca en el Registro público de la Autoridad Nacional Competente (NCA) del |

|   |   |
|---|---|
|   | Estado Miembro de origen o en los registros oficiales de la Autoridad Bancaria Europea (EBA).   |
| <b>Organization identifier (OI)</b>                         | Número de autorización PSD2 de la organización, codificado según la especificación técnica ETSI TS 119 495  |
| <b>SerialNumber (SERIALNUMBER)</b>                          | NIF de la Persona Jurídica  |
| <b>Country (C)</b>  | Código de país de dos dígitos según ISO 3166-1.   |
| <b>State or Province (S)</b>                                | Región, comunidad autónoma o provincia del suscriptor.  |
| <b>Locality Name (L)</b>                                    | Ciudad del suscriptor.  |
| <b>Business Category</b>                                    | <ul style="list-style-type: none"> <li>· "Private Organization"</li> <li>· "Government Entity"</li> <li>· "Business Entity"</li> <li>· "Non-Commercial Entity"</li> </ul> |
| <b>Jurisdiction Of Incorporation Country Name</b>           | Subject Jurisdiction of Incorporation or Registration   |
| <b>Jurisdiction Of Incorporation State Or Province Name</b> | Subject Jurisdiction of Incorporation or Registration (no siempre está presente)  |
| <b>Jurisdiction Of Incorporation Locality Name</b>          | Subject Jurisdiction of Incorporation or Registration (no siempre está presente)  |

#### 4.3.2. Extensiones

| Extensión                           | Descripción  |
|-------------------------------------|--|
| <b>Certificate Policies</b>         | <p>OID de Política de certificación de ANF AC correspondiente al certificado:</p> <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.55.1.1.8.22</li> </ul> <p>OID de Políticas de certificación europeas:</p> <ul style="list-style-type: none"> <li>• 0.4.0.19495.3 (Qcp-w-psd2)</li> <li>• 0.4.0.194112.1.4 (Qcp-w)</li> </ul> <p>OID de CAB/Forum:</p> <ul style="list-style-type: none"> <li>• 2.23.140.1.1 (EVCP)</li> </ul> |
| <b>Basic Constraints</b>            | CA:FALSE   |
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Key Encipherment</i>  |
| <b>Extended Key Usage</b>           | clientAuth<br>serverAuth   |
| <b>Subject Alternative Name</b>     | dNSName que contenga Fully-Qualified Domain Name (FQDN) verificado.  |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash  |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash   |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | <p>Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)</p> <p>Access Location 1: <a href="http://ocsp.anf.es/spain/AV">http://ocsp.anf.es/spain/AV</a></p> <p>Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)</p> <p>Access Location 2: <a href="http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer">http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer</a></p>   |
| <b>cabfOrganizationIdentifier</b>   | <ul style="list-style-type: none"> <li>• 3 caracteres, identificador del esquema</li> </ul>  |

|                    |  |
|--------------------|--|
|                    | <ul style="list-style-type: none"> <li>• Código de país de dos dígitos ISO 3166-1</li> <li>• Identificador de la organización conforme al esquema</li> </ul> |
| <b>QCStatement</b> | Mínimo:<br>QcCompliance: 0.4.0.1862.1.1<br>QcType: 0.4.0.1862.1.6.3<br>PSD2QcStatement: 0.4.0.19495.2 incluyendo el RolPSD2, nCAName y nCAId.                |

#### 4.4. Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel alto

##### 4.4.1. Sujeto

| Campo   | Descripción   |
|---|---|
| <b>Organizational unit (OU)</b>                   | SEDE ELECTRONICA  |
| <b>Organizational unit (OU)</b>                   | Nombre descriptivo de la sede   |
| <b>Organization name (O)</b>                      | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.                   |
| <b>Organization identifier (OI)</b>               | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |
| <b>SerialNumber (SERIALNUMBER)</b>                | El NIF de la entidad responsable  |
| <b>Country (C)</b>                                | Código de país de dos dígitos según ISO 3166-1.   |
| <b>State or Province (S)</b>                      | Región, comunidad autónoma o provincia del suscriptor.  |
| <b>Locality Name (L)</b>                          | Ciudad del suscriptor.  |
| <b>Business Category</b>                          | "Government Entity"   |
| <b>Jurisdiction Of Incorporation Country Name</b> | Subject Jurisdiction of Incorporation or Registration   |

##### 4.4.2. Extensiones

| Extensión                   | Descripción  |
|-----------------------------|--|
| <b>Certificate Policies</b> | OID de Política de certificación de ANF AC correspondiente al certificado: <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.55.1.1.6.322</li> </ul> OID según SGIADS: <ul style="list-style-type: none"> <li>• 2.16.724.1.3.5.5.1 (Nivel alto)</li> <li>• 0.4.0.2042.1.4 (OID de SSL EV)</li> </ul> OID de Políticas de certificación europeas: <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.4 (Qcp-w)</li> </ul> OID de CAB/Forum: <ul style="list-style-type: none"> <li>• 2.23.140.1.1 (EVCP)</li> </ul> |
| <b>Basic Constraints</b>    | CA:FALSE   |

|                                     |   |
|-------------------------------------|---|
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Key Encipherment</i>   |
| <b>Extended Key Usage</b>           | serverAuth  |
| <b>Subject Alternative Name</b>     | dNSName que contenga Fully-Qualified Domain Name (FQDN) verificado.   |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)<br>Access Location 1: <a href="http://ocsp.anf.es/spain/AV">http://ocsp.anf.es/spain/AV</a><br>Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)<br>Access Location 2: <a href="http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer">http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer</a> |
| <b>cabfOrganizationIdentifier</b>   | <ul style="list-style-type: none"> <li>• 3 caracteres, identificador del esquema</li> <li>• Código de país de dos dígitos ISO 3166-1</li> <li>• Identificador de la organización conforme al esquema</li> </ul>   |
| <b>QCStatement</b>                  | Mínimo:<br>QcCompliance: 0.4.0.1862.1.1<br>QcType: 0.4.0.1862.1.6.3   |

## 4.5. Certificado Cualificado de Sede Electrónica con Validación Extendida (EV) Nivel medio

### 4.5.1. Sujeto

| Campo   | Descripción   |
|---|---|
| <b>Organizational unit (OU)</b>                   | SEDE ELECTRONICA  |
| <b>Organizational unit (OU)</b>                   | Descriptive name of the electronic headquarters   |
| <b>Organization name (O)</b>                      | Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.                   |
| <b>Organization identifier (OI)</b>               | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000) |
| <b>SerialNumber (SERIALNUMBER)</b>                | NIF de la Persona Jurídica  |
| <b>Country (C)</b>                                | Código de país de dos dígitos según ISO 3166-1.   |
| <b>State or Province (S)</b>                      | Región, comunidad autónoma o provincia del suscriptor.  |
| <b>Locality Name (L)</b>                          | Ciudad del suscriptor.  |
| <b>Business Category</b>                          | "Government Entity"   |
| <b>Jurisdiction Of Incorporation Country Name</b> | Subject Jurisdiction of Incorporation or Registration   |

### 4.5.2. Extensiones

| Extensión | Descripción |
|-----------|-------------|
|-----------|-------------|

|                                     |   |
|-------------------------------------|---|
| <b>Certificate Policies</b>         | <p>OID de Política de certificación de ANF AC correspondiente al certificado:</p> <ul style="list-style-type: none"> <li>• 1.3.6.1.4.1.18332.55.1.1.5.322</li> </ul> <p>OID según SGIADS:</p> <ul style="list-style-type: none"> <li>• 2.16.724.1.3.5.5.2 (Nivel medio)</li> </ul> <p>OID de Políticas de certificación europeas:</p> <ul style="list-style-type: none"> <li>• 0.4.0.194112.1.4 (QEVCP-w)</li> </ul> <p>OID de CAB/Forum:</p> <ul style="list-style-type: none"> <li>• 2.23.140.1.1 (EVCP)</li> </ul> |
| <b>Basic Constraints</b>            | CA:FALSE  |
| <b>Key Usage</b>                    | <i>Digital Signature</i><br><i>Key Encipherment</i>   |
| <b>Extended Key Usage</b>           | serverAuth  |
| <b>Subject Alternative Name</b>     | dNSName que contenga Fully-Qualified Domain Name (FQDN) verificado.   |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash   |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash  |
| <b>CRL Distribution Points</b>      | URI de la CRL   |
| <b>Authority Information Access</b> | <p>Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1)<br/>           Access Location 1: <a href="http://ocsp.anf.es/spain/AV">http://ocsp.anf.es/spain/AV</a><br/>           Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)<br/>           Access Location 2: <a href="http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer">http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer</a></p>  |
| <b>cabfOrganizationIdentifier</b>   | <ul style="list-style-type: none"> <li>• 3 caracteres, identificador del esquema</li> <li>• Código de país de dos dígitos ISO 3166-1</li> <li>• Identificador de la organización conforme al esquema</li> </ul>   |
| <b>QCStatement</b>                  | <p>Mínimo:<br/>           QcCompliance: 0.4.0.1862.1.1<br/>           QcType: 0.4.0.1862.1.6.3</p>  |

## 5. Certificados de respondedor OCSP

En el presente apartado expone el perfil de los certificados OCSP de ANF Autoridad de certificación.

Las Políticas de Certificación asociadas estos certificados están publicadas y accesibles en la web de ANF AC:  
<https://www.anf.es/repositorio-legal/>

Para la elaboración de estos perfiles se ha tenido en cuenta las siguientes disposiciones:

- **Reglamento (UE) 910/2014** del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- **ETSI EN 319 412-1**. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- **IETF RFC 6960**. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

### 5.1. Certificado de Respondedor OCSP

#### 5.1.1. Sujeto

| Campo   | Descripción  |
|---|--|
| <b>Common Name (CN)</b>                           | Nombre CA + Responder + N°                           |
| <b>Organization name (O)</b>                      | ANF Autoridad de Certificación                       |
| <b>Organization Identifier (OI)</b>               | VATES-G63287510                                      |
| <b>Organizational Unit (OU)</b> <i>(opcional)</i> | ANF Autoridad Intermedia de Identidad                |
| <b>Country (C)</b>                                | Código de país de dos dígitos según ISO 3166-1. (ES) |

#### 5.1.2. Extensiones

| Extensión                           | Descripción  |
|-------------------------------------|--|
| <b>Certificate Policies</b>         | 1.3.6.1.4.1.18332.56.1.1   |
| <b>Basic Constraints</b>            | CA:FALSE   |
| <b>Key Usage</b>                    | Digital Signature<br>Non repudiation   |
| <b>Extended Key Usage</b>           | OCSPSigning  |
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash  |
| <b>Authority Key Identifier</b>     | No incluido  |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | OCSP - URI<br>CA Issuers - URI   |
| <b>QCStatement</b>                  | QcCompliance: 0.4.0.1862.1.1<br>QcType: 0.4.0.1862.1.6.2<br>QcRetentionPeriod: 0.4.0.1862.1.3 (15 años)<br>QcPDS: 0.4.0.1862.1.5 ( <a href="https://anf.es/en/">https://anf.es/en/</a> ) |

|  |                    |
|--|--------------------|
| <b>id-pkix-ocspnocheck</b><br>(1.3.6.1.5.5.7.48.1.5) | ocspNoCheck (OCSP) |
|--|--------------------|

## 6. Certificados de TSU

En el presente apartado expone el perfil de los certificados TSU de ANF Autoridad de certificación.

Las Políticas de Certificación asociadas estos certificados están publicadas y accesibles en la web de ANF AC:  
<https://www.anf.es/repositorio-legal/>

Para la elaboración de estos perfiles se ha tenido en cuenta las siguientes disposiciones:

- **Reglamento (UE) 910/2014** del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- **ETSI EN 319 422** Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- **ETSI EN 319 412-3**. "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"
- **IETF RFC 3739**. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- **IETF RFC 3161** Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

Tal y como indica ETSI EN 319 412-2, el tamaño de los campos *givenName*, *surname*, *pseudonym*, *commonName*, *organizationName* y *organizationUnitName* pueden ser más largos que el límite establecido en IETF RFC 5280.

### 6.1. Certificado de TSU

#### 6.1.1. Sujeto

| Campo                                      | Descripción  |
|--|--|
| <b>Common Name (CN)</b>                    | Identificador de TSU. Identifica de manera única la TSU correspondiente ( <i>p.ej: ANF Timestamp Unit 1341</i> ) |
| <b>Country (C)</b>                         | Código de país de dos dígitos según ISO 3166-1 en el que está establecida la TSA (ES).                           |
| <b>Organization name (O)</b>               | ANF Autoridad de Certificación   |
| <b>Organization Identifier (OI)</b>        | VATES-G63287510  |
| <b>Organizational Unit (OU) (opcional)</b> | TSU  |

#### 6.1.2. Extensiones

| Extensión                   | Descripción   |
|-----------------------------|---|
| <b>Certificate Policies</b> | Policy:1.3.6.1.4.1.18332.15.1<br>CPS: <a href="https://www.anf.es/documentos">https://www.anf.es/documentos</a> |
| <b>Basic Constraints</b>    | CA:FALSE  |
| <b>Key Usage</b>            | Digital Signature<br>Non repudiation  |
| <b>Extended Key Usage</b>   | Time Stamping   |

|                                     |  |
|-------------------------------------|--|
| <b>Subject Key Identifier</b>       | ID clave pública del certificado obtenido a partir del hash          |
| <b>Authority Key Identifier</b>     | ID clave pública del certificado de la CA obtenido a partir del hash |
| <b>CRL Distribution Points</b>      | URI de la CRL  |
| <b>Authority Information Access</b> | OCSP - URI<br>CA Issuers - URI                                       |

Los Tokens de Timestamp cualificados, deberían incluir una instancia de la extensión qcStatements, de acuerdo con la sintaxis definida en IETF RFC 3739, cláusula 3.2.6.

La extensión debería incluir una instancia de "esi4-qtstStatement-1" de acuerdo con lo definido en el Anexo B de la norma ETSI TS 319 422.