

Perfiles de Certificados de Firma electrónica 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 – 2020 Copyright © ANF Autoridad de Certificación

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

Teléfono: 902 902 172 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

ÍNDICE

| | |
|---|-----------|
| 1. Introducción | 4 |
| 1.1. Visión general | 4 |
| 1.2. Nombre del documento e identificación..... | 4 |
| 2. Certificado de Clase 2 de Persona física | 5 |
| 2.1. Sujeto..... | 5 |
| 2.2. Extensiones..... | 5 |
| 3. Certificados de Representante Legal de Persona Jurídica | 6 |
| 3.1. Sujeto..... | 6 |
| 3.2. Extensiones..... | 6 |
| 4. Certificado de Representante Legal para administradores únicos y solidarios | 8 |
| 4.1. Sujeto..... | 8 |
| 4.2. Extensiones..... | 8 |
| 5. Certificado de Representante Legal de Entidad sin Personalidad Jurídica | 10 |
| 5.1. Sujeto..... | 10 |
| 5.2. Extensiones..... | 10 |
| 6. Certificado de Empleado Público | 12 |
| 6.1. Sujeto..... | 12 |
| 6.2. Extensiones..... | 12 |

1. Introducción

1.1. Visión general

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

- **Certificados 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

1.2. Nombre del documento e identificación

| | | | |
|-----------------------------|---|-----------------------------|------------|
| Nombre del documento | Perfiles de Certificados de Firma electrónica de ANF AC | | |
| Versión | 1.0 | | |
| OID | 1.3.6.1.4.1.18332.3.1.1 | | |
| Fecha de aprobación | 18/01/2020 | Fecha de publicación | 18/01/2020 |

1.2.1. Revisiones

| Versión | Cambios | Aprobación | Publicación |
|----------------|--|-------------------|--------------------|
| 1.0. | <p>Unificación de los documentos</p> <ul style="list-style-type: none">• “Certificados de Clase 2 de Persona Física Perfil Técnico” OID 1.3.6.1.4.1.18332.3.4.1.2• “Certificados de Representante Legal de Personas Jurídicas Perfil Técnico” OID 1.3.6.1.4.1.18332.2.5.3• “Certificados de Representante Legal de Administradores Únicos y Solidarios. Perfil Técnico” OID 1.3.6.1.4.1.18332.2.5.2• “Certificados de Representante Legal de Entidad sin Personalidad Jurídica. Perfil Técnico” OID 1.3.6.1.4.1.18332.2.5.4• “Certificados de Empleado Público Perfil Técnico” OID 1.3.6.1.4.1.18332.4.1.2 | 18/01/2020 | 18/01/2020 |

2. Certificado de Clase 2 de Persona física

2.1. Sujeto

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

2.2. Extensiones

| Extensión | Descripción |
|------------------------------|---|
| Certificate Policies | OID de Política de certificación de AN F AC correspondiente al certificado: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.3.4.1.2.22 (Software) 1.3.6.1.4.1.18332.3.4.1.4.22 (QSCD) 1.3.6.1.4.1.18332.3.4.1.5.22 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> 0.4.0.194112.1.0 (QCP-n) 0.4.0.194112.1.2 (QCP-n-qscd) |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Content Commitment |
| Extended Key Usage | clientAuth emailProtection |
| Subject Alternative Name | (Opcional) RFC822: email del firmante |
| 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 | OCSP - URI CA Issuers - URI |
| QCStatement | Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.1 |

3. Certificados de Representante Legal de Persona Jurídica

3.1. Sujeto

| Campo | Descripción |
|------------------------------|---|
| Common Name (CN) | Nombre y apellidos del firmante. |
| Given name (G) | Nombre del firmante tal y como aparece en el documento de identidad. |
| Surname | Apellidos del firmante tal y como aparece en el documento de identidad. |
| Email (E) | Correo electrónico del firmante. |
| Country (C) | Código de país de dos dígitos según ISO 3166-1. |
| Locality Name (L) | Ciudad del firmante. |
| State or Province (S) | Región, comunidad autónoma o provincia del firmante. |
| Organization name (O) | Nombre de la persona jurídica sobre la que el firmante tiene suficientes poderes de representación. |
| Organizational Unit (OU) | Certificado de Representante Legal de Persona Jurídica (FIRMA) |
| Title (T) | Cargo o posición del firmante en la organización. |
| Organization identifier (OI) | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B0085974Z) |
| SerialNumber (SERIALNUMBER) | NIF, NIE o número de pasaporte del firmante. |

3.2. Extensiones

| Extensión | Descripción |
|------------------------------|--|
| Certificate Policies | OID de Política de certificación de AN F AC correspondiente al certificado: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.2.5.1.3 (Software) • 1.3.6.1.4.1.18332.2.5.1.10 (QSCD) • 1.3.6.1.4.1.18332.2.5.1.14 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> • 0.4.0.194112.1.0 (QCP-n) • 0.4.0.194112.1.2 (QCP-n-qscd) |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Content Commitment |
| Extended Key Usage | clientAuth emailProtection |
| Subject Alternative Name | (Opcional) RFC822: email del firmante |
| 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 | OCSP - URI: CA Issuers - URI: |
| QCStatement | Mínimo: |

| | |
|--|--|
| | QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.1 |
|--|--|

4. Certificado de Representante Legal para administradores únicos y solidarios

4.1. Sujeto

| Campo | Descripción |
|-------------------------------------|---|
| Common Name (CN) | Nombre y apellidos del firmante. |
| Given name (G) | Nombre del firmante tal y como aparece en el documento de identidad. |
| Surname | Apellidos del firmante tal y como aparece en el documento de identidad. |
| Email (E) | Correo electrónico del firmante. |
| Country (C) | Código de país de dos dígitos según ISO 3166-1. |
| Locality Name (L) | Ciudad del firmante. |
| State or Province (S) | Región, comunidad autónoma o provincia del firmante. |
| Organization name (O) | Nombre de la persona jurídica sobre la que el firmante tiene suficientes poderes de representación. |
| Organizational Unit (OU) | Certificado de Representante Legal para administradores únicos y solidarios (FIRMA) |
| Title (T) | Cargo o posición del firmante en la organización. |
| Organization identifier (OI) | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B0085974Z) |
| SerialNumber (SERIALNUMBER) | NIF, NIE o número de pasaporte del firmante. |

4.2. Extensiones

| Extensión | Descripción |
|---------------------------------|--|
| Certificate Policies | OID de Política de certificación de AN F AC correspondiente al certificado: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.2.5.1.9 (Software) • 1.3.6.1.4.1.18332.2.5.1.12 (QSCD) • 1.3.6.1.4.1.18332.2.5.1.13 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> • 0.4.0.194112.1.0 (QCP-n) • 0.4.0.194112.1.2 (QCP-n-qscd) |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Content Commitment |
| Extended Key Usage | clientAuth emailProtection |
| Subject Alternative Name | (Opcional) RFC822: email del firmante |
| 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 | OCSP - URI: CA Issuers - URI: |
| QCStatement | Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.1 |

5. Certificado de Representante Legal de Entidad sin Personalidad Jurídica

5.1. Sujeto

| Campo | Descripción |
|-------------------------------------|--|
| Common Name (CN) | Nombre y apellidos del firmante. |
| Given name (G) | Nombre del firmante tal y como aparece en el documento de identidad. |
| Surname | Apellidos del firmante tal y como aparece en el documento de identidad. |
| Email (E) | Correo electrónico del firmante. |
| Country (C) | Código de país de dos dígitos según ISO 3166-1. |
| Locality Name (L) | Ciudad del firmante. |
| State or Province (S) | Región, comunidad autónoma o provincia del firmante. |
| Organization name (O) | Nombre de la entidad sin personalidad jurídica sobre la que el firmante tiene suficientes poderes de representación. |
| Organizational Unit (OU) | Certificado de Representante Legal de Entidad sin personalidad jurídica (FIRMA) |
| Title (T) | Cargo o posición del firmante en la organización. |
| Organization identifier (OI) | NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B0085974Z) |
| SerialNumber (SERIALNUMBER) | NIF, NIE o número de pasaporte del firmante. |

5.2. Extensiones

| Extensión | Descripción |
|---------------------------------|--|
| Certificate Policies | OID de Política de certificación de AN F AC correspondiente al certificado: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.2.5.1.6 (Software) • 1.3.6.1.4.1.18332.2.5.1.11 (QSCD) • 1.3.6.1.4.1.18332.2.5.1.15 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> • 0.4.0.194112.1.0 (QCP-n) • 0.4.0.194112.1.2 (QCP-n-qscd) |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Content Commitment |
| Extended Key Usage | clientAuth emailProtection |
| Subject Alternative Name | (Opcional) RFC822: email del firmante |
| 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 | OCSP - URI: CA Issuers - URI: |
| QCStatement | Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.1 |

6. Certificado de Empleado Público

6.1. Sujeto

| Campo | Descripción |
|-----------------------------|--|
| Common Name (CN) | Nombre y apellidos del firmante. + “ - DNI “ + NIF del empleado público |
| Given name (G) | Nombre del firmante tal y como aparece en el documento de identidad. |
| Surname | Apellidos del firmante tal y como aparece en el documento de identidad. + “ - DNI “ + NIF del empleado público. |
| Email (E) | Correo electrónico del firmante. |
| Country (C) | Código de país de dos dígitos según ISO 3166-1. |
| Locality Name (L) | Ciudad del firmante. |
| State or Province (S) | Región, comunidad autónoma o provincia del firmante. |
| Organization name (O) | Denominación de la Administración, organismo o entidad de derecho público a la que se encuentra vinculada el empleado. |
| Organizational Unit (OU) | Certificado de Empleado Público (FIRMA) |
| Title (T) | Cargo o posición del firmante que le vincula con la Administración, organismo o entidad de derecho público. |
| SerialNumber (SERIALNUMBER) | NIF, NIE o número de pasaporte del firmante. |

6.2. Extensiones

| Extensión | Descripción |
|------------------------------|---|
| Certificate Policies | OID de Política de certificación de AN F AC correspondiente al certificado: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.4.1.1.22 (Autenticación nivel alto) • 1.3.6.1.4.1.18332.4.1.4.22 (Cifrado nivel alto) • 1.3.6.1.4.1.18332.4.1.3.22 (Firma nivel alto) • 1.3.6.1.4.1.18332.4.1.2.22 (Nivel medio) OID de Políticas de certificación europeas (no concurrencia): <ul style="list-style-type: none"> • 0.4.0.194112.1.0 (QCP-n) • 0.4.0.194112.1.2 (QCP-n-qscd) |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Content Commitment |
| Extended Key Usage | clientAuth emailProtection |
| Subject Alternative Name | (Opcional) RFC822: email del firmante |
| 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 | OCSP - URI: CA Issuers - URI: |

| | |
|--------------------|---|
| QCStatement | Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.1 |
|--------------------|---|