Perfiles de Certificados de Firma electrónica

de ANF AC

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

Teléfono: 902 902 172 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

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

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

Web: www.anf.es

ÍNDICE

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 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

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

Nombre del documento	Perfiles de Certificados de Firma electrónica de ANF AC		
Versión	1.5		
OID	1.3.6.1.4.1.18332.3.1.1		
Fecha de aprobación	07/08/2023	**Fecha de publicación**	07/08/2023

1.3.1. Revisiones

Versión	Cambios	Aprobación	Publicación
1.5	Aclaración sobre límites de uso de los certificados	07/08/2023	07/08/2023
1.4.	Revisión anual e inclusión de las extensiones propietarias 1.3.6.1.4.1.18332.19 and 1.3.6.1.4.1.18332.19.1	22/02/2023	22/02/2023
1.3.	Revisión anual e inclusión del certificado corporativo de persona física.	01/02/2022	01/02/2022
1.2.	Aclaración tamaño campos. Limite de RFC 5280 ampliado por EN 319 412-2.	30/11/2020	30/11/2020
1.1.	Introducción de OIDs propietarios en la extensión Subject Alternative Nave	01/07/2020	01/07/2020
1.0.	Unificación de los documentos • "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 Ténico" OID 1.3.6.1.4.1.18332.2.5.2 • "Certificados de Representante Legal de Entidad sin Personalidad Jurídica. Perfil Ténico" 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) *(opcional)*	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 Fisica (FIRMA)
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte[1] del firmante codificado según ETSI EN 319 412-1

2.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 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): • 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 • 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF del firmante

[1] Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud

3. Certificado Corporativo de Persona física

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) *(opcional)*	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 corporativo de Persona Física
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte [2] del firmante codificado según ETSI EN 319 412-1
Organization name (O)	Nombre de la persona jurídica con la que el firmante tiene relación laboral.
Organization identifier (OI)	NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000)

3.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.3.4.1.6.22 (Software) • 1.3.6.1.4.1.18332.3.4.1.7.22 (QSCD) • 1.3.6.1.4.1.18332.3.4.1.8.22 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): • 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 • 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.

[2] Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

	• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF 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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud

4. Certificados de Representante Legal de Persona Jurídica

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) *(opcional)*	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-B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte[3] del firmante.

4.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 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): • 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 • 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.

[3] Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

	• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF 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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud

5. Certificado de Representante Legal para administradores únicos y solidarios

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) *(opcional)*	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- B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte[4] del firmante.

5.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 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): • 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

[4] Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

	• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF 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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud

6. Certificado de Representante Legal de Entidad sin Personalidad Jurídica

6.1. 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) *(opcional)*	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- B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte[5] del firmante.

6.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de AN F AC correspondiente al certificado: • 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): • 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

[5] Con las limitaciones de uso consignadas en el apartado 3.1.1 de la DPC.

	• 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF 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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud

7. Certificado de Empleado Público

7.1. 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) *(opcional)*	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.

7.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 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): • 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 • 1.3.6.1.4.1.18332.10.1 Nombre de pila del firmante como aparece en el documento de identidad. • 1.3.6.1.4.1.18332.10.2 Primer apellido del firmante como aparece en el documento de identidad.

	• 1.3.6.1.4.1.18332.10.3 Segundo apellido del firmante como aparece en el documento de identidad (puede no estar presente). • 1.3.6.1.4.1.18332.10.4 DNI/NIE/NIF 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
1.3.6.1.4.1.18332.19	Localizador de la solicitud del certificado generado al momento de procederse a la identificación.
1.3.6.1.4.1.18332.19.1	Localizador del Operador OVP que tramitó la solicitud