Perfiles de Certificados

de ANF AC

Registro Nacional de Asociaciones. Número 171.443. CIF G-63287510.

© ANF Autoridad de Certificación

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

Teléfono: 932 661 614

www.anf.es

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 – 2026 CC-BY- ND (Creative commons licenses)

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

Teléfono: 932 661 614

www.anf.es

ÍNDICE

1. Introducción 5
1.1. Visión general 5
1.2. Aspectos comunes 5
1.3. Nombre del documento e identificación 5
2. Certificados de firma electrónica 7
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
3. Certificados de sello electrónico 18
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
4. Certificados de autenticación de sitio web SSL 23
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
5. Certificados de respondedor OCSP 30
5.1. Certificado de Respondedor OCSP 30
5.1.1. Sujeto 30
5.1.2. Extensiones 30
6. Certificados de TSU 31
6.1. Certificado de TSU 31
6.1.1. Sujeto 31
6.1.2. Extensiones 31

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

Nombre del documento	Perfiles de Certificados de ANF AC		
Versión	1.5		
OID	1.3.6.1.4.1.18332.3.1.1		
Fecha de aprobación	12/11/2026	**Fecha de publicación**	12/11/2026

1.3.1. Revisiones

Versión	Cambios	Aprobación	Publicación
1.5	Eliminación de los atributos organizationIdentifier (OI) y Organizational Unit (OU) del sujeto de los certificados de respondedor OCSP.	12/11/2026	12/11/2026
1.4	Actualización de las extensiones y base normativa del Certificado de Respondedor OCSP.	15/10/2026	15/10/2026
1.3	Provincia y Localidad opcional en todos los perfiles de firma y sello.	21/03/2025	21/03/2025

	Retirada de los perfiles de “Autenticación” y “Cifrado” de Empleado Público		
1.2	Revisión periodica. Mayor explicación en campo “Description” de los perfiles de Representación. 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 Respondedor OCSP	17/12/2024	17/12/2024
1.0.	Unificación de los documentos: • Perfiles de Certificados de Firma electrónica de ANF AC (OID 1.3.6.1.4.1.18332.3.1.1) – v.1.5 • Perfiles de Certificados de Sello electrónico de ANF AC (OID 1.3.6.1.4.1.18332.3.2.1) – v.2.4 • Perfiles de Certificados Autenticación de sitio Web SSL (OID 1.3.6.1.4.1.18332.3.3.1) – v.2.7. • Perfiles de Certificados OCSP de ANF AC (OID 1.3.6.1.4.1.18332.24.1) – v.1.0. • Perfiles de Certificados TSU de ANF AC (OID 1.3.6.1.4.1.18332.1.9.1.2.1) – v.1.2.	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
Common Name (CN)	Nombre, apellidos, guión (-) y DNI/NIE del firmante.
Given name (G)	Nombre del firmante tal y como aparece en el documento de identidad.
Surname (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del firmante.
Organizational Unit (OU)	Certificado de Clase 2 de Persona Fisica
SerialNumber (SERIALNUMBER)	NIF, NIE o número de pasaporte[1] del firmante codificado según ETSI EN 319 412-1

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

2.1.2. 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
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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
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

2.2. Certificado Corporativo de Persona física

2.2.1. Sujeto

Campo	Descripción
Common Name (CN)	Nombre, apellidos, guión (-) y DNI/NIE del firmante.
Given name (G)	Nombre del firmante tal y como aparece en el documento de identidad.
Surname (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del firmante.
Description (2.5.4.13)	Cargo 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)
Title (T)	Cargo, rol o posición del firmante en la organización.

2.2.1. 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.

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

	• 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 • 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial 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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
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

2.3. Certificados de Representante Legal de Persona Jurídica

2.3.1. Sujeto

Campo	Descripción
Common Name (CN)	DNI/NIE, Nombre y apellidos del firmante, seguido de (R: NIF de la entidad representada). Ejemplo: *00000000T NOMBRE APELLIDO APELLLIDO (R: A00000000)*
Given name (G)	Nombre del firmante tal y como aparece en el documento de identidad.
Surname (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	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

Title (T)	Cargo o posición del firmante en la organización.
Description (2.5.4.13)	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
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.
1.3.6.1.4.1.18838.1.1	DNI/NIE del firmante.

2.3.1. 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 según Secretaría SGIADSC de Persona Física representante de Persona Jurídica: 2.16.724.1.3.5.8 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 • 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial 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 (indica que es un certificado cualificado)

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

	• QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
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

2.4. Certificado de Representante Legal para administradores únicos y solidarios

2.4.1. 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 (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del firmante.
Description (2.5.4.13)	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
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
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.
1.3.6.1.4.1.18838.1.1	DNI/NIE del firmante.

2.4.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.2.5.1.9 (Software)

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

	• 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 según Secretaría SGIADSC de Persona Física representante de Persona Jurídica: 2.16.724.1.3.5.8 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 • 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial 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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
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

2.5. Certificado de Representante Legal de Entidad sin Personalidad Jurídica

2.5.1. 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 (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del firmante.
Description (2.5.4.13)	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
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
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.
1.3.6.1.4.1.18838.1.1	DNI/NIE del firmante.

2.5.2. 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 según Secretaría SGIADSC de Persona Física representante de Persona sin Entidad Jurídica: 2.16.724.1.3.5.9 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

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

	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 • 1.3.6.1.4.1.18332.1 Fecha de la identificación inicial 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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
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

2.6. Certificado de Empleado Público

2.6.1. 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 (SN)	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) *(opcional)*	Ciudad del firmante.
State or Province (S) *(opcional)*	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
Title (T)	Cargo o posición del firmante que le vincula con la Administración, organismo o entidad de derecho público.
SerialNumber (SERIALNUMBER)	NIF, NIE

2.6.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.4.1.3.22 (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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.1 (indica que es un certificado de firma electrónica) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)

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

3.1.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.25.1.1.1 (Software) • 1.3.6.1.4.1.18332.25.1.1.4 (QSCD) • 1.3.6.1.4.1.18332.25.1.1.9 (Centralizado) OID de Políticas de certificación europeas (no concurrencia): • 0.4.0.194112.1.1 (QCP-l) • 0.4.0.194112.1.3 (QCP-l-qscd)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Content Commitment* *Key Encipherment*
Extended Key Usage	clientAuth emailProtection
Subject Alternative Name	(Opcional) RFC822: email del contacto • 1.3.6.1. 4.1.18332.10.4 - NIF de la entidad
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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
1.3.6.1.4.1.18332.19	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
Common Name (CN)	Nombre comercial de la persona jurídica.
Email (E) *(opcional)*	Correo electrónico de contacto de la organización.
Country (C)	Código de país de dos dígitos según ISO 3166-1.
Locality Name (L) *(optional)*	Ciudad del suscriptor.

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

3.2.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.25.1.1.3 (Software) – nivel medio • 1.3.6.1.4.1.18332.25.1.1.12 (Dis.Claves) – nivel medio • 1.3.6.1.4.1.18332.25.1.1.2 (QSCD) – nivel alto • 1.3.6.1.4.1.18332.25.1.1.11 (Centralizado) – nivel alto OID de Políticas de certificación europeas (no concurrencia): • 0.4.0.194112.1.1 (QCP-l) • 0.4.0.194112.1.3 (QCP-l-qscd) OID según SGIADS: • 2.16.724.1.3.5.6.1 (nivel alto) • 2.16.724.1.3.5.6.2 (nivel medio)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Content Commitment* *Key Encipherment*
Extended Key Usage	clientAuth emailProtection
Subject Alternative Name	(Opcional) RFC822: email de contacto Directoryname: 2.16.724.1.3.5.6.2.1 = “SELLO ELECTRONICO DE NIVEL MEDIO” o “SELLO ELECTRONICO DE NIVEL ALTO” 2.16.724.1.3.5.6.1.2 = <O del DN> 2.16.724.1.3.5.6.1 .3 = <serialNumber del DN> (opcional) 2.16.724.1.3.5.6.1 .4 = <NIF/NIE del custodio> 2.16.724.1.3.5.6.1 .5 = <CN del DN> (opcional) 2.16.724.1.3.5.6.1 .6 = <Given name> (opcional) 2.16.724.1.3.5.6.1 .7 = <Primer apellido del custodio> (opcional) 2.16.724.1.3.5.6.1 .8 = <Segundo apellido del custodio> (opcional) 2.16.724.1.3.5.6.1 .9 = <correo electrónico del custodio>
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 (indica que es un certificado cualificado) • QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico) En caso de certificado en QSCD o centralizado, también: • QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un QSCD)
1.3.6.1.4.1.18332.19	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
Common Name (CN)	Nombre comercial de la persona jurídica.
Email (E) *(opcional)*	Correo electrónico de contacto de la organización.
Country (C)	Código de país de dos dígitos según ISO 3166-1.
Locality Name (L) *(opcional)*	Ciudad del suscriptor.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del suscriptor.
Organization name (O)	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).
Organizational Unit (OU) *(opcional)*	Certificado de Sello Electrónico PSD2
Organizational Unit (OU) *(opcional)*	Departamento o Unidad dentro de la organización.
Organization identifier (OI)	Número de autorización PSD2 de la organización, codificado según la especificación técnica ETSI TS 119 495
SerialNumber (SERIALNUMBER)	NIF de la entidad

3.3.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.25.1.1.5 (Software) OID de Políticas de certificación europeas (no concurrencia): • 0.4.0.194112.1.1 (QCP-l)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Content Commitment* *Key Encipherment*
Extended Key Usage	clientAuth

	emailProtection
Subject Alternative Name	(Opcional) RFC822: email del contacto 1.3.6.1. 4.1.18332.10.4 - NIF de la entidad
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 (indica que es un certificado cualificado)
	• QcType: 0.4.0.1862.1.6.2 (indica que es un certificado de sello electrónico)
	• PSD2QcStatement: 0.4.0.19495.2 incluyendo:
	  • RolPSD2:
	  ○ servicio de cuentas (PSP_AS);
	  ○ iniciación de pago (PSP_PI);
	  ○ información de la cuenta (PSP_AI);
	  ○ emisión de instrumentos de pago basados en tarjeta (PSP_IC).
	  • Nombre de la Autoridad Nacional Competente donde el PSP está registrado. Esta información se proporciona en dos formas: la cadena de nombre completo (*NCAName*) y un identificador único abreviado (*NCAId*).
	Conforme a ETSI TS 119 495 clausula 5.1.

1.3.6.1.4.1.18332.19	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
Organization name (O)	Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.
SerialNumber (SERIALNUMBER)	NIF de la Persona Jurídica
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L) *(opcional)*	Ciudad del suscriptor.

4.1.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.7.322 OID de CAB/Forum: • 2.23.140.1.2.2 (OVCP)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Key Encipherment*
Extended Key Usage	clientAuth 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) Access Location 1: http://ocsp.anf.es/spain/AV Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer

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) *(opcional)*	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L) *(opcional)*	Ciudad del suscriptor.
Business Category	· "Private Organization" · "Government Entity" · "Business Entity" · "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)

Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (no siempre está presente)

4.2.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.2.322 OID de Políticas de certificación europeas: • 0.4.0.194112.1.4 (Qcp-w) OID de CAB/Forum: • 2.23.140.1.1 (EVCP)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Key Encipherment*
Extended Key Usage	clientAuth 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) Access Location 1: http://ocsp.anf.es/spain/AV Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer
cabfOrganizationIdentifier	• 3 caracteres, identificador del esquema • Código de país de dos dígitos ISO 3166-1 • Identificador de la organización conforme al esquema
QCStatement	Mínimo: QcCompliance: 0.4.0.1862.1.1 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
Organization name (O)	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).
Organization identifier (OI)	Número de autorización PSD2 de la organización, codificado según la especificación técnica ETSI TS 119 495
SerialNumber (SERIALNUMBER)	NIF de la Persona Jurídica
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L) *(opcional)*	Ciudad del suscriptor.
Business Category	· "Private Organization" · "Government Entity" · "Business Entity" · "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)
Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (no siempre está presente)

4.3.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.8.22 OID de Políticas de certificación europeas: • 0.4.0.19495.3 (Qcp-w-psd2) • 0.4.0.194112.1.4 (Qcp-w) OID de CAB/Forum: • 2.23.140.1.1 (EVCP)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Key Encipherment*
Extended Key Usage	clientAuth 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) Access Location 1: http://ocsp.anf.es/spain/AV Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer
cabfOrganizationIdentifier	• 3 caracteres, identificador del esquema

	• Código de país de dos dígitos ISO 3166-1 • Identificador de la organización conforme al esquema
QCStatement	Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.3 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
Organizational unit (OU)	SEDE ELECTRONICA
Organizational unit (OU)	Nombre descriptivo de la sede
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)	El NIF de la entidad responsable
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S) *(opcional)*	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.
Business Category	"Government Entity"
Jurisdiction Of Incorporation Country Name	Subject Jurisdiction of Incorporation or Registration

4.4.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.6.322 OID según SGIADS: • 2.16.724.1.3.5.5.1 (Nivel alto) • 0.4.0.2042.1.4 (OID de SSL EV) OID de Políticas de certificación europeas: • 0.4.0.194112.1.4 (Qcp-w) OID de CAB/Forum: • 2.23.140.1.1 (EVCP)
Basic Constraints	CA:FALSE

Key Usage	*Digital Signature* *Key Encipherment*
Extended Key Usage	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) Access Location 1: http://ocsp.anf.es/spain/AV Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer
cabfOrganizationIdentifier	• 3 caracteres, identificador del esquema • Código de país de dos dígitos ISO 3166-1 • Identificador de la organización conforme al esquema
QCStatement	Mínimo: QcCompliance: 0.4.0.1862.1.1 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
Organizational unit (OU)	SEDE ELECTRONICA
Organizational unit (OU)	Descriptive name of the electronic headquarters
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) *(optional)*	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.
Business Category	"Government Entity"
Jurisdiction Of Incorporation Country Name	Subject Jurisdiction of Incorporation or Registration

4.5.2. Extensiones

Extensión	Descripción

Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.5.322 OID según SGIADS: • 2.16.724.1.3.5.5.2 (Nivel medio) OID de Políticas de certificación europeas: • 0.4.0.194112.1.4 (QEVCP-w) OID de CAB/Forum: • 2.23.140.1.1 (EVCP)
Basic Constraints	CA:FALSE
Key Usage	*Digital Signature* *Key Encipherment*
Extended Key Usage	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) Access Location 1: http://ocsp.anf.es/spain/AV Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://www.anf.es/es/certificates-download/ANFSecureServerCA.cer
cabfOrganizationIdentifier	• 3 caracteres, identificador del esquema • Código de país de dos dígitos ISO 3166-1 • Identificador de la organización conforme al esquema
QCStatement	Mínimo: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.3

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
- **Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates** publicado por CA/Browser Forum.

5.1. Certificado de Respondedor OCSP

5.1.1. Sujeto

Campo	Descripción
Common Name (CN)	Nombre CA + Responder + Nº
Organization name (O)	ANF Autoridad de Certificacion
Country (C)	Código de país de dos dígitos según ISO 3166-1. (ES)

5.1.2. Extensiones

Extensión	Descripción
Certificate Policies	No incluído
Basic Constraints	CA:FALSE
Key Usage	Digital Signature
Extended Key Usage	OCSPSigning
Subject Key Identifier	ID clave pública del certificado obtenido a partir del hash
Authority Key Identifier	keyIdentifier con el valor del campo subjectKeyIdentifier de la CA emisora
CRL Distribution Points	No incluído
Authority Information Access	No incluído
QCStatements	No incluído
id-pkix-ocsp-nocheck (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
Common Name (CN)	Identificador de TSU. Identifica de manera única la TSU correspondiente *(p.ej: ANF Timestamp Unit 1341)*
Country (C)	Código de país de dos dígitos según ISO 3166-1 en el que está establecida la TSA (ES).
Organization name (O)	ANF Autoridad de Certificacion
Organization Identifier (OI)	VATES-G63287510
Organizational Unit (OU) *(opcional)*	TSU

6.1.2. Extensiones

Extensión	Descripción
Certificate Policies	Policy:1.3.6.1.4.1.18332.15.1 CPS: https://www.anf.es/documentos
Basic Constraints	CA:FALSE
id-ceprivateKeyUsagePeriod 2.5.29.16 *(opcional)*	Limita la validez de la clave privada.

Key Usage	Digital Signature Non repudiation
Extended Key Usage	Time Stamping
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

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.