Perfiles de Certificados de Sello electrónico

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: 902 902 172 (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 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

Tal y como indica ETSI EN 319 412-3, el tamaño de los campos *commonName, organizationName y organizationUnitName* pueden ser más largos que el límite establecido en IETF RFC 5280.

Dentro de los certificados, además de los campos comunes ya estandarizados, se incluyen un conjunto de campos "propietarios" que aportan información relativa al suscriptor, u otra información de interés.

Se han asignado identificadores unívocos a nivel internacional. Concretamente:

- Los campos referenciados con el identificador de objeto (OID) 1.3.6.1.4.1.18332.x.x, son extensiones propietarias de ANF AC. 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 el ISO/IANA del MPR 2.16.724.1.3.5.x.x, son extensiones propietarias requeridas e identificadas en el Esquema de Identificación y Firma Electrónica v.1.7.6 publicado por el Consejo Superior de Administración Electrónica.
- Los campos con el OID 1.3.6.1.4.1.18838.1.1, son extensiones propietarias de la Agencia Estatal de Administración Tributaria (AEAT).

1.2. Nombre del documento e identificación

Nombre del documento	Perfiles de Certificados de Sello electrónico de ANF AC

Versión	2.1		
OID	1.3.6.1.4.1.18332.3.2.1		
Fecha de aprobación	30/11/2020	**Fecha de publicación**	30/11/2020

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
2.0.	Revisión anual	18/01/2020	18/01/2020
2.1.	Aclaración tamaño campos. Limite de RFC 5280 ampliado por EN 319 412-3.	30/11/2020	31/11/2020

2. Certificado de Sello electrónico *(QSealC)*

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)	Ciudad del suscriptor.
State or Province (S)	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)

2.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.25.1.1.1 (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) • 1.3.6.1.4.1.18332.25.1.1.10 (Distribución claves) 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 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: 0.4.0.1862.1.6.2

3. Certificados de Sello electrónico para Administración Pública *(QSealC APP)*

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)	Ciudad del suscriptor.
State or Province (S)	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. 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) • 1.3.6.1.4.1.18332.25.1.1.2 (QSCD) • 1.3.6.1.4.1.18332.25.1.1.11 (Centralizado) • 1.3.6.1.4.1.18332.25.1.1.12 (Distribución claves) 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 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: 0.4.0.1862.1.6.2 QcRetentionPeriod: 0.4.0.1862.1.6.3 Integer:=15 QcPDS: https://www.anf.es/documentos

4. Certificado de Sello electrónico para PSD2 *(QSealC PSD2)*

4.1. 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)	Ciudad del suscriptor.
State or Province (S)	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

4.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.25.1.1.5 (Software) • 1.3.6.1.4.1.18332.25.1.1.6 (QSCD) • 1.3.6.1.4.1.18332.25.1.1.7 (Centralizado) • 1.3.6.1.4.1.18332.25.1.1.8 (Distribución claves) 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 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: 0.4.0.1862.1.6.2
	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.