Perfiles de Certificados Autenticación de sitio Web SSL

de ANF AC

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

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

Este documento es propiedad de ANF Autoridad de Certificación

Está prohibida su reproducción y difusión sin autorización expresa de 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

1.1. Visión general

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

- **Certificados SSL Domain Validation** *(SSL DV)*
- **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

1.2. Nombre del documento e identificación

Nombre del documento	Perfiles de Certificados Autenticación de sitio Web SSL		
Versión	2.4		
OID	1.3.6.1.4.1.18332.3.3.1		
Fecha de aprobación	12/01/2021	**Fecha de publicación**	12/01/2021

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
2.4.	Revisión anual 2021	12/01/2021	12/01/2021
2.3.	Revisión anual 2020	18/01/2020	18/01/2020

2. Certificados SSL Domain Validation *(SSL DV)*

2.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro SSL DV

2.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.1.322 OID de CAB/Forum: • 2.23.140.1.2.1 (DVCP)
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

3. Certificados SSL Organization Validation *(SSL OV)*

3.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro SSL OV
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)	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.

3.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.7.322 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. Certificado SSL Validación Extendida *(EV)* – Certificado Cualificado de Autenticación de Sitio Web *(QWAC)*

4.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.
Organization identifier (OI)	NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF de la Persona Jurídica
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S)	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.
Business Category	· "Private Organization" · "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. 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: 0.4.0.1862.1.6.2

5. Certificado Cualificado de Autenticación de Sitio Web para PSD2 *(QWAC PSD2)*

5.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro QWAC PSD2
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)	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	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)

5.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.8.22 OID de Políticas de certificación europeas: • 0.4.0.19495.3 (Qcp-w-psd2) 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: 0.4.0.1862.1.6.2 PSD2QcStatement: 0.4.0.19495.2 incluyendo el RolPSD2, nCAName y nCAId.

6. Certificado Cualificado de Sede Electrónica con Validación Extendida *(EV)* Nivel alto

6.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.
Organization identifier (OI)	NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF de la Persona Jurídica
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S)	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.
Business Category	· "Private Organization" · "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)

6.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.6.322 OID según SGIADS: • 2.16.724.1.3.5.5.1 (Nivel alto) 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: 0.4.0.1862.1.6.2

7. Certificado Cualificado de Sede Electrónica con Validación Extendida *(EV)* Nivel medio

7.1. Sujeto

Campo	Descripción
Organizational Unit (OU) *(opcional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Denominación exacta de la persona jurídica según aparezca en el Registro mercantil.
Organization identifier (OI)	NIF, como figura en los registros oficiales, codificado según ETSI EN 319 412-1 (Ej: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF de la Persona Jurídica
Country (C)	Código de país de dos dígitos según ISO 3166-1.
State or Province (S)	Región, comunidad autónoma o provincia del suscriptor.
Locality Name (L)	Ciudad del suscriptor.
Business Category	· "Private Organization" · "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)

7.2. Extensiones

Extensión	Descripción
Certificate Policies	OID de Política de certificación de ANF AC correspondiente al certificado: • 1.3.6.1.4.1.18332.55.1.1.5.322 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 (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: 0.4.0.1862.1.6.2