SSL Website Authentication Certificate Profile

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

Security Level

Public Document

Important Notice

Address: Paseo de la Castellana, 79 - 28046 - Madrid (Spain)

Phone: 902 902 172 (calls from Spain) International (+34) 933 935 946

Website: www.anf.es

INDEX

1. Introduction

1.1. Overview

This document describes the profiles of the different types of SSL website authentication certificates issued by ANF Autoridad de Certificación:

- **SSL Domain Validation certificate** *(SSL DV)*
- **SSL Organization Validation certificate** *(SSL OV)*
- **SSL Extended Validation** *(EV)* **– Qualified Website Authentication certificate** *(QWAC)*
- **Qualified Website Authentication for PSD2** *(QWAC PSD2)*
- **Qualified Electronic Headquarters with Extended Validation** *(EV)* **High Level**
- **Qualified Electronic Headquarters with Extended Validation** *(EV)* **Medium Level**

The Certification Policies associated with these certificates are published and accessible at ANF ACs website: https://www.anf.es/repositorio-legal/

For the elaboration of these profiles, the following provisions have been taken into account:

- **Regulation (EU) 910/2014** of the european parliamente and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).
- **ETSI EN 319 412** Electronic Signatures and Infrastructures (ESI); Certificate Profiles (parts 1, 4 and 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 at https://cabforum.org/baseline-requirements-documents,
- **CA/B Forum Guidelines for Extended Validation** Certificates at 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. Document name and identification

Document name	Perfiles de Certificados Autenticación de sitio Web SSL		
Version	2.4		
OID	1.3.6.1.4.1.18332.3.3.1		
Approval Date	12/01/2021	**Fecha de publicación**	12/01/2021

1.2.1. Revisions

Version	Changes	Approval	Publication
2.4.	Annual review 2021	12/01/2021	12/01/2021
2.3.	Annual review 2020	18/01/2020	18/01/2020

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

2.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	Certificado de Servidor Seguro SSL DV

2.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 1.3.6.1.4.1.18332.55.1.1.1.322 CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash
CRL Distribution Points	CRL URI
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. SSL Organization Validation Certificates *(SSL OV)*

3.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	Certificado de Servidor Seguro SSL OV
Organization name (O)	Exact name of the legal person as it appears in the Registry.
SerialNumber (SERIALNUMBER)	NIF (identifier) of the Legal Person
Country (C)	Two-digit country code according to ISO 3166-1.
State or Province (S)	Region, autonomous community or province of the subscriber.
Locality Name (L)	Subscriber city.

3.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 1.3.6.1.4.1.18332.55.1.1.7.322 CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash
CRL Distribution Points	CRL URI
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. SSL Extended Validation *(EV)* – Qualified Website Authentication *(QWAC)* Certificate

4.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Exact name of the legal person as it appears in the Registry.
Organization identifier (OI)	NIF, as it appears in the official records, coded according to ETSI EN 319 412-1 (E.g: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF (identifier) of the Legal Person
Country (C)	Two-digit country code according to ISO 3166-1.
State or Province (S)	Region, autonomous community or province of the subscriber.
Locality Name (L)	Subscriber city.
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 (not always present)
Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (not always present)

4.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 1.3.6.1.4.1.18332.55.1.1.2.322 European Certification Policies OID: • 0.4.0.194112.1.4 (Qcp-w) CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash
CRL Distribution Points	CRL URI
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 character Registration Scheme identifier • 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated • Registration Reference allocated in accordance with the identified Registration Scheme
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2

5. Qualified Website Authentication for PSD2 Certificate *(QWAC PSD2)*

5.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	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 (identifier) of the Legal Person
Country (C)	Two-digit country code according to ISO 3166-1.
State or Province (S)	Region, autonomous community or province of the subscriber.
Locality Name (L)	Subscriber city.
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 (not always present)
Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (not always present)

5.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 1.3.6.1.4.1.18332.55.1.1.8.22 European Certification Policies OID: • 0.4.0.19495.3 (Qcp-w-psd2) CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash
CRL Distribution Points	CRL URI

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 character Registration Scheme identifier • 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated • Registration Reference allocated in accordance with the identified Registration Scheme
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2 PSD2QcStatement: 0.4.0.19495.2 including RolPSD2, nCAName and nCAId.

6. Qualified Electronic Headquarters with Extended Validation *(EV)* Certificate High level

6.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Exact name of the legal person as it appears in the Registry.
Organization identifier (OI)	NIF, as it appears in the official records, coded according to ETSI EN 319 412-1 (E.g: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF (identifier) of the Legal Person
Country (C)	Two-digit country code according to ISO 3166-1.
State or Province (S)	Region, autonomous community or province of the subscriber.
Locality Name (L)	Subscriber city.
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 (not always present)
Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (not always present)

6.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 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) European Certification Policies OID: • 0.4.0.194112.1.4 (Qcp-w) CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash

CRL Distribution Points	CRL URI
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 character Registration Scheme identifier • 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated • Registration Reference allocated in accordance with the identified Registration Scheme
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2

7. Qualified Electronic Headquarters with Extended Validation *(EV)* Certificete medium level

7.1. Subject

Field	Description
Organizational Unit (OU) *(optional)*	Certificado de Servidor Seguro SSL EV
Organization name (O)	Exact name of the legal person as it appears in the Registry.
Organization identifier (OI)	NIF, as it appears in the official records, coded according to ETSI EN 319 412-1 (E.g: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF (identifier) of the Legal Person
Country (C)	Two-digit country code according to ISO 3166-1.
State or Province (S)	Region, autonomous community or province of the subscriber.
Locality Name (L)	Subscriber city.
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 (not always present)
Jurisdiction Of Incorporation Locality Name	Subject Jurisdiction of Incorporation or Registration (not always present)

7.2. Extensions

Extension	Description
Certificate Policies	ANF AC Certification Policy OID corresponding to the certificate: • 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) European Certification Policies OID: • 0.4.0.194112.1.4 (Qcp-w) CAB/Forum OID: • 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 containing verified Fully-Qualified Domain Name (FQDN).
Subject Key Identifier	Public key ID of the certificate obtained from the hash
Authority Key Identifier	Public key ID of the CA certificate obtained from the hash

CRL Distribution Points	CRL URI
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 character Registration Scheme identifier • 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated • Registration Reference allocated in accordance with the identified Registration Scheme
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2