

Certificates for electronic seal Profiles de ANF AC



Security Level

Public Document

Important Notice

This document is the property of ANF Autoridad de Certificación

Reproduction and dissemination without the express authorization of ANF Autoridad de Certificación is prohibited.

2000 – 2021 CC-BY- ND (Creative commons licenses)

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

ÍNDIX

1. Introduction	4
1.1. Overview.....	4
1.2. Document name and identification.....	4
2. Certificates for Electronic Seal (<i>QSealC</i>)	6
2.1. Subject	6
2.2. Extensions.....	6
3. Certificates for Electronic Seal for Public Administration (<i>QSealC APP</i>)	7
3.1. Subject	7
3.2. Extensions.....	7
4. Certificates for Electronic Seal for PSD2 (<i>QSealC PSD2</i>)	9
4.1. Subject	9
4.2. Extensions.....	9

1. Introduction

1.1. Overview

This document sets out the profiles of the different types of qualified certificates for electronic signature issued by ANF Autoridad de Certificación:

- **Certificate for Electronic Seal** (*QSealC*)
- **Certificate for Electronic Seal for Public Administration** (*QSealC AAPP*)
- **Certificate for Electronic Seal for PSD2** (*QSealC PSD2*)

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

To prepare these profiles, the following provisions have been taken into account:

- **Regulation (EU) No 910/2014** of the european parliament 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 (all 5 parts)
- **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

As ETSI EN 319 412-2 indicates, the size of the *commonName*, *organizationName* and *organizationUnitName* fields can be longer than the limit established in IETF RFC 5280.

Within the certificates, besides the already standardized common fields, there are also included a group of "proprietary" fields which provide information in relation to the subscriber, or other information of interest.

Internationally unambiguous identifiers have been assigned. Specifically:

- Fields referenced with OID 1.3.6.1.4.1.18332.x.x are proprietary extensions of ANF AC. The complete list of OID codes and the information associated to the same may be consulted in the section "Proprietary fields of ANF AC" of the Certification Practice Statement of ANF AC.
- Fields with ISO/IANA of MPR 2.16.724.1.3.5.x.x, are proprietary extensions required and identified in the Identification and Electronic Signature Scheme v.1.7.6 published by the High Council of Electronic Administration.
- Fields with OID 1.3.6.1.4.1.18838.1.1 are proprietary of the Spanish State Tax Administration Agency (Agencia Estatal de Administración Tributaria "AEAT").

1.2. Document name and identification

Name of the document	Certificates for electronic seal Profiles
Version	2.1

OID	1.3.6.1.4.1.18332.3.2.1		
Approval date	30/11/2020	Publication date	30/11/2020

1.2.1. Revisions

Versions	Changes	Approval	Publication
2.0.	Revisión anual	18/01/2020	18/01/2020
2.1.	Clarification of fields size. Limit of RFC 5280 extended by EN 319 412-3.	30/11/2020	31/11/2020

2. Certificates for Electronic Seal (QSeal/C)

2.1. Subject

Campo	Descripción
Common Name (CN)	Commercial name of the legal person.
Email (E) <i>(optional)</i>	Organization contact email.
Country (C)	Two-digit country code according to ISO 3166-1.
Locality Name (L)	Subscriber's city.
State or Province (S)	Region, autonomous community or province of the subscriber.
Organization name (O)	Exact name of the legal entity as it appears in the Commercial Register.
Organizational Unit (OU) <i>(optional)</i>	Certificado de Sello Electrónico
Organizational Unit (OU) <i>(optional)</i>	Department or Unit within the organization.
Organization identifier (OI)	NIF, as it appears in official records, codified according to ETSI EN 319 412-1 (Ex: VATES-B00000000)

2.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: 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 (Centralised) 1.3.6.1.4.1.18332.25.1.1.10 (Key distribution) OID of European Certification Policies (only one): 0.4.0.194112.1.1 (QCP-I) 0.4.0.194112.1.3 (QCP-I-qscd)
Basic Constraints	CA:FALSE
Key Usage	<i>Digital Signature</i> <i>Content Commitment</i> <i>Key Encipherment</i>
Extended Key Usage	clientAuth emailProtection
Subject Alternative Name	(Optional) RFC822: email del firmante
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	URI of the CRL
Authority Information Access	OCSP - URI CA Issuers - URI
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2

3. Certificates for Electronic Seal for Public Administration (*QSealC APP*)

3.1. Subject

Campo	Descripción
Common Name (CN)	Commercial name of the legal person.
Email (E) <i>(optional)</i>	Organization contact email.
Country (C)	Two-digit country code according to ISO 3166-1.
Locality Name (L)	Subscriber's city.
State or Province (S)	Region, autonomous community or province of the subscriber.
Organization name (O)	Exact name of the legal entity as it appears in the Commercial Register.
Organizational Unit (OU) <i>(optional)</i>	Certificado de Sello Electrónico
Organizational Unit (OU) <i>(optional)</i>	Department or Unit within the organization.
Organization identifier (OI)	NIF, as it appears in official records, codified according to ETSI EN 319 412-1 (Ex: VATES-B00000000)

3.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: 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 (Centralised) 1.3.6.1.4.1.18332.25.1.1.12 (Key distribution) OID of European Certification Policies (only one): 0.4.0.194112.1.1 (QCP-I) 0.4.0.194112.1.3 (QCP-I-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	<i>Digital Signature</i> <i>Content Commitment</i> <i>Key Encipherment</i>
Extended Key Usage	clientAuth emailProtection
Subject Alternative Name	(Optional) RFC822: email del firmante
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	URI of the CRL
Authority Information Access	OCSP - URI: CA Issuers - URI:
QCStatement	Minimum: 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. Certificates for Electronic Seal for PSD2 (QSeal/ PSD2)

4.1. Subject

Campo	Descripción
Common Name (CN)	Commercial name of the legal person.
Email (E) <i>(optional)</i>	Organization contact email.
Country (C)	Two-digit country code according to ISO 3166-1.
Locality Name (L)	Subscriber's city.
State or Province (S)	Region, autonomous community or province of the subscriber.
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) <i>(optional)</i>	Certificado de Sello Electrónico PSD2
Organizational Unit (OU) <i>(optional)</i>	Department or Unit within the organization.
Organization identifier (OI)	Número de autorización PSD2 de la organización, codificado según la especificación técnica ETSI TS 119 495

4.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: 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 (Centralised) 1.3.6.1.4.1.18332.25.1.1.8 (Key distribution) OID of European Certification Policies (only one): 0.4.0.194112.1.1 (QCP-I) 0.4.0.194112.1.3 (QCP-I-qscd)
Basic Constraints	CA:FALSE
Key Usage	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	clientAuth emailProtection
Subject Alternative Name	(Optional) RFC822: email del firmante
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	URI of the CRL
Authority Information Access	OCSP - URI: CA Issuers - URI:
QCStatement	Minimum: QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2

	PSD2QcStatement: 0.4.0.19495.2 including: • RoIPSD2: ○ account service (PSP_AS); ○ initiation of payment (PSP_PI); ○ account information (PSP_AI); ○ issuance of card-based payment instruments (PSP_IC). • Name of the Competent National Authority where the PSP is registered. This information is provided in two forms: the full name string (<i>NCAName</i>) and an abbreviated unique identifier (<i>NCAId</i>). In accordance with ETSI TS 119 495 section 5.1.
--	--