

Certificates for electronic signature Profile

ANF AC



© ANF Autoridad de Certificación

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

Phone: 902 902 172 (Calls from Spain)

International +34 933 935 946

Website: www.anf.es

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 – 2022 CC-BY- ND (Creative commons licenses)

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

Phone: 932 661 614 (calls from Spain) International (+34) 933 935 946

Website: www.anf.es

ÍNDIX

1. Introduction	4
1.1. Overview.....	4
1.2. Common aspects	4
1.3. Document name and identification.....	5
2. Class 2 Natural Person certificate	6
2.1. Subject	6
2.2. Extensions.....	6
3. Corporate Natural Person certificate	8
3.1. Subject	8
3.2. Extensions.....	8
4. Legal Representative of Legal Person certificate	10
4.1. Subject	10
4.2. Extensions.....	10
5. Legal Representative for Sole and joint Directors certificate	12
5.1. Subject	12
5.2. Extensions.....	12
6. Legal Representative of Entity without Legal Personality certificate	14
6.1. Subject	14
6.2. Extensions.....	14
7. Public Employee Certificate	16
7.1. Subject	16
7.2. Extensions.....	16

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:

- **Natural Person certificate**
- **Corporate Natural Person Certificate**
- **Legal representative certificates**
 - Legal Representative of Legal Person certificate
 - Legal Representative for Sole and joint Directors certificate
 - Legal Representative of Entity without Legal Personality certificate
- **Public Employee certificate**

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)
- **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

1.2. Common aspects

All certificates issued under this policy are in accordance with X.509 Version 3 standard.

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

Within the certificates, besides the already standardized fields, there are also included a group of ANF AC OIDs (1.3.6.1.4.1.18332.x.x) which provide information in relation to the subscriber, or other information of interest. 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 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"). Fields with OID 2.16.724.1.3.5.x.x, are required and identified in the Identification and Electronic Signature Scheme v.1.7.6 published by the High Council of Electronic Administration.

All literals are entered in capital letters, with the exceptions of the email that will be in lowercase. No more than one space is entered between alphanumeric strings, or at the beginning or end of alphanumeric strings.

The inclusion of abbreviations based on a simplification is admitted, provided they do not difficult the interpretation of information.

1.3. Document name and identification

Name of the document	Certificates for electronic signature Profiles		
Version	1.3		
OID	1.3.6.1.4.1.18332.3.1.1		
Approval date	01/02/2022	Publication Date	01/02/2022

1.3.1. Revisions

Version	Changes	Approval	Publication
1.3.	Annual review and inclusion of the corporate natural person certificate.	01/02/2022	01/02/2022
1.2.	Clarification of fields size. Limit of RFC 5280 extended by EN 319 412-2.	30/11/2020	30/11/2020
1.1.	Introduction of proprietary OIDs in the Subject Alternative Nave extension	01/07/2020	01/07/2020
1.0.	Unification of the following documents <ul style="list-style-type: none"> • “Class 2 Natural Person certificate Profile“ OID 1.3.6.1.4.1.18332.3.4.1.2 • “Legal representative of Legal Person certificates Profile“ OID 1.3.6.1.4.1.18332.2.5.3 • “Legal Representative for Sole and Joint Directors certificates Profile“ OID 1.3.6.1.4.1.18332.2.5.2 • “Legal Representative for Entities without Legal personality certificate Profile“ OID 1.3.6.1.4.1.18332.2.5.4 • “Public employee certificates Profile“ OID 1.3.6.1.4.1.18332.4.1.2 	18/01/2020	18/01/2020

2. Class 2 Natural Person certificate

2.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber.
Given name (G)	Name of the subscriber as it appears on the identity document.
Surname	Surnames of the subscriber as it appears on the identity document.
Email (E) (opcional)	Subscriber's 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.
Organizational Unit (OU)	Certificado de Clase 2 de Persona Física (FIRMA)
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber coded according to ETSI EN 319 412-1.

2.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 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 (Centralised) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
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: 0.4.0.1862.1.6.1
--------------------	--

3. Corporate Natural Person certificate

3.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber.
Given name (G)	Name of the subscriber as it appears on the identity document.
Surname	Surnames of the subscriber as it appears on the identity document.
Email (E) (opcional)	Subscriber's 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.
Organizational Unit (OU)	Certificado corporativo de Persona Física
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber coded according to ETSI EN 319 412-1.
Organization name (O)	Name of the legal person with which the signatory has employment relationship.
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: <ul style="list-style-type: none"> 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 (Centralised) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
Subject Key Identifier	Public key ID of the certificate obtained from the hash

Certificates for electronic signature Profiles

OID 1.3.6.1.4.1.18332.3.1.1

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: 0.4.0.1862.1.6.1

4. Legal Representative of Legal Person certificate

4.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber.
Given name (G)	Name of the subscriber as it appears on the identity document
Surname	Surnames of the subscriber as it appears on the identity document.
Email (E) (opcional)	Subscriber's 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)	Name of the legal person over which the signatory has sufficient powers of representation.
Organizational Unit (OU)	Certificado de Representante Legal de Persona Juridica (FIRMA)
Title (T)	Position or position of the signatory in the organization.
Organization identifier (OI)	NIF, as it appears in official records, codified according to ETSI EN 319 412-1 (Ex: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber.

4.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 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 (Centralised) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
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: 0.4.0.1862.1.6.1

5. Legal Representative for Sole and joint Directors certificate

5.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber.
Given name (G)	Name of the subscriber as it appears on the identity document..
Surname	Surnames of the subscriber as it appears on the identity document.
Email (E) (opcional)	Subscriber's 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)	Name of the legal person over which the signatory has sufficient powers of representation.
Organizational Unit (OU)	Certificado de Representante Legal para administradores únicos y solidarios (FIRMA)
Title (T)	Position or position of the signatory in the organization.
Organization identifier (OI)	NIF, as it appears in official records, codified according to ETSI EN 319 412-1 (Ex: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber.

5.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.2.5.1.9 (Software) 1.3.6.1.4.1.18332.2.5.1.12 (QSCD) 1.3.6.1.4.1.18332.2.5.1.13 (Centralised) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
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: 0.4.0.1862.1.6.1

6. Legal Representative of Entity without Legal Personality certificate

6.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber.
Given name (G)	Name of the subscriber as it appears on the identity document.
Surname	Surnames of the subscriber as it appears on the identity document.
Email (E) (opcional)	Subscriber's 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)	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 (FIRMA)
Title (T)	Position or position of the signatory in the organization.
Organization identifier (OI)	NIF, as it appears in official records, codified according to ETSI EN 319 412-1 (Ex: VATES-B00000000)
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber.

6.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 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 (Centralised) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
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: 0.4.0.1862.1.6.1

7. Public Employee Certificate

7.1. Subject

Campo	Descripción
Common Name (CN)	Name and surname of the subscriber. + - DNI +NIF of public employee
Given name (G)	Name of the subscriber as it appears on the identity document..
Surname	Surnames of the subscriber. + - DNI +NIF of public employee
Email (E) (opcional)	Subscriber's 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)	Name of the Administration, body or entity of public law to which the employee is linked.
Organizational Unit (OU)	Certificado de Empleado Público (FIRMA)
Title (T)	Position or position of the signatory that link them to the Administration, body or entity of public law.
SerialNumber (SERIALNUMBER)	NIF, NIE or passport number of the subscriber.

7.2. Extensions

Extensión	Descripción
Certificate Policies	OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.4.1.1.22 (Autenticación nivel alto) 1.3.6.1.4.1.18332.4.1.4.22 (Cifrado nivel alto) 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 of European Certification Policies (only one): <ul style="list-style-type: none"> 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	(Optional) RFC822: email of the signatory <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.10.1 Name of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.2 First surname of the signer as it appears on the ID. 1.3.6.1.4.1.18332.10.3 Second surname of the signer as it appears on the ID. (may not be present) 1.3.6.1.4.1.18332.10.4 DNI/NIE of the signatory
Subject Key Identifier	Public key ID of the certificate obtained from the hash

Certificates for electronic signature Profiles

OID 1.3.6.1.4.1.18332.3.1.1

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: 0.4.0.1862.1.6.1