

Certificates Profiles

ANF AC



© ANF Autoridad de Certificación

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

Phone: 932 661 614 (Calls from Spain)

International +34 933 935 946

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 – 2025 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

www.anf.es

ÍNDIX

| | |
|---|-----------|
| 1. Introduction | 5 |
| 1.1. Overview..... | 5 |
| 1.2. Common aspects | 5 |
| 1.3. Document name and identification..... | 5 |
| 2. Certificates for electronic signature..... | 7 |
| 2.1. Class 2 Natural Person certificate..... | 7 |
| 2.1.1. Subject | 7 |
| 2.1.2. Extensions..... | 8 |
| 2.2. Corporate Natural Person certificate | 8 |
| 2.2.1. Subject | 8 |
| 2.2.2. Extensions..... | 9 |
| 2.3. Legal Representative of Legal Person certificate | 10 |
| 2.3.1. Subject | 10 |
| 2.3.2. Extensions..... | 10 |
| 2.4. Legal Representative for Sole and joint Directors certificate..... | 11 |
| 2.4.1. Subject | 11 |
| 2.4.2. Extensions..... | 11 |
| 2.5. Legal Representative of Entity without Legal Personality certificate..... | 12 |
| 2.5.1. Subject | 12 |
| 2.5.2. Extensions..... | 13 |
| 2.6. Public Employee Certificate..... | 14 |
| 2.6.1. Subject | 14 |
| 2.6.2. Extensions..... | 14 |
| 3. Certificates for electronic seal | 16 |
| 3.1. Certificates for Electronic Seal (<i>QSealC</i>)..... | 16 |
| 3.1.1. Subject | 16 |
| 3.1.2. Extensions..... | 17 |
| 3.2. Certificates for Electronic Seal for Public Administration (<i>QSealC APP</i>) | 17 |
| 3.2.1. Subject | 17 |
| 3.2.2. Extensions..... | 18 |

| | | |
|-----------|--|-----------|
| 3.3. | Certificates for Electronic Seal for PSD2 (<i>QSealC PSD2</i>)..... | 18 |
| 3.3.1. | Subject | 18 |
| 3.3.2. | Extensions..... | 19 |
| 4. | Certificates for website authentication SSL..... | 21 |
| 4.1. | SSL Organization Validation Certificates (<i>SSL OV</i>) | 21 |
| 4.1.1. | Subject | 21 |
| 4.1.2. | Extensions..... | 22 |
| 4.2. | SSL Extended Validation (<i>EV</i>) – Qualified Website Authentication (<i>QWAC</i>) Certificate | 22 |
| 4.2.1. | Subject | 22 |
| 4.2.2. | Extensions..... | 23 |
| 4.3. | Qualified Website Authentication for PSD2 Certificate (<i>QWAC PSD2</i>) | 23 |
| 4.3.1. | Subject | 23 |
| 4.3.2. | Extensions..... | 24 |
| 4.4. | Qualified Electronic Headquarters with Extended Validation (<i>EV</i>) Certificate High level..... | 25 |
| 4.4.1. | Subject | 25 |
| 4.4.2. | Extensions..... | 25 |
| 4.5. | Qualified Electronic Headquarters with Extended Validation (<i>EV</i>) Certificate medium level | 26 |
| 4.5.1. | Subject | 26 |
| 4.5.2. | Extensions..... | 26 |
| 5. | Certificates for OCSP Responder..... | 28 |
| 5.1. | OCSP Responder certificate..... | 28 |
| 5.1.1. | Subject | 28 |
| 5.1.2. | Extensions..... | 28 |
| 6. | Certificates for electronic seal | 29 |
| 6.1. | TSU certificate | 29 |
| 6.1.1. | Subject | 29 |
| 6.1.2. | Extensions..... | 29 |

1. Introduction

1.1. Overview

This document details the profiles of the certificates issued by ANF Certification Authority.

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 | Certificate Profiles | | |
| Version | 1.1 | | |
| OID | 1.3.6.1.4.1.18332.3.1.1 | | |
| Approval date | 17/12/2024 | Publication Date | 17/12/2024 |

1.3.1. Revisions

| Version | Changes | Approval | Publication |
|---------|---|------------|-------------|
| 1.1 | AIA extension removed from OCSP Responder certificates | 17/12/2024 | 17/12/2024 |
| 1.0 | Unification of the following documents: <ul style="list-style-type: none"> Certificates for electronic signature Profiles (OID 1.3.6.1.4.1.18332.3.1.1) – v.1.5. Certificates for electronic seal Profiles (OID 1.3.6.1.4.1.18332.3.2.1) – v.2.4. | 21/10/2024 | 21/10/2024 |

| | | | |
|--|---|--|--|
| | <ul style="list-style-type: none">• Certificates for website authentication SSL Profiles (OID 1.3.6.1.4.1.18332.3.3.1) – v.2.7.• OCSP Certificates Profile (OID 1.3.6.1.4.1.18332.24.1) – v.1.0.• TSU Certificate Profile (OID 1.3.6.1.4.1.18332.1.9.1.2.1) – v.1.0 | | |
|--|---|--|--|

2. Certificates for electronic signature

This section 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

2.1. Class 2 Natural Person certificate

2.1.1. 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 ¹ number of the subscriber coded according to ETSI EN 319 412-1. |

¹ With the limitations of use set forth in section 3.1.1 of the CPS.

2.1.2. 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
| 1.3.6.1.4.1.18332.19.1 | IVO Operator locator that processed the request |

2.2. Corporate Natural Person certificate

2.2.1. 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 corporativo de Persona Física |
| SerialNumber (SERIALNUMBER) | NIF, NIE or passport ² 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) |

2.2.2. Extensions

| Extensión | Descripción |
|-------------------------------------|--|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.3.4.1.6.22 (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 |
| 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |

² With the limitations of use set forth in section 3.1.1 of the CPS.

| | |
|------------------------|---|
| 1.3.6.1.4.1.18332.19.1 | IVO Operator locator that processed the request |
|------------------------|---|

2.3. Legal Representative of Legal Person certificate

2.3.1. 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. |
| 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 ³ number of the subscriber. |

2.3.2. Extensions

| Extensión | Descripción |
|---------------------------------|---|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.2.5.1.3 (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. |

³ With the limitations of use set forth in section 3.1.1 of the CPS.

| | |
|-------------------------------------|--|
| | <ul style="list-style-type: none"> 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
| 1.3.6.1.4.1.18332.19.1 | IVO Operator locator that processed the request |

2.4. Legal Representative for Sole and joint Directors certificate

2.4.1. 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 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 ⁴ number of the subscriber. |

2.4.2. Extensions

| Extensión | Descripción |
|-----------------------------|--|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.2.5.1.9 (Software) 1.3.6.1.4.1.18332.2.5.1.12 (QSCD) |

⁴ With the limitations of use set forth in section 3.1.1 of the CPS.

| | |
|-------------------------------------|--|
| | <ul style="list-style-type: none"> 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
| 1.3.6.1.4.1.18332.19.1 | IVO Operator locator that processed the request |

2.5. Legal Representative of Entity without Legal Personality certificate

2.5.1. 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) | 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 ⁵ number of the subscriber. |

2.5.2. Extensions

| Extensión | Descripción |
|-------------------------------------|---|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.2.5.1.6 (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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
| 1.3.6.1.4.1.18332.19.1 | IVO Operator locator that processed the request |

⁵ With the limitations of use set forth in section 3.1.1 of the CPS.

2.6. Public Employee Certificate

2.6.1. 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) <i>(opcional)</i> | 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. |

2.6.2. Extensions

| Extensión | Descripción |
|--------------------------|---|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.4.1.1.22 (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 |
| 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
| 1.3.6.1.4.1.18332.19.1 | I/O Operator locator that processed the request |

3. Certificates for electronic seal

This section 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

3.1. Certificates for Electronic Seal (*QSealC*)

3.1.1. 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) |

3.1.2. Extensions

| Extensión | Descripción |
|------------------------------|--|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.25.1.1.1 (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) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |

3.2. Certificates for Electronic Seal for Public Administration (QSealC APP)

3.2.1. Subject

| Campo | Descripción |
|-------------------------------------|---|
| Common Name (CN) | Commercial name of the legal person. |
| Email (E) (optional) | Organization contact email. |
| Country (C) | Two-digit country code according to ISO 3166-1. |
| Locality Name (L) (optional) | Subscriber's city. |
| State or Province (S) (optional) | 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) (optional) | Certificado de Sello Electrónico |
| Organizational Unit (OU) (optional) | 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) |

3.2.2. Extensions

| Extensión | Descripción |
|------------------------------|---|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.25.1.1.3 (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) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 0.4.0.194112.1.1 (QCP-I) 0.4.0.194112.1.3 (QCP-I-qscd) OID según SGIADS: <ul style="list-style-type: none"> 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 |
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |

3.3. Certificates for Electronic Seal for PSD2 (QSealC PSD2)

3.3.1. Subject

| Campo | Descripción |
|----------------------------------|--|
| Common Name (CN) | Commercial name of the legal person. |
| Email (E) (optional) | Organization contact email. |
| Country (C) | Two-digit country code according to ISO 3166-1. |
| Locality Name (L) (optional) | Subscriber's city. |
| State or Province (S) (optional) | 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 |

3.3.2. Extensions

| Extensión | Descripción |
|-------------------------------------|---|
| Certificate Policies | OID of ANF AC Certification Policy corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.25.1.1.5 (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) OID of European Certification Policies (only one): <ul style="list-style-type: none"> 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 PSD2QcStatement: 0.4.0.19495.2 including: <ul style="list-style-type: none"> RoIPSD2: <ul style="list-style-type: none"> 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>). <p>In accordance with ETSI TS 119 495 section 5.1.</p> |

| | |
|-----------------------------|---|
| 1.3.6.1.4.1.18332.19 | Locator of the certificate request generated at the time of identification. |
|-----------------------------|---|

4. Certificates for website authentication SSL

This section 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

4.1. SSL Organization Validation Certificates (SSL OV)

4.1.1. Subject

| Field | Description |
|------------------------------------|---|
| 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. |

4.1.2. Extensions

| Extension | Description |
|------------------------------|---|
| Certificate Policies | ANF AC Certification Policy OID corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.55.1.1.7.322 CAB/Forum OID: <ul style="list-style-type: none"> 2.23.140.1.2.2 (OVCP) |
| Basic Constraints | CA:FALSE |
| Key Usage | <i>Digital Signature</i> <i>Key Encipherment</i> |
| 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 |

4.2. SSL Extended Validation (EV) – Qualified Website Authentication (QWAC) Certificate

4.2.1. Subject

| Field | Description |
|--|---|
| 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) |

4.2.2. Extensions

| Extension | Description |
|-------------------------------------|---|
| Certificate Policies | ANF AC Certification Policy OID corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.55.1.1.2.322 European Certification Policies OID: <ul style="list-style-type: none"> 0.4.0.194112.1.4 (Qcp-w) CAB/Forum OID: <ul style="list-style-type: none"> 2.23.140.1.1 (EVCP) |
| Basic Constraints | CA:FALSE |
| Key Usage | <i>Digital Signature</i> <i>Key Encipherment</i> |
| 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 | <ul style="list-style-type: none"> 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: 0.4.0.1862.1.6.3 |

4.3. Qualified Website Authentication for PSD2 Certificate (QWAC PSD2)

4.3.1. Subject

| Field | Description |
|-------------------------------------|--|
| 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 | <ul style="list-style-type: none"> · "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) |

4.3.2. Extensions

| Extension | Description |
|-------------------------------------|---|
| Certificate Policies | ANF AC Certification Policy OID corresponding to the certificate: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.55.1.1.8.22 European Certification Policies OID: <ul style="list-style-type: none"> • 0.4.0.19495.3 (Qcp-w-psd2) CAB/Forum OID: <ul style="list-style-type: none"> • 2.23.140.1.1 (EVCP) |
| Basic Constraints | CA:FALSE |
| Key Usage | <i>Digital Signature</i> <i>Key Encipherment</i> |
| 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 | <ul style="list-style-type: none"> • 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: 0.4.0.1862.1.6.3 PSD2QcStatement: 0.4.0.19495.2 including RolPSD2, nCAName and nCAId. |

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

4.4.1. Subject

| Field | Description |
|--|---|
| Organizational unit (OU) | SEDE ELECTRONICA |
| Organizational unit (OU) | Descriptive name of the electronic headquarters |
| 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 responsible entity |
| 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 | "Government Entity" |
| Jurisdiction Of Incorporation Country Name | Subject Jurisdiction of Incorporation or Registration |

4.4.2. Extensions

| Extension | Description |
|------------------------------|---|
| Certificate Policies | ANF AC Certification Policy OID corresponding to the certificate: <ul style="list-style-type: none"> 1.3.6.1.4.1.18332.55.1.1.6.322 OID según SGIADS: <ul style="list-style-type: none"> 2.16.724.1.3.5.5.1 (Nivel alto) 0.4.0.2042.1.4 (OID de SSL EV) European Certification Policies OID: <ul style="list-style-type: none"> 0.4.0.194112.1.4 (Qcp-w) CAB/Forum OID: <ul style="list-style-type: none"> 2.23.140.1.1 (EVCP) |
| Basic Constraints | CA:FALSE |
| Key Usage | <i>Digital Signature</i> <i>Key Encipherment</i> |
| Extended Key Usage | 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 | <ul style="list-style-type: none"> 3 character Registration Scheme identifier |

| | |
|--------------------|---|
| | <ul style="list-style-type: none"> • 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: 0.4.0.1862.1.6.3 |

4.5. Qualified Electronic Headquarters with Extended Validation (EV) Certificate medium level

4.5.1. Subject

| Field | Description |
|---|---|
| Organizational unit (OU) | SEDE ELECTRONICA |
| Organizational unit (OU) | Descriptive name of the electronic headquarters |
| 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 | "Government Entity" |
| Jurisdiction Of Incorporation Country Name | Subject Jurisdiction of Incorporation or Registration |

4.5.2. Extensions

| Extension | Description |
|---------------------------------|--|
| Certificate Policies | ANF AC Certification Policy OID corresponding to the certificate: <ul style="list-style-type: none"> • 1.3.6.1.4.1.18332.55.1.1.5.322 OID según SGIADS: <ul style="list-style-type: none"> • 2.16.724.1.3.5.5.2 (Nivel medio) European Certification Policies OID: <ul style="list-style-type: none"> • 0.4.0.194112.1.4 (QEVPC-w) CAB/Forum OID: <ul style="list-style-type: none"> • 2.23.140.1.1 (EVCP) |
| Basic Constraints | CA:FALSE |
| Key Usage | <i>Digital Signature</i> <i>Key Encipherment</i> |
| Extended Key Usage | 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 | <ul style="list-style-type: none"> • 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: 0.4.0.1862.1.6.3 |

5. Certificates for OCSP Responder

This section presents the profile of the OCSP certificates of ANF Autoridad de Certificación.

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 319 412-1**. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- **IETF RFC 6960**. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

5.1. OCSP Responder certificate

5.1.1. Subject

| Campo | Descripción |
|---|--|
| Common Name (CN) | CA Name + "Responder" + N° |
| Organization name (O) | ANF Autoridad de Certificación |
| Organization Identifier (OI) | VATES-G63287510 |
| Organizational Unit (OU) <i>(opcional)</i> | ANF Autoridad Intermedia de Identidad |
| Country (C) | Two-digit country code according to ISO 3166-1 (ES). |

5.1.2. Extensions

| Extensión | Descripción |
|-------------------------------------|--|
| Certificate Policies | 1.3.6.1.4.1.18332.56.1.1 |
| Basic Constraints | CA:FALSE |
| Key Usage | Digital Signature Non repudiation |
| Extended Key Usage | OCSPSigning |
| Subject Key Identifier | Public key ID of the certificate obtained from the hash |
| Authority Key Identifier | Not included |
| CRL Distribution Points | URI de la CRL |
| Authority Information Access | OCSP - URI CA Issuers - URI |
| QCStatement | QcCompliance: 0.4.0.1862.1.1 QcType: 0.4.0.1862.1.6.2 QcRetentionPeriod: 0.4.0.1862.1.3 (15 años) QcPDS: 0.4.0.1862.1.5 (https://anf.es/en/) |

6. Certificates for electronic seal

This section presents the profile of the TSU certificates of ANF Autoridad de Certificación.

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 319 422** Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
- **ETSI EN 319 412-3**. "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"
- **IETF RFC 3739**. Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
- **IETF RFC 3161** Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

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.

6.1. TSU certificate

6.1.1. Subject

| Campo | Descripción |
|---|--|
| Common Name (CN) | TSU identifier. Uniquely identifies the corresponding TSU (<i>ex: ANF Timestamp Unit 1341</i>) |
| Country (C) | Two-digit country code according to ISO 3166-1 in which the TSA (ES) is established. |
| Locality Name (L) | City where the TSA is established |
| State or Province (S) | Region, autonomous community or province in which the TSA is established. |
| Organization name (O) | ANF Autoridad de Certificación |
| Organization Identifier (OI) | VATES-G63287510 |
| Organizational Unit (OU) (<i>opcional</i>) | TSU |

6.1.2. Extensions

| Extensión | Descripción |
|-----------------------------|---|
| Certificate Policies | Policy:1.3.6.1.4.1.18332.15.1 CPS: https://www.anf.es/documentos |
| Basic Constraints | CA:FALSE |

| | |
|-------------------------------------|--|
| Key Usage | Digital Signature Non repudiation |
| Extended Key Usage | Time Stamping |
| 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 de la CRL |
| Authority Information Access | OCSP - URI CA Issuers - URI |
| QCStatement | id_qcs_pkixQCSyntax_v2 id_etsi_tsts_EuQCompliance |