Certificate Policy

Certificates for electronic signature

Paseo de la Castellana, 79 - 28046 - Madrid (Spain)
Telephone: 902 902 172 (Calls from Spain)
International (+34) 933 935 946
Fax: (+34) 933 031 611 · Web: www.anf.es/en

Security Level

Public

Important Notice

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

Telephone: 902 902 172 (Calls from Spain) International (+34) 933 935 946

Web: www.anf.es/en

Index

1 Introduction

ANF Autoridad de Certificación (hereinafter, ANF AC) is a legal entity, incorporated under Spanish Organic Law 1/2002 of March 22nd, and registered in the Ministry of the Interior with national number 171.443 and VAT number G-63287510.

The Public Key Infrastructure (PKI) of ANF AC has been designed and is managed in accordance with the legal framework of the European Parliament [UE] 910/2014 Regulation, and with the Spanish Law 59/2003 on Electronic Signature of Spain. The PKI of ANF AC complies with ETSI EN 319 401 *(General Policy Requirements for Trust Service Providers),* ETSI EN 319 411-1 (*Part 1: General Requirements),* ETSI EN 319 411-2 (Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates), ETSI EN 319 412 *(Electronic Signatures and Infrastructures (ESI): Certificate Profiles)* and RFC 3739 (*Internet X.509 Public Key Infrastructure: Qualified Certificate Profile*) standards.

ANF AC uses OIDs in accordance with the ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (*Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs*) standards. ANF AC has been assigned the SMI Network Management Private Enterprise Code 18332 by the international organization IANA - Internet Assigned Numbers Authority - under the branch iso.org.dod.internet.private.enterprise (*1.3.6.1.4.1 -IANA –Registered Private Enterprise-*).

This document is the Certification Policy (CP) corresponding to the qualified certificates for electronic signature issued by ANF AC. These certificates are issued with the consideration of qualified in accordance with the provisions of 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 with consideration of recognized as defined in Spanish Law 59/2003 of electronic signature.

To develop its content the IETF RFC 3647 PKIX structure has been followed, including those sections that are specific to this type of certificate.

This document defines the operational and procedural requirements to which the usage of these certificates is subjected, and defines the guidelines that ANF AC uses for its issuance, management, revocation, renewal, and any other process that affects the life cycle. The roles, responsibilities, and relationships between the end user, ANF AC and trusted third parties are described, as well as the application, renewal and revocation rules that must be met.

This document is only one of the several documents governing the PKI of ANF AC, it details and supplements the definitions in the Certification Practice Statement and its addendum. ANF AC oversees and supervises that this CP is compatible and consistent with the other documents drafted. All documentation is freely available to users and relying parties at www.anf.es/en.

This Certification Policy assumes that the reader knows and understands the PKI, certificate, and electronic signature concepts. If this is not the case, the reader is recommended to be educated in these concepts before continuing the reading of this document.

1.1 Certificates description

These certificates are issued with a maximum validity of 5 years, in different supports and according to the security levels determined in the Commission Implementing Regulation (EU) 2015/1502 of the Commission of 8 September 2015 on setting specifications and minimum technical procedures for the security levels of electronic identification media in accordance with the provisions of Article 8, paragraph 3 of eIDAS Regulation:

- **Cryptographic software token.**
- **Cryptographic token (HSM)**. Devices exclusively certified specifically in accordance with the applicable requirements established in Article 30.3 of the eIDAS Regulation and, therefore, included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.
  https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
- **Centralized service of electronic signature certificates**. It uses only cryptographic Token (HSM).

The Natural Person certificate will be issued with different use modes:

- Authentication.
- Electronic Signature.
- Encryption.

Regarding their consideration, only the certificate "electronic signature" is issued by ANF AC with the consideration of "qualified". The certificate, to have this legal consideration, incorporates the extension of "qualified" as described in this document per the ETSI EN 319 412 standard. The qualified certificate of natural persons of centralized service of electronic signature, is issued in the modality of use Electronic Signature.

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

Identity verification will be done in person before a Registration Authority (RA), and based on original valid documentation. The RA is responsible for processing the application in accordance with the provisions stated in ANF AC's Certification Practice Statement. The person may waive appearance before the RA only in the cases expressly contemplated and authorized by law.

The verification of the information obtained by a Registration Authority, or any other provided by the subscriber, will be conducted by ANF AC, or collaborating entities classified for the purposes of this

document as Issuance Reports Managers (IRM), with which ANF AC subscribe the applicable legal document.

1.1.1. Natural Person Certificate

This is a certificate in which the subscriber will be a natural person. Links its holder to a signature verification data and confirms its identity.

In accordance to article 6 paragraph 2 of Spanish Law 59/2003, of December 19th, on Electronic Signature (per the Final Provision of Spanish Law 25/2015, of July 28th):

> "*the signer is the person who possess a signature creation device and acts on its own behalf or on behalf of a natural or legal person who he represents.*"

To identify the certificates, ANF AC has assigned the following object identifiers (OID).

Type	Certificate	Storage	OID
Natural Person Class 2	Authentication	Cryptographic software.	1.3.6.1.4.1.18332.3.4.1.1.22
	Encryption	Cryptographic software.	1.3.6.1.4.1.18332.3.4.1.3.22
	Signature	Cryptographic software.	1.3.6.1.4.1.18332.3.4.1.2.22
		QSCD	1.3.6.1.4.1.18332.3.4.1.4.22
		QSCD. Centralised service.	1.3.6.1.4.1.18332.3.4.1.5.22

1.1.2. Legal Representative Certificates

These certificates can offer a natural person representing a legal person the electronic signature tool with which to perform procedures on behalf of the represented legal person.

The certificate in addition to identifying the natural person representative as subscriber/signatory and attests his/her powers of attorney over the represented legal person, includes information on it, on whose behalf it acts.

ANF AC issues the following Legal Representative certificates:

- **Legal Representative of a Legal Person Certificate**
  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity. They are linked to a legal person, the Signatory acts on behalf of a legal person as a legal representative with powers of attorney.
- **Legal Representative of an Entity without Legal Personality Certificate**
  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity for the sole purpose of being used in the tax and other Public Administration fields that are expressly allowed. These certificates are issued under the terms set forth in the Order EHA/3256/2004, September 30, (Spanish Official Gazette Nº 246, October 12th).
  It is an entity without legal personality, the one to which article 35.4 of the Spanish General Tax Law and other applicable legislation refers to.

- **Legal Representative of Sole and Joint and Several Directors Certificate**
  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity. The Signatory acts in representation of a Legal Person as a legal representative with his position, as sole or joint and several directors, registered in the Mercantile Registry.

To identify the certificates, ANF AC has assigned the following object identifiers (OID):

Legal Representative of Legal Person	Authentication	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.1
	Encryption	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.2
	Signature	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.3
		QSCD	1.3.6.1.4.1.18332.2.5.1.10
		QSCD. Centralised service.	1.3.6.1.4.1.18332.2.5.1.14
Legal Representative of Entity without Legal Personality	Authentication	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.4
	Encryption	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.5
	Signature	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.6
		QSCD	1.3.6.1.4.1.18332.2.5.1.11
		QSCD. Centralised service.	1.3.6.1.4.1.18332.2.5.1.15
Legal Representative for Sole and Joint Directors	Authentication	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.7
	Encryption	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.8
	Signature	Cryptographic software.	1.3.6.1.4.1.18332.2.5.1.9
		QSCD	1.3.6.1.4.1.18332.2.5.1.12
		QSCD. Centralised service.	1.3.6.1.4.1.18332.2.5.1.13

1.1.3. Public Employee Certificates

This is a certificate in which the subscriber is a representative of a Public Administration with sufficient competences to solicit the certificate. and the subject, which is in possession of the signature creation device, is personnel from the Public Administration., being public servant, staff, or temporary personnel. The subject, by being in possession of the signature creation device, and acting as personnel of the Public Administration, adopts the obligations and responsibilities of the certificate responsible.

In accordance to article 6 section 2 of the Spanish Law 59/2003, of December 19th, on Electronic Signature (per the Final Provision of Spanish Law 25/2015, of July 28th):

> *"the signer is the person who possess a signature creation device and acts on its own behalf or on behalf of a natural or legal person who he represents."*

For the purposes of these types of certificates, only the president of the Governing Board of the PKI can intervene as the Issuance Reports Manager.

This policy, in terms of the certificates of the type "Public Employee", follows the definitions set by the Directorate of Information and Communications Technology in its document "Electronic certificates Profiles" of April 2016. The following assurance levels are defined:

a. **Medium level/Substantial:**

This level corresponds to a configuration of security mechanisms suitable for most applications. The expected risk for this level corresponds to the guarantee level 3 provided in the IDABC [1] Authentication Basic Policy. Is appropriate to access applications classified by ENS in the levels of Integrity and Authenticity as low or medium risk.

Likewise, the expected risk in this level corresponds to the low and substantial security levels of the electronic identification systems of the Regulation (EU) 910/2014. Safety levels of the eIDAS regulation apply only to electronic identification systems.

Minimum acceptable security mechanisms include X.509 software certificates. In the case of certificates issued to natural persons, it corresponds to a "qualified certificate", as defined in the Regulation (EU) 910/2014 for qualified electronic seal without a qualified signature creation device. The use of signature hardware devices (HSM or qualified signature creation device) is also permitted.

b. High level:

This level corresponds to a configuration of security mechanisms suitable for applications that require additional measures, per the risk analysis performed. The expected risk for this level corresponds to guarantee level 4 provided in IDABC Authentication Basic Policy. Is appropriate to access classified applications per the ENS in the levels of Integrity and Authenticity as high risk.

Likewise, the expected risk in this level corresponds to the high security level of electronic identification systems of the Regulation (EU) 910/2014. Safety levels of the eIDAS regulation apply only to the electronic identification systems.

Acceptable security mechanisms include X.509 certificates in hardware. In the case of certificates issued to natural persons, it corresponds with the "qualified certificate", as defined in the Regulation (EU) 910/2014. Furthermore, this type of certificates need to be stored in SSCD devices (HSM).

To identify the certificates, ANF AC has assigned the following object identifiers (OID):

Public Employees	Authentication High Level	HSM Token	1.3.6.1.4.1.18332.4.1.1.22
	Encryption High Level	HSM Token	1.3.6.1.4.1.18332.4.1.4.22
	Signature High Level	HSM Token	1.3.6.1.4.1.18332.4.1.3.22
	Medium Level	Cryptographic software.	1.3.6.1.4.1.18332.4.1.2.22

[1] *The IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business, and Citizens) program. Decision of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses, and citizens (IDABC) [Official Journal L 144 of 30 April 2004]*

1.2 Document name and identification

Name of the document	Certification Policy for Natural Person Class 2 Certificates		
Version	1.15		
Status	APROBADO		
OID	1.3.6.1.4.1.18332.3.4.1		
Approval date	20/03/2020	**Publication date**	20/03/2020

The identifier of this Certification Policy shall only be changed if substantial changes occur that affect its applicability.

Version	Changes	Approval	Publication
1.0.	New Certification Policy for Certificates for electronic signature that gathers the different previous policies that of each one of the certificates issued by ANF AC of this type. The previous Policies can be consulted in the policy history on the ANF AC website.	20/03/2020	20/03/2020

1.3 PKI Parties

As defined in the CPS of ANF AC.

1.4 Scope

1.4.1. Allowed usage

Generally, as defined in the CPS of ANF AC, and specifically:

- Certificates of the type " **AUTENTHICATION** ", specially indicated to: Authenticate before information systems and **computer** applications in general.
- Certificates of the type "**SIGNATURE** ", specially indicated to: Performing signature operations that require non-repudiation.
- Certificates of the type "**ENCRYPTION**", specially indicated to: Perform data encryption operations.
- Certificates of the type "**SIGNATURE** ", in centralized service of electronic signature, especially indicated for: Performing signature operations that require non-repudiation.

1.4.2. Limits of certificates uses

Generally, as set out in the Certification Practice Statement of ANF AC

Specifically, it must be stated that this certificate will be used by subscribers to maintain relationships with relying parties, per the uses permitted in the fields 'Key Usage' and 'Extended Key Usage' of the certificate,

the limitations of use set out in the certificate, and assuming the responsibility limitation established in OID 1.3.6.1.4.1.18332.41.1 and/or in QcLimitValue OID 0.4.0.1862.1.2.

Certificates issued under a pseudonym may only be used in those processes requiring signature or authentication that require, or expressly authorize the usage of this form of identification.

The subscriber may only use the key pair and certificate after accepting the conditions of use established in the CPS and its addendum.

1.4.3. Prohibited certificate uses

As defined in the CPS of ANF AC.

1.5. Certification Entity contact details

As defined in the CPS of ANF AC.

1.6. Definitions and acronyms

As defined in the CPS of ANF AC

2. Repositories and Publication of Information

2.1. Repositories

As defined in the CPS of ANF AC.

2.2. Publication of information

As defined in the CPS of ANF AC.

2.3. Updates frequency

As defined in the CPS of ANF AC.

2.4. Access controls on repositories

As defined in the CPS of ANF AC.

3. Identification and Authentication

3.1 Name registration

3.1.1 Types of names

ETSI has developed European standards in compliance with the European Commission Mandate M / 460 for the streamline of standards in the field of electronic signatures. The ETSI EN 319 412 family specifies the content of the certificates issued to natural persons.

Specifically, part 2 of this document, ETSI EN 319 412-2 (*Part 2: certificate profile for certificates issued to natural persons*) defines the content requirements of certificates issued to natural persons. The profile is based on IETF RFC 5280 recommendations and the ITU-T X.509 standard.

All certificates contain a Distinguished Name (DN) of the natural person holder of the certificate, defined per Recommendation ITUT X.501 and contained in the Subject field, including a Common Name (CN) component.

If it is a certificate issued with a pseudonym, the reference (PSEUDONYM) shall be included

Attribute O (Organization), in case of inclusion, needs to refer to the collegiate certification: Name of the Official College of which he/she is an active member. Moreover, the collegiate number is included, separated by the character "/". E.g. O = Collegiate Name / collegiate number.

In case of certificates of natural person legal representative of a legal person, the company name is included in the "organizationName" attribute and the VAT number in the "organizationIdentifier" attribute.

In the case of professional training: it may be included the name of the association, guild, or group to which he/she belongs. Or issuer of the professional training qualification. Additionally, it may be included the associate number as specified in the previous paragraph.

In the case of autonomous may include: registered trade name or registered trademark on behalf of the subscriber.

Personal circumstances and attributes of the persons and organizations identified in the certificates are included in predefined attributes in regulations and technical specifications for general recognition.

3.1.2 Specific fields completion guide

Per RFC 5280, which uses UTF-8*[1] string, since it encodes international character sets including Latin alphabet characters with diacritics (“Ñ”, “ñ”, “Ç”, “ç”, “Ü”, “ü “, etc.). For example, the character (ñ), is represented in Unicode as 0x00F1.

For all literal variables:

- All literals are entered in capital letters, with the exceptions of the domain name/subdomain and email that will be in lowercase.
- Do not include accent marks in the alphabetic literals
- Do not include more than one space between alphanumeric strings.
- Do not include blank characters 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 *For more information see RFC 2279 improved in 3629 (UTF-8, a transformation format of ISO 10646)*

National (DNI) / Foreign Citizens ID Card (NIE)

The term tax identification number covers both, the National Citizens ID Card, and the Foreign Citizens ID Card.
In case of opting on a specific ID card, instead of the tax identification number, the corresponding ID card will be used.

The following coding is allowed:

1.- Semantics proposed by the ETSI EN 319 412-1 standard. Consisting in:

- Three characters to indicate the type of document per the following coding:

- "PAS" for identification based on passport number.
- "IDC" for identification based on the ID card (DNI/NIE).
- "PNO" for identification based on () national personal number (number of national civic register).
- "TAX" for identification based on a personal tax identification number issued by a national tax authority. This value is in disuse. The value "ID number" should be used instead. Tax Identification Number "TIN" per the European Commission - Taxation and Customs Union, specification published in:
  (Https://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

- Two characters to identify the country. Encoded in accordance with "ISO 3166-1- alpha-2 code elements".

- Identity number with tax identification letter.

e.g.: IDCES-00000000G.

2.- Basic semantics. Consisting in:

The number and letter as stated in the ID card.

e.g.: ID00000000G.

3.1.3 Need for names to be meaningful

Distinguished names should make sense, except in the case of certificates issued under pseudonyms.

3.1.4 Anonymous or pseudonyms

In the case of certificates issued under a pseudonym, the CN attribute shall specify the concept "Pseudonym".

3.1.5 Rules for interpreting various name forms

As defined in the CPS of ANF AC.

3.1.6 Uniqueness of names

As defined in the CPS of ANF AC.

3.1.7 Resolution of conflicts in relation to names and trademarks

ANF AC is not liable for the use of trademarks in the issuance of Certificates issued under this Certification Policy. ANF AC is not required to verify ownership or registration of trademarks and other distinctive signs.

Certificate subscribers shall not include names in applications that may involve infringement.

It is not allowed to use distinctive signs whose right of usage is not owned by the subscriber, or is not duly authorized to do so.

ANF AC reserves the right to refuse a certificate request because of name conflict.

3.2 Identity initial validation

3.2.1 Private key possession test

As defined in the CPS of ANF AC.

3.2.2 Subscriber identity authentication

Certificates issued under this Certification Policy will identify the subject under whose name the certificate is issued and the certificate subscriber.

In the case of pseudonym certificates, ANF AC will verify his/her identity and will retain documentation that accredits it.

The Issuance Reports Manager shall use appropriate means to ensure the accuracy of the information contained in the certificate. Among these means it is included external registry databases and the ability to require information or documents to the subscriber.

The tax identification of the subject and subscriber will be incorporated into the certificate. Furthermore, the subscriber must provide a mobile phone number and an email address of his trust. The email address and the SMS or WhatsApp service associated with their mobile phone shall be considered as authorized mailboxes for ANF AC to be able to deliver certified electronic mail, including double authentication in the case of a centralized electronic signature service, or any other as deemed necessary. The user assumes the obligation to inform ANF AC of any change of e-mail address or mobile phone number.

In accordance with art. 13.3 of Spanish Law 59/2003 on Electronic Signature, when the qualified certificate contains other personal circumstances or attributes of the subscriber, such as its status as holder of a public office or membership of a professional association or qualification, this must be verified with official documents that prove it, in accordance with the applicable legislation. Likewise, when the subscriber wants to include a representative capacity which has been granted by a third party, either by mandate or powers of attorney, the subscriber shall prove such condition with the original document.

The documentation type, processing forms, authentication and validation procedures are specified in this document.

3.3 Re-key requests

In the event of re-keying, ANF AC shall previously inform the subscriber about any changes that may have occurred in the terms and conditions in relation to the previous issuance.

A new certificate may be issued maintaining the previous public key, if it is considered cryptographically secure.

3.4 Revocation requests

All revocation requests must be authenticated. ANF AC verifies the subscriber's ability to handle this requirement.

4 Operational Requirements

4.1 Interoperability National Scheme and Security National Scheme.

4.1.1 Operation and management of Public Key Infrastructure

Operations and procedures performed for the implementation of this Certification Policy are made following the controls required by the standards recognized for such purpose, describing these actions in sections "Physical Security, Facilities, Management and Operational Controls" and "Technical Security Controls" of the Certification Practice Statement of ANF AC.

The Certification Practice Statement of ANF AC, responds to different sections of the ETSI EN 319 411-2 standard.

4.1.2 Interoperability

The certificates corresponding to this Certification Policy are issued by ANF AC in accordance with Resolution of November 29th, 2012, of the Secretariat of State for Public Administration, by which the Approval Agreement of the Electronic Signature Policy and of General State Administration Certificates is published, and its publication is announced in the corresponding electronic office, and specifically the profile of this type of certificates is in accordance with the profile approved by the Higher Council for Electronic Administration, at a meeting of the Permanent Commission, on May 30th, 2012 and published in Annex II of the mentioned Resolution

4.2 Certificate application

ANF AC only accepts certificate issuance requests processed by natural persons of legal age, with full legal capacity to act.

The subscriber must complete the Application Form of the certificate undertaking responsibility for the accuracy of the information provided, and submitting it to ANF AC using any of the following means:

a) **In person**: the subscriber may appear before a Recognized Registration Authority, in whose presence will proceed to sign the application form, which shall be dully fill out.

b) **By ordinary mail**: certificate request form handwritten signed by the subscriber and his/her signature legitimized by public notary. Documentation sent by ordinary mail.

4.3 Procedure processing

4.3.1 Identity authentication

4.3.1.1 Processing in the RRA or IVO

When the processing is carried out in person at the office of a Recognized Registration Authority (ARR) or an Identity Verification Office (IVO), the subscriber must prove their identity and personal affiliation data through legally sufficient documentation. At a minimum, the following will be credited:

a) Physical address and other contact details of the subscriber. If deemed necessary by the Registration Authority or the Issuance Reports Manager, additional documents may be solicited to verify the reliability of the information, such as recent utility bills or bank statements. In case the RRA or the IRM know the subscriber personally, they shall issue and sign a Declaration of Identity[2].

b) Accreditation of the face-to-face act in order to make the repudiation of the procedure carried out impossible, for which one or several evidences will be obtained that will be associated with the application form, e.g. handwritten signature, graphic metric photograph, or video signature, or voice, or fingerprints.

c) ID card or passport in case of national citizens, whose photograph allows verifying the identity of the person appearing. In case of low sharpness of the picture, another official document with a better quality picture may be requested (e.g. driver's license).

d) In case of foreign citizens, the following will be required:

I. To European Union members or European Economic Area members:

- National ID Card (or local equivalent), or Foreign ID Card (issued by the Registry of Citizen Members of the Union), or passport. The physical identification must be performed using as a reference one of these documents which includes a photograph of the person appearing before them. In case of low sharpness of the picture, another official document with a better quality picture may be requested (e.g. driver's license).
- Certificate issued by the Registry of Citizens of Members of the European Union.

[2] **Declaration of Identity.** *It consists of a formal declaration under oath, in which the declarant states he/she personally and directly knows a natural person or a legal entity. Besides, it states, up to their direct knowledge, that he/she has verified that the filiation data outlined in the Application Form is true: the address, telephone, and e-mail.*

The Declaration of Identity incorporates the identity of the declarant, his/her ID card number, the data verified, the date and time of verification, the signature of the declarant and the appropriate legal warnings in case of lying under oath.

II. To non-EU citizens:

- Passport, residence permit or work permit with photograph that allows comparing the identity of the person appearing. In case of low sharpness of the picture, another official document with a better quality picture may be requested (e.g. driver's license).

e) In case the subscriber has a representation mandate or powers of attorney, and request that the document be attached to the certificate. It will be required to:

1. **Representation mandate**. The document must be in pdf format and signed by the client, using a qualified certificate for electronic signature issued by ANF AC. The request for inclusion of the mandate presupposes for the subscriber the full acceptance of the representation mandate.
2. **Powers of attorney**. The original document will be digitized by the RA operator who will sign it electronically.

f) The subscriber who processes the certificate application, must submit original or certified copies of the following valid documents:

1. **Regarding the legal form**:
   - Corporations and other legal entities which registration is compulsory in the Mercantile Registry, shall attest their valid incorporation by providing the authentic copy, the deed of incorporation registered in the Mercantile Registry, or certification issued by the Mercantile Registry.
     To prove the representation:
     - in the case of Administrators or the Board of Directors, an authentic copy of the deed of appointment registered in the Mercantile Registry or certification of the appointment issued by the Mercantile Registry,
     - in the case of Representatives, authentic copy of the power of attorney.
   - Associations, Foundations, and Cooperatives shall attest their valid incorporation by providing original or certified copy of a public record certificate detailing the registration of their incorporation.
   - Civil societies and other legal entities shall provide an original or certified copy of the document attesting their incorporation in an irrefutable manner.
   - Public Administrations and entities belonging to the public sector:
     - Entities whose registration is mandatory in a Registry attest their valid incorporation by providing original or certified copy of a certificate in relation to the incorporation data and their legal personality.
     - Entities incorporated in accordance to a regulation, shall provide reference to such regulation.

2. **Document certifying the valid incorporation of the entity:**
   Certificates or certified copies evidencing registration, issued on the date of the application or on the preceding 15 days, specifically:

- In the case of investments funds, venture capital funds, mortgage securities market regulation funds, mortgage qualifications funds, assets titling funds, investment guarantee funds and pension funds: certificate of registration in the corresponding registry the Ministry of Finance or the National Securities Market Commission, the identification of the management body must be recorded in the certificate.
- In the case of joint ventures that have benefited from the special tax regime, and if they were registered in the special register of joint ventures by the Ministry of Economy and Finance, attached to the State Tax Administration Agency, shall provide certificate of such registration. In case they are not registered, a document signed by a majority of members or partners, confirming the validity of the entity.
- When the entity does not correspond to any of the types outlined above and, therefore, does not need to be registered in any Registry, it shall be submitted alongside the application, all documents the subscriber deems as valid, being the IRM the responsible to determine the sufficiency or insufficiency thereof.

g) If the subscriber requests to include other personal circumstances such as his status as holder of a public office, his membership of a professional association or his degree, these must be verified through the official documents that accredit them, in accordance with its specific regulation.

In case of intervention of a public notary, the authentication of the signature of the subscriber shall be required in order to issue a certificate (LFE 59/2003, Art. 13.1).

4.3.1.2 Processing in the RRA or IVO

The following procedure will be highlighted:

a) ANF AC makes available to the subscriber the certification policies, prices and the application form and the contract for the provision of certification services, as well as the technical means to carry out the application process: fill out the application form and provide supporting documents and identity and personal affiliation.
b) The documents required for accreditation will be the same as those required in the procedure before ARR and IVO.
c) The subscriber, if applicable, stamps their handwritten signature or graphometric (biometric) signature on the documents corresponding to the certificate application process.
d) Once this process is completed, ANF AC makes available to the subscriber the technical means necessary to carry out the generation of its key pair, selection of PIN (signature activation data), and generation of the request certificate (CSR under standard PKCS #10).

e) The signature of the application form and the service provision contract will be legitimized by knowledge of the signature by a notary public or certified by an IVO or ARR operator".

4.3.2 Approval or rejection of certificate applications

The Issuance Reports Manager (IRM) assumes the final response assumes the ultimate responsibility to verify the information contained in the Application Form, and to assess the adequacy of the documents provided and of the application, in accordance with the provisions of this Certification Policy.

Moreover, he/she will determine:

- That the subscriber has access to the terms and conditions relating to the use of the certificate, as well as to the issuance fees.
- That the subscriber has had access and has permanent access to all documents relating to the obligations and responsibilities of the CA, the subscriber, subject, certificate responsible and relying parties, especially to the CPS and Certification Policies.
- Shall monitor compliance with any requirement imposed by the legislation on data protection, as established in the security document included in the CPS, per article 19.3 of Spanish Law 59/2003, of December 19th, on Electronic Signature.

The process of issuing the certificate shall not begin if the Issuance Reports Manager has not issued the corresponding compliance report. The maximum period established for issuing the report is 15 days. After that period without issuing the mandatory report, the subscriber may immediately cancel the order and be reimbursed of the fees paid.

The IRM may require additional information or documentation from the subscriber, which will have 15 days to deliver it. After this period, without having completed the requirement, the IRM will issue a report denying the issuance. Should the subscriber meet the requirement, the IRM will have 7 days to issue the final report.

In case the IRM verifies that the information provided by the subscriber is not true, he/she will deny the issuance of the certificate, and will generate an incident report to the Security Manager, to determine whether to include the subscriber in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18332.56.2.1.

The validation procedure to be followed, depending on the type of certificate, is the following:

- The IRM shall verify the documentation provided by the subscriber and the Registration Authority.
- The validation process will be supported by the Legal and Technical Departments, which will review and technically validate the PKCS#10 certificate request.
- In the process of verification of the information and documentation received, the following means may be used:

- Consultation of official public registries in which the entity must be registered to verify existence valid management positions and other legal aspects such as activity and date of incorporation.
- National or regional Official Gazettes of public bodies to which public bodies or companies belong to.

- It is verified that none of the natural or legal persons associated with the request appear in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18332.56.2.1.

4.3.3 Time to process certificate issuance

The issuance of a certificate means the complete and final approval of an application by the Issuance Reports Manager. The issuance of certificate must be made within 48 hours, once issued the report of the IRM, as defined in the CPS of ANF AC.

4.4 Certificate issuance

As defined in the CPS of ANF AC. ANF AC will avoid generating certificates that expire after the CA's certificates that issued them.

4.4.1 Certification Entity actions during issuance process

As defined in the CPS of ANF AC.

Once the electronic certificate is issued, the certificate delivery is always done electronically. The same cryptographic device that the subscriber or his legal representative used to generate the cryptographic key pair and the PKCS#10 request certificate must be used.

The cryptographic device establishes secure connection to ANF AC trusted servers. The system automatically performs the appropriate security verifications, and in case of validation the certificate is automatically downloaded and installed.

4.4.2 Notification to subscriber

ANF AC notifies the subscriber via e-mail, the certificate issuance and publication.

4.5 Certificate acceptance

4.5.1 Acceptance

As established in the ANF AC CPS.

4.5.2 Return

The subscriber has a period of 7 days, from the delivery of the certificate, to verify its correct functioning.

In case of malfunction, or due to technical errors in the data contained in the certificate, the subscriber, or the certificate responsible can send an electronically signed e-mail to ANF AC, reporting the reason for the return.

ANF AC shall verify the causes for return, revoke the certificate issued and issue a new certificate within 72 hours.

4.5.3 Monitoring

ANF AC is not responsible for the monitoring, investigation, or confirmation of the accuracy of the information contained in the certificate after issuance. For information on the inaccuracy or no current applicability of the information contained in the certificate, it can be revoked.

4.5.4 Certificate Publication

The certificate is published in the repositories of ANF AC within a maximum period of 24 hours since its emission has occurred.

4.5.5 Notification of certificate issuance to third parties

No notification is made to third parties.

4.6 Rejection

As defined in the CPS of ANF AC.

4.7 Certificate renewal

Generally, as defined in the CPS of ANF AC.

4.7.1 Valid certificates

ANF AC notifies the subscriber the expiration of the certificate expiration via email, forwarding the application form to proceed with its renovation. These notifications are sent 90, 30 and 15 days prior to the expiration date of the certificate.

Only valid certificates can be renewed, provided that the identification made has not exceeded the period of five years.

4.7.2 Persons authorized to apply for the renewal

The renewal application form must be signed by the subscriber, or by the legal representative with enough powers of attorney. The personal circumstances of the subscriber should not have changed

4.7.3 Routine renewal requests authentication and identification

Identification and authentication for certificate renewal can be done in person using one of the methods described in this section, or processed electronically by completing the corresponding form and signing it with a valid certificate electronically issued as "qualified", and stating as holder the certificate subscriber of which renewal is requested.

In accordance with article 13.4 b) of Spanish Law 59/2003, December 19th, on Electronic Signature, certificate renewal by electronically signed applications requires that less than five years have passed since the personal identification took place.

To ensure compliance with art. 13.4. b) of the Electronic Signature Law and to not exceed the period of 5 years from the initial identification, ANF AC applies the following procedures and technical security measures:

- Certificates of ANF AC shall be always generated using a token that must be used to perform any renewal process, including the electronic certificates of centralized electronic signature.

- ANF AC follows a system of registration of applications, distinguishing date of request, -which coincides with the identification - and of issuance of the certificate. This control allows a second renewal if the period of 5 years has not been reached since the initial identification. The technical system requires a specific request of the user, the direct intervention of an ANF AC operator, which in turn, requires validating the application by applying coherent security verification. If 5 years have exceeded, the application itself blocks the process, otherwise facilitates the operator the process until the certificate renewal.

  Renewal of certificates that have exceeded 5 years from the initial identification. The formalization of the application is done with the handwritten signature of the subscriber, done in-situ by the interested party, or by authentication performed before a public notary and using

sufficient original documentation. The procedures with physical personification may be carried out before:

- **Recognized Registration Authority** which, per the definition of the CPS of ANF AC, are the natural or legal persons to whom ANF AC has equipped with the necessary technology to perform the functions of a registry entity, having formalized the corresponding liability assumption and collaboration agreement.

- **Collaborating Registration Authority** which, per the definition of the CPS of ANF AC, are persons who, in accordance to current legislation, have powers of public notary.

- **Trust Entities** which, per the definition of the CPS of ANF CP, are entities that have the necessary capacity to determine the identity, capacity, and freedom of action of the subscribers.

4.7.4 Approval or rejection of applications for renewal

Same procedure as that performed in the issuance process specified herein.

4.7.5 Notification of certificate renewal

Same procedure as that performed in the issuance process specified herein.

4.7.6 Acceptance of certificate renewal

Same procedure as that performed in the issuance process specified herein.

4.7.7 Publication of the renewal certificate

Same procedure as that performed in the issuance process specified herein.

4.7.8 Notification to third entities

As specified in section 4.4.5 "Notification of certificate issuance to third parties."

4.7.9 Identification and authentication of key renewal applications after revocation (uncommitted key)

The renewal of expired or revoked certificates is not authorized.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

Generally, as defined in the CPS of ANF AC.

4.9.1 Circumstances for revocation

Besides those defined in the CPS, ANF AC shall:

- Provide instructions and legal support for reporting complaints or suspicions regarding the compromise of the private key, of certificate misuse or about any type of fraud or misconduct.
- ANF AC shall investigate incidents of which they become aware within twenty-four hours from their receipt. The Security Manager, based on inquiries and verifications, shall issue a report to the Issuance Reports Manager, whom shall determine, if appropriate, the corresponding revocation in a substantiated minute, which shall include:
  - Nature of the incident.
  - Received information.
  - Legal standards and regulations on which the revocation order is substantiated on.

4.9.2 Authentication and identification of revocation requests

The revocation of a certificate may be requested by:

- The certificate subscriber.
- The legal representative of the subscriber.
- ANF AC.
- The Recognized Registration Authority that intervene in the processing of the certificate issuance application.

The identification policy for revocation requests accepts the following methods of identification:

- **Electronically**: by the subscriber or certificate responsible electronically signing the revocation request on the date of the revocation request.

- **By telephone**: by replying to the questions asked from the telephone support service available at the number 902 902 172 (calls from Spain) or (+34) 933 935 946 (International).
- **In person**: the subscriber or the legal representative of the certificate holder appearing before any of ANF AC's offices published in the web address https://www.anf.es/en/show/section/offices_725, proving their identity through original documentation, and manually signing the appropriate form.

ANF AC, or any of the Recognized Registration Authorities that form the National Proximity Network, may request the revocation of a certificate if they knew or suspected the private key associated to the certificate has been compromised, or any other fact that would recommend taking such action.

ANF AC must authenticate requests and reports relating to the revocation of a certificate, verifying they come from an authorized person.

These requests and reports will be confirmed following the procedures set out in the Certification Practice Statement.

4.9.3 Procedure for revocation request

The subscriber of a revocation must fill the Certificate Revocation Application Form and process it before ANF AC by any of the means provided herein.

The revocation application shall contain at least the following information:

- Revocation request date.
- Identity of the subscriber.
- Reason given for the revocation request.
- Name and title of the person requesting the revocation.
- Contact information of the person requesting the revocation.

The revocation application shall be processed upon receipt.

The request must be authenticated, in accordance to the requirements established in the corresponding section of this policy, before proceeding with the revocation.

Once the request has been authenticated, ANF AC may directly revoke the certificate and inform the subscriber and, where appropriate, the certificate responsible on the certificate's change of status.

4.9.4 Revocation request grace period

As defined in the CPS of ANF AC.

4.9.5 Time within which CA must process the revocation request

As defined in the CPS of ANF AC.

4.9.6 CRL lists verification requirements

The relying parties must verify the status of the certificates on which they will rely; for such purpose, they can verify the latest CRL issued within the period of validity of the certificate of interest.

4.9.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.9.8 On-line verification availability of the revocation

ANF AC offers relying third parties an on-line revocation verification service, which is available 24 hours a day, 7 days a week.

4.9.9 On-line verification requirements of the revocation

Relying parties may verify online the revocation of a certificate in the website https://www.anf.es/en.

The ANF AC's certificate consultation system requires prior knowledge of some parameters of the certificate of interest. This procedure prevents massive data collection.

This service meets the requirements in terms of personal data protection and only provides copies of these certificates to duly authorized third parties.

Access to this system is free.

4.9.10 Certificate suspension

Not applicable.

4.9.11 Suspension applications authentication and identification

Certificate suspension is not allowed.

4.10 Key storage and recovery

Except for centralized electronic signature certificates, ANF AC does not store, nor has the ability to store the private key of the subscribers and, therefore, does not provide key recovery service.

5 Facilities, physical security, management and operational controls

ANF AC maintains the following criteria in relation to the information available for audit and analysis of incidents related to certificates.

a) Control and incident detection

Any interested person can communicate their complaints or suggestions through the following means:

- By telephone: 902 902 172 (calls from Spain); (+34) 933 935 946 (International).
- By email: info@anf.es
- Filling the electronic form available on the website https://www.anf.es/en.
- In person at one of the offices of the Recognized Registration Authorities.
- In person at one of the offices of ANF AC.

The annual internal audit protocol specifically requires the completion of a review of the operation of certificates issuance, with a minimum sample of 3% of the issued certificates.

b) **Incident Registry**

ANF AC has an Incident Registry in which it is registered every incident that has occurred with the certificates issued and the evidences obtained. These incidents are registered, analyzed, and resolved per the procedures of ANF AC's Information Security Management System.

The Security Manager determines the severity of the incident and names a responsible and, in case of significant security incidents, reports to the PKI Governing Board.

5.1 Physical security controls

As defined in the CPS of ANF AC.

5.2 Procedural controls

As defined in the CPS of ANF AC.

5.3 Personnel controls

As defined in the CPS of ANF AC.

6 Technical security controls

As defined in the CPS of ANF AC.

7 Certificate, CRL and OCSP profiles

The certificate incorporates information structured in agreement with THE IETF's X.509 v3 standard as defined in the specification RFC 5280 *(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)*.

Certificates which are issued as qualified comply with the standards:

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI) Certificate Profiles, Part 5: QCStatements
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

The certificate validity period is outlined in Universal Coordinated Time, and coded per the specification RFC 5280.

The subject public key is encoded per the specification RFC 5280, as well as the signature's generation and codification.

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.

Proprietary fields

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").

QCStatements

The certificates issued by ANF AC follow what is defined in the ETSI EN 319 412-5 *(Certificate Profiles-QCStatements)*:

- **QcCompliance**, refers to a declaration of the issuer in which it states the qualification with which the certificate is issued, and the legal framework to which it is submitted. Specifically, the certificates submitted to this policy, issued as qualified, outline:

"This certificate is issued with the qualification of qualified in accordance with Annex I of Regulation (EU) 910/2014 of the European Parliament "

- **QcLimitValue**, informs about the monetary limit, which the CA assumes as a liability for the loss of transactions attributable to it. This OID contains the values sequence: currency (coded in accordance to the ISO 4217), quantity and exponent. E.g. EUROS 100x10 raised to 1, which presupposes a monetary limit of 1000 EUROS.

  Furthermore, to facilitate the consultation of this information, the liability limit is included in the proprietary extension of the OID 1.3.6.1.4.1.18332.41.1, outlining the amount in euros. In case of doubt or dispute, one must always give preference to the reading value outlined in the OID 1.3.6.1.4.1.18332.41.1.

- **QcEuRetentionPeriod**, determines the period in which all the information relevant to the use of the certificate, after it has expired, is stored. In case of ANF AC, it is 15 years.

- **QcSSCD**, determines that the private key associated to the public key contained in the electronic certificate, is in a qualified signature creation device as defined in accordance with Annex II of the Regulation (UE) 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 the Directive 1999/93/CE.

- **QcType**, when the certificate is issued with the profile (SIGNATURE), QcType 1 is outlined

- **QcPDS,** The URL that allows access to all the ANF AC PKI policies in English is provided. In accordance with ETSI 319 412-5, https protocol shall be used.

Subject Alternative Name

Specification IETF RFC 5280 provides the use of the following data type:

- Email-based identity.
- Identity based on Distinguished Name (DN), which is often used to construct an alternative name based on proprietary attributes, which are not ambiguous in any case.
- Identity based on internet domain name (DNS).
- IP address-based identity.
- Identity based on universal resource identifier (URI).

7.1 Certificate Profiles

As defined in the technical profiles document.

7.2 CRL profile

As defined in the CPS of ANF AC.

7.3 OCSP profile

As defined in the CPS of ANF AC.

8 Compliance audit

As defined in the CPS of ANF AC.

9 General regulations

As defined in the CPS of ANF AC.