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
Website: www.anf.es/en

Security Level

Public Document

Important Notice

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

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

Website: 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 (hereinafter eIDAS Regulation), and with the Spanish Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. 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.

This document is the Certification Policy (CP) corresponding to the **qualified certificates for electronic signature** issued by ANF AC in accordance with the provisions in Annex I of the eIDAS Regulation and as defined in Spanish Law 6/2020. It details and supplements what is specified in ANF AC Certification Practices Statement and its addendum, defines the operational and procedural requirements to which the usage of these certificates is subjected, and 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.
To develop its content the IETF RFC 3647 structure has been followed, including those sections that are specific to this type of certificate.

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 https://anf.es/en/legal-repository/

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

Qualified certificates for electronic signature are electronic statements that associate validation data of a signature with a natural person, and confirm name or pseudonym of that person. ANF AC issues the following types of qualified certificates for electronic signature:

- **Natural Person Certificates:** The subscriber is a natural person with no connection to any entity.

- **Corporate Natural Person Certificates: The** subscriber is a natural person employed by a legal person, without power of attorney.

- **Certificates of Representation:** The subscriber is a natural person representing an organization, with powers of representation to carry out procedures on behalf of the entity. ANF AC issues the following representation certificates:

  - **Legal Representative of a Legal Person Certificate**
    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**
    The signatory acts 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).
    Entity without legal personality, are those to which article 35.4 of the Spanish General Tax Law and other applicable legislation refer to.

  - **Legal Representative of Sole and Joint and Several Directors Certificate**
    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. This type of certificate for exclusive use for legal representatives of commercial companies *(Sociedades Mercantiles)* and other legal persons whose registration is mandatory in the Commercial Registry, and who meet the condition of sole administrator or joint administrator of the same.

- **Public Employee Certificates:** Certificate in accordance with the requirements established in article 43 of Spanish Law 40/2015, of October 1, on the Legal Regime of the Public Sector for the electronic signature of personnel at the service of Public Administrations, in which the subscriber is a representative of a Public Administration with sufficient competences to request 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). These certificates are adapted to the profiles and definitions established by the *Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas* in its document "*Perfiles de certificados electrónicos*" *(section 10: Certificado de empleado público)* for **high** assurance levels [1]*(section 10.3)* and **medium/substantial** *(section 10.4).*

ANF AC qualified certificates for electronic signature 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.** Downloadable file that the holder can download in his computer terminal or register it in the centralized remote electronic signature service, managed by ANF AC**.**

[1] *See section **2.1 Niveles de aseguramiento** of the document "Perfiles de certificados electrónicos".*

- **Qualified Signature Creation Device (QSCD[2])**. The key pair has been generated in the QSCD device that stores them.
- **Centralized service for electronic signature certificates**. The signature creation data has been generated in a cryptographic token QSCD and, in accordance with the requirements of art. 8 and art. 24 (b and c), the use environment is managed by ANF AC on behalf of the signature creator, and are under the exclusive control of its owner.

1.2 Document name and identification

Name of the document	Certification Policy for certificates for electronic signature		
Version	1.3		
Status	APROVED		
OID	1.3.6.1.4.1.18332.3.4.1		
Approval date	22/02/2023	**Publication date**	22/02/2023

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

Version	Changes	Approval	Publication
1.3.	Annual review without relevant changes	22/02/2023	22/02/2023
1.2.	Inclusion of the Corporate Natural Person Certificate	01/03/2022	01/03/2022
1.1.	Annual review: correction of errors, LFE references, restructuring of OIDs, clarification of references for Public Employee certificates.	02/03/2021	02/03/2021
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

[2] *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

Qualified certificates for electronic signature issued by ANF AC can be used for the following purposes:

- Guarantee the identity of the signatory.
- Guarantee the integrity of the signed document.
- Identify the signatory of the document. (In the case of a Public Employee with a pseudonym, the identification will be by pseudonym.)

These certificates must be used in accordance with Spanish Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. The use of the keys and the certificate by the subscriber, presupposes the acceptance of the conditions of use established in the CPS of ANF AC and its addendum.

The use of these certificates is allowed in the relations of the signer with the Public Administrations and in strictly particular uses. In the case of certificates of Legal Representation before Public Administrations, the use is limited to those that allow the powers of representation.

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.

The use of Public Employee certificates and public employee certificates with a pseudonym for uses other than that established in Law 40/2015, of October 1, on the Public Sector Legal Regime for this type of certificates is not allowed.

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

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, including a Common Name (CN) field.

Attribute O *(Organization name)*, in case of inclusion needs to refer to:

- In the case of **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 the case of **Legal representative of a legal person certificates**, the name of the company they represent, and the VAT number in the "organizationIdentifier" attribute.
- In the case of **Professional attribute**: 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 **Freelancer** 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.

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.

3.1.1. Need for names to be meaningful

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

3.1.2. Anonymous or pseudonyms

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

3.1.3. Rules for interpreting various name forms

As defined in the CPS of ANF AC.

3.1.4. Uniqueness of names

As defined in the CPS of ANF AC.

3.1.5. 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. Proof of Private key possession

As defined in the CPS of ANF AC.

3.2.2. Subscriber identity authentication

See section 4.3.1.

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 requests for qualified certificate for electronic signature for natural persons of legal age, with full legal capacity to act.

The subscriber must complete the Certificate Request Form assuming responsibility for the veracity of the information outlined, and process it before ANF AC using one of the following means:

a) **In person**: the subscriber may appear before an Operator of an Identity Verification Office (IVO) attached to a Registration Authority (RA), identifying the applicant by means of an identity document accepted by national legislation, being an original document and in valid status. In his presence, he will proceed to sign the application form, which must be duly completed.

It may be possible to dispense with face-to-face verification in the following cases:

b) **By ordinary mail**: If the corresponding forms have been duly completed, and the subscriber's signature has been legitimized in the presence of a notary public, attaching certified copies of the identity, authorization and legal representation documents.

c) **Telematically**: On the website https://www.anf.es, interested parties have the application form, which must be completed and signed electronically by means of a valid qualified electronic signature certificate or by identifying themselves and accepting the documents by means of one of the means of remote identification that are legally approved, in accordance with Art.7. 2) of Law 6/2020.

4.3. Procedure processing

The RA will be in charge of processing the application in accordance with what is established for this purpose in the CPS of ANF AC.

4.3.1. Identity authentication

The subscriber must provide a mobile phone number and an email address of his trust. ANF AC sends 2 verification codes to these mailboxes in order to confirm the request. 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. 7.5 of Spanish Law 6/2020, 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.

4.3.2. Supporting documentation

- **About the Natural Person:**
  - DNI or passport *(Spanish citizens)*
  - Identity Document / Passport / NIE card (issued by the Registry of Citizen Members of the Union), and Certificate issued by the Registry of Citizen Members of the Union*. (Foreign citizens, members of the EU or European Economic Area)*
  - Passport or permanent residence card. *(Foreign citizens not members of the EU)*
  - Physical address and other data that allows contact with them. In particular, personal contact mailboxes such as mobile phone number and email address. If deemed necessary by the IVO, ARR, or IRM, they may request additional documents to verify the reliability of the information,

such as recent utility bills or bank statements. If the IVO, ARR or IRM know the subscriber personally, they can issue and sign a Declaration of Identity[3].

The documents used to verify identity (DNI, NIE, Passport, residence card) must include a photograph that allows the identity of the person appearing to be verified. In case of poor clarity, or doubt in your recognition of it, another official document that incorporates a higher quality photograph (eg, driver's license) may be requested.

- 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:
  - **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.
  - **Powers of attorney**. The original document will be digitized by the RA operator who will sign it electronically.

- **In case of representation:**

Regarding legal form	
Corporations and other legal entities which registration is compulsory in the Mercantile Registry	Authentic copy, the deed of incorporation registered in the Mercantile Registry, or certification issued by the Mercantile Registry. To prove the representation: o 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, o in the case of Representatives, authentic copy of the power of attorney.
Associations, Foundations, and Cooperatives	Original or certified copy of a public record certificate detailing the registration of their incorporation
Civil societies and other legal entities	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.

[3] **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.

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
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.
Other legal forms	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.

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

4.3.3. Processing in the IVO or RRA

When the procedure is carried out in person before an Operator of an Identity Verification Office (IVO) attached to a Registration Authority (RA), accreditation of the face-to-face act will be required in order to make it impossible to repudiate the procedure carried out, for this purpose they will obtain one or more evidences that will be associated with the application form, eg. handwritten signature, graphometric signature, photograph, video, voice, fingerprints, or reading of the chip assembled on the official identity document.

4.3.4. Processing by legitimation of signature by a notary public or certified by the ARR or IVO operator

In the case of the intervention of a Notary Public, the signature of the subscriber will be required in the request for issuance of a certificate (LRDASEC 6/2020, Art. 7.1). 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".

4.3.5. Approval or rejection of certificate applications

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 (hereinafter IRM), with which ANF AC subscribe the applicable legal document.

The IRM 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 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, they 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, for the purposes of the GDPR, the LOPDPGDD and as provided in article 8 of Spanish Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

The IRM may require additional information or documentation from the subscriber, which will have 30 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, they will reject the certificate request.

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

4.3.6. Time to process certificate issuance

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.

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.

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.

4.4.1. Certification Entity actions during issuance process

As defined in the CPS of ANF AC.

4.4.2. Notification to subscriber

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

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.

4.5. 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, especially its legal representation capacity.

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 7.5. of the Spanish Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, certificate renewal by electronically signed applications requires that less than five years have passed since the personal identification took place.

To ensure compliance with article 7.5. of the Spanish Law 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza and to not exceed the period of 5 years from the initial identification, ANF AC applies the following procedures and technical security measures:

- 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

As defined in the CPS of ANF AC.

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

7.1. Certificate Profiles

The ETSI EN 319 412 family, and specifically part 2 (ETSI EN 319 412-2), specifies the content of qualified electronic signature certificates issued to natural persons. The profile is based on IETF RFC 5280 recommendations and the ITU-T X.509 standard.

As defined in the qualified certificates for electronic signature profiles document of ANF AC.

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

Type	Storage		OID
Natural Person Class 2	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
Corporate Natural Person	Cryptographic software.		1.3.6.1.4.1.18332.3.4.1.6.22
	QSCD		1.3.6.1.4.1.18332.3.4.1.7.22
	QSCD. Centralised service.		1.3.6.1.4.1.18332.3.4.1.8.22
Legal Representative of Legal Person	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	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	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
Public Employees	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

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.