Certificate Policy

Certificates for Electronic Seal

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: 932 661 614 (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. Certificates of type PSD2 are in conformity with ETSI TS 119 495, comply with the technical regulation standards of Delegated Regulation (EU) 2018/389 of the Commission, which complements the Directive (EU) 2015/2366, and the Royal Decree-Law 19/2018 of Spain, respecting the guidelines established by the Competent National Authority for payment services.

This document is the Certification Policy (CP) corresponding to the **qualified certificates for electronic seal** issued by ANF AC in accordance with the provisions in Annex III 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 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 produced. 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. Description of Certificates

These certificates, in accordance with Annex III Regulation UE 910/2014 (eIDAS), serve as proof that an electronic document has been issued by a legal entity, providing certainty about the origin and integrity of the document. ANF AC issues the following types of qualified certificates for electronic seal:

- **Qualified Electronic Seal Certificate:** Certificates with basic electronic seal profile.

- **Qualified Public Administration Electronic Seal Certificate:** They are electronic certificates in public services in accordance with article 37 of Regulation (EU) 910/2014, derived from Royal Decree 1671/2009 and in accordance with the provisions of Law 39/2015 of October 1, Common Administrative Procedure of the Public Administrations, Law 40/2015 of October 1, of Legal Regime of the Public Sector (LRJ). 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 9: Certificado de sello electrónico)* for **high** assurance levels [1]*(section 9.2)* and **medium/substantial** *(section 9.3).*

- **Qualified PSD2 Electronic Seal Certificate:** They are qualified certificates of electronic seal PSD2, in accordance with Directive (EU) 2015/2366, and Royal Decree-law 19/2018 of Spain, are in compliance with ETSI TS 119 495, and respect the guidelines established by the Authority National Competent Payment Services

The maximum validity period for qualified certificates for electronic seal issued by ANF AC is 5 years.

These certificates can be issued in the following support formats:

- **Cryptographic software**, including the key distribution service.
- **Qualified Seal Creation Device (QSCD[2])**. The key pair has been generated in the QSCD device that stores them.
- **Centralized service for electronic seal 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] *See section **2.1 Niveles de aseguramiento** of the document "Perfiles de certificados electrónicos".*

[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

1.2. Document name and identification

Name of the document	Certification Policy Certificates for Electronic Seal		
Version	1.9		
Policy status	APPROVED		
OID	1.3.6.1.4.1.18332.25.1.1		
Approval date	01/03/2022	**Publication date**	01/03/2022

The version of this Certification Policy will only be changed if there are substantial changes that affect its applicability.

Version	Changes	Approval	Publication
1.9.	Review and clarifications.	01/03/2021	01/03/2021
1.8.	Review and clarifications.	19/02/2021	19/02/2021
1.7.	Review and inclusion of certificates for PSD2.	30/01/2019	30/01/2019
1.6.	Review.	30/03/2017	30/03/2017
1.5.	Review and adaptation to eIDAS.	19/10/2016	19/10/2016
1.4.	Review.	03/04/2015	03/04/2015
1.3.	Review.	03/05/2014	03/05/2014
1.2.	Inclusion of more certificates for electronic seal available	08/07/2014	08/07/2014
1.1.	Inclusion of High Level Electronic Seal Certificate	01/06/2012	01/06/2012
1.0.	Document creation	06/02/2011	06/02/2011

1.3. Parties of the PKI

As defined in the CPS of ANF AC.

1.3.1. Subject

1.3.1.1. Electronic Seal Certificate

It is a legal person, which subscribes to the terms and conditions of a certificate, and whose identity is linked to the seal verification data (Public Key) of the certificate issued by ANF AC. Therefore, the identity of the subscriber is linked to the electronically sealed by the signer, using the seal creation data (Private Key) linked to the certificate issued by ANF AC.

1.3.1.2. Public Administration Electronic Seal Certificate

It is a public administration, body, or entity, which subscribes to the terms and conditions of a certificate, and which identity, and where appropriate, its electronic office, is linked to the seal verification data (Public Key) of the certificate issued by ANF AC. Therefore, the identity of the subscriber is linked to the

electronically signed by the signer, using the seal creation data (Private Key) linked to the certificate issued by ANF AC.

1.3.1.3. PSD2 Electronic Seal Certificate

It is a Payment Service Provider (PSP), which subscribes the terms and conditions of use of the certificate in accordance with the requirements established in Delegated Regulation (EU) 2018/389 of the Commission, which complements the Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for enhanced customer authentication and common and secure open communication standards. The identity of the subscriber is linked to the verification data of the Seal (Public Key) of the certificate issued by ANF AC.

1.4. Certificates usage

1.4.1. Allowed usage

These certificates must be used in accordance with Law 6/2020, of November 11, regulating certain aspects of electronic trust services. 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.

- Documents sealing
- Legal person asset authentication certificate" (acting as component certificate for example for authentication on applications servers) (*keyusage will have the bit "digitalSignature" combined with the keyEncipherment (or KeyAgreement) and with extendedkeyusage ("serverAuth", "clientAuth").*

1.4.2. Limits of certificate usage

The subscriber can only use the private key and the certificate for uses authorized on this CP and restricted to the application or department that appears on the certificate.

Its use and acceptance must follow the usage limitations stated in the certificate, assuming the limitation of liability contained in the OID 1.3.6.1.4.1.18332.40.1. and / or in QcLimitValue OID 0.4.0.1862.1.2. Similarly, the holder may only use the key pair and the certificate after accepting the conditions of use established in the CPS.

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

1.4.3. Prohibited usage

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. Information Publication and Repositories

2.1. Repositories

As defined in the CPS of ANF AC.

2.2. Information publication

As defined in the CPS of ANF AC.

2.3. Frequency of Updates

As defined in the CPS of ANF AC.

2.4. Access controls to repositories

As defined in the CPS of ANF AC.

2.5. PSD2 Certificates

The Competent National Authority may request information about certificates that contain an authorization number from a Payment Service Provider (PSP) assigned by that institution. ANF AC will report on the certificates issued in accordance with the provisions of each repository.

3. Identification and Authentication

3.1. Name registration

3.1.1. Types of names

The CN (CommonName) attribute must refer to the name of the application or department that uses it. In case of electronic seal certificates, due to compatibility reasons, it is possible the inclusion in the CommonName of the Subject certain attributes that may be necessary for treatment, such as the name of the entity subscriber or responsible for the seal, and its VAT number.

In the electronic seal certificates, the company name is included in the attribute “organizationName” and the VAT number in the attribute “organizationIdentifier”:

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.

3.1.2. Need for names to be meaningful

In all cases the distinguished names must make sense.

3.1.3. Anonymous or pseudonyms

Are not allowed.

3.1.4. Rules for interpreting various name formats

As defined in the CPS of ANF AC.

3.1.5. Uniqueness of names

As defined in the CPS of ANF AC.

3.1.6. 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.

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

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

3.2. Initial identity validation

3.2.1. Proof of possession of the private key

As defined in the CPS of ANF AC.

3.2.2. Authentication of the identity

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

The Issuance Reports Manager will 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 the 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.

The documentation type, processing forms, authentication and validation procedures are specified in the 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 request

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

4. Operational Requirements

4.1. National Interoperability scheme and national security scheme.

4.1.1. Operations and management of the 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 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. Processing procedure

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.

4.3.1.1. Subscriber

When the application is done before an IVO or a RA, the subscribers must prove their identity and submit valid original or certified copies of the following documents:

- 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 representative must have sufficient powers of attorney.

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.

[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.

4.3.1.2. Certificate responsible

The same procedure will be followed as the one specified in the preceding paragraph "4.3.1.1 Subscriber", with the particularity that, in this case, the required powers of attorney of the subscriber will be replaced with the signature of the Authorization and Acceptance of Liability Certificate found on www.anf.es/en. The certificate shall be signed by the legal representative and the certificate responsible.

4.3.1.3. Subject

The subscriber processing the application for a certificate, must submit original or certified copy of the following valid documentation:

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: ○ 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	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.
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.

4.3.2. 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.

4.3.3. 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).

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".

4.3.4. 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.
- In the PSD2 Electronic seal certificate, ANF AC will verify, using authentic information of the Competent National Authority, the specific attributes of PSD2,
    - authorization number,
    - roles, and
    - name of the Competent National Authority provided by the subject,

  If the Competent National Authority provides standards for the validation of these attributes, ANF AC will apply those standards.
- It is automatically verified that none of the natural or legal persons associated with the request appear in the blacklist of individuals and entities.

4.3.5. 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's actions during the certificate 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 defined in the CPS of ANF AC.

4.5.2. Return of Certificate

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

In case of malfunction due to technical reasons or erros 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 will 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 monitoring, investigating or confirming the accuracy of the information contained in the certificate after its issuance. In case of receiving information regarding the inaccuracy or the current non-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. Renewal of Certificates

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 request the renewal

The renewal application form must be signed by the same subscriber, be the subscriber or the legal representative that processed the certificate request. The personal circumstances of the subscriber should not have changed, especially its legal representation capacity.

4.7.3. Identification and authentication of the Routine renewal applications

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 Spanish 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.

This token is unique to any other provided by ANF AC and is programmed so that the user may be able to make a single renewal. This technical procedure prevents an automatic processing once 5 years have passed since the initial identification.

- 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.

- Before the renewal of the PSD2 certificates, ANF AC will repeat the verification of the specific attributes of PSD2 included in the certificate. If the Competent National Authority provides standards for the validation of these attributes, ANF AC will apply those standards.

4.7.4. Approval or rejection of applications for renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.5. Notification of certificate renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.6. Acceptance of the certificate renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.7. Publication of the renewal certificate

The same procedure performed for the emission process specified herein shall be followed.

4.7.8. Notification of certificate renewal

Not contemplated

4.7.9. Identification and authentication of re-keying applications after revocation (non-compromised key)

The renewal of expired or revoked certificates is not authorized.

4.8. Certificate modification

Not applicable.

4.9. Certificate revocation

Generally, as defined in the CPS of ANF AC.

In the PSD2 certificates, if the National Competent Authority (NCA), as the owner of the specific information of PSD2, notifies ANF AC that it has changed relevant information, ANF AC will investigate this notification regardless of its content and format. ANF AC will determine if the changes affect the validity of the certificate, in which case it will revoke the affected certificate (s). ANF AC will carry out this verification and evaluation within a maximum period of 72 hours, unless justified.

The NCA, to notify changes in the relevant PSD2 regulatory information of the Payment Service Provider (PSP), can send email to info@anf.es

The NCA, as the owner of the specific information of PSD2, can request the revocation of PSD2 certificates following the procedure defined in the CPS. This procedure allows the Competent National Authority to specify the reason for the revocation.

ANF AC will process these requests and validate their authenticity. If a reason is not provided or the reason is not in the area of responsibility of the NCA, ANF AC may decide not to take action. Based on an authentic request, ANF AC will revoke the certificate if any of the following conditions are met:

- The PSP authorization has been revoked,
- the authorization number of the PSP has changed,
- the name or identifier Competent National Authority has changed,
- any PSP role included in the certificate has been revoked,
- Revocation is mandatory by law.
- Any other cause of revocation established in this Certification Policy.

4.10. Keys 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. Physical Security, Facilities, 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. Certificates profiles, CRL and OCSP

7.1. Certificate Profiles

As defined in the certificate profile document.

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

Tipo	Soporte		OID
Certificate for electronic seal	Cryptographic software		1.3.6.1.4.1.18332.25.1.1.1
	QSCD		1.3.6.1.4.1.18332.25.1.1.4
	Centralized Service		1.3.6.1.4.1.18332.25.1.1.9
Certificate for electronic seal AAPP	Medium level	Cryptographic software	1.3.6.1.4.1.18332.25.1.1.3
	High level	QSCD	1.3.6.1.4.1.18332.25.1.1.2
		Centralized Service	1.3.6.1.4.1.18332.25.1.1.11
Certificate for electronic seal for PSD2	Cryptographic software		1.3.6.1.4.1.18332.25.1.1.5
	QSCD		1.3.6.1.4.1.18332.25.1.1.6
	Centralized Service		1.3.6.1.4.1.18332.25.1.1.7

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 Provisions

As defined in the CPS of ANF AC.