ANF AUTORIDAD DE CERTIFICACION

Certification Policy Electronic Seal Certificates

National Registry of Associations. Number 171,443. CIF G-63287510

. CIF G-63287510

© ANF Certification Authority

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

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

Web: www.anf.es

Security level

Public Document

Important announcement

This document is the property of ANF Certification Authority

Its reproduction and dissemination is prohibited without the express authorization of ANF Certification Authority

2000 - 2021 CC-BY- ND (Creative commons licenses)

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

Telephone: 932 661 614 (Calls from Spain) International (+34) 933 935 946

Web: www.anf.es

INDEX

1. Introduction

ANF Certification Authority (ANF AC) is a legal entity established under Organic Law 1/2002 of March 22 and registered with the Ministry of the Interior with the national number 171.443 and CIF G-63287510.

The Public Key Infrastructure (PKI) of ANF AC has been designed and is managed in accordance with the legal framework of Regulation [EU] 910/2014 of the European Parliament, and with Law 6/2020, of November 11, regulating certain aspects of electronic trust services. ANF AC's PKI is in compliance 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 Certificates Profile).* PSD2 type certificates are in compliance with ETSI TS 119 495, comply with the regulatory technical standards of Commission Delegated Regulation (EU) 2018/389, which complements 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.

ANF AC uses OID's according to the ITU-T Rec. X.660 standard and the ISO / IEC 9834-1: 2005 standard (*Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).*
ANF AC has been assigned the private company code (*SMI Network Management Private Enterprise Codes)* 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 (PC) corresponding to the certificates issued by ANF AC of the type "Electronic Seal", "Electronic Seal AA.PP." and, "Electronic Seal PSD2". These certificates can be 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 July 23, 2014, regarding electronic identification and trust services for companies. electronic transactions in the internal market, and with the consideration of qualified as defined in the current legislation.

To prepare its content, the structure of the IETF RFC 3647 PKIX has been taken into account, including those sections that are specific for this type of certificate.

This document defines the procedural and operational requirements to which the use of these certificates is subject, and defines the guidelines that ANF AC uses for their 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 just one of the various documents that govern the PKI of ANF AC, it details and complements what is defined in the Certification Practice Statement and its addendum. ANF AC supervises and supervises that this PC is compatible and consistent with the rest of the documents you have prepared. All the documentation is freely available to users and third parties who trust https://www.anf.es

This Certification Policy assumes that the reader knows the concepts of PKI, certificate and electronic seal. Otherwise, the reader is recommended to learn the above concepts before continuing to read this document.

1.1. Description of the certificates

These certificates, in accordance with Annex III of EU Regulation 910/2014 (eIDAS), serve as proof that an electronic document has been issued by a legal person, providing certainty about the origin and integrity of the document.

ANF AC, within the framework of its service of qualified certificates of electronic seal, issues the following types:

- **Qualified Certificate of Electronic Seal:** They are certified with the basic profile.

- **Qualified Certificate of Electronic Seal AA.PP:** 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, on Common Administrative Procedure of the Public Administrations, Law 40/2015 of October 1, on the Legal Regime of the Public Sector (LRJ). It adapts to the profiles and definitions established by the General Subdirectorate for Information, Documentation and Publications of the Ministry of Finance and Public Administrations in its document "*Electronic certificate profiles*"(*section 10: Electronic seal certificate)* for assurance levels[1]

  tall (*section 9.2)* Y **medium / substantial (***section 9.3).*

- **Qualified Certificate of Electronic Seal PSD2:** They are qualified certificates of PSD2 electronic seal, 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 Competent National of payment services.

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

These certificates can be issued on the following media:

- **Cryptographic software token,** including the key distribution service.
- **QSCD (***Qualified Seal Creation Device):* Cryptographic token, exclusively devices certified specifically in accordance with the applicable requirements in accordance with article 39 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-andqscds

[1] *See section **2.1 Levels of assurance** of the document "Profiles of electronic certificates".*

- **Centralized Service** of qualified certificates of electronic seal. The creation data of**stamp** have been generated in a QSCD cryptographic token and, in accordance with the requirements of art. 8 and art. 24 (b and c), the usage environment is managed by ANF AC on behalf of the label creator, and is under the exclusive control of its owner.

1.2. Document name and identification

Document name	Certification Policy for Electronic Seal Certificates		
Version	1.8		
OID policy status	PASSED		
	1.3.6.1.4.1.18332.25.1.1		
Approval date	02/19/2021	**Publication date**	02/19/2021

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

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

1.3. Parts of the PKI

As defined in the CPS of ANF AC.

1.3.1. Subject

As defined in the CPS of ANF AC.

1.3.1.1. Electronic Seal Certificate

It is a legal person, which subscribes the terms and conditions of use 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 certificate subscriber is linked to what is electronically stamped by the stamp creator, using the Stamp Creation Data (Private Key) associated with the certificate issued by ANF AC.

1.3.1.2. Electronic Seal Certificate AA.PP.

It is a Public Administration, body or entity of public law, which subscribes the terms and conditions of use of a certificate, whose identity and, where appropriate, electronic headquarters, are linked to the Seal verification data (Public Key) of the certificate issued by ANF AC. Therefore, the identity of the certificate subscriber is linked to what is electronically stamped by the Signatory, using the Seal Creation Data (Private Key) associated with the certificate issued by ANF AC.

1.3.1.3. Electronic Seal Certificate PSD2.

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 regarding regulatory technical standards for strong 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. Use of certificates

1.4.1. Permitted uses

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.

- **Stamping of documents.** Key usage will have the “ContentComitment” bit.
- Authentication of assets of the legal entity. Acting as a component certificate for example for authentication in application servers) (keyusage will have the bit "digitalSignature" combined with the keyEncipherment (or KeyAgreement) and with extendedkeyusage ("serverAuth", "clientAuth").

1.4.2. Certificate usage limits

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

Its use and acceptance must be in accordance with the limitations of use that appear in the certificate, assuming the limitation of responsibility that appears in the OID 1.3.6.1.4.1.18332.40.1. and / or in QcLimitValueOID 0.4.0.1862.1.2. In the same way, the holder may only use the pair of keys 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 uses

As defined in the CPS of ANF AC.

1.5. Contact details of the Certification Entity

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 the information

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 on the certificates that contain an authorization number of 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 the department that uses it. In the case of Electronic Seal Certificates, for compatibility reasons, it is possible to include in the CommonName of the Subject certain attributes that may be necessary for processing, such as the name of the subscriber entity or entity responsible for the seal, and your NIF.

In the Electronic Seal certificates, the company name is included in the "organizationName" attribute and the NIF in the "organizationIdentifier" attribute:

> *"Additional attributes other than those listed above may be present. In particular, when a natural person subject is associated with an organization, the subject attributes**may** also identify such organization using attributes such as **organizationName** and **organizationIdentifier.** Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which defines the semantics for the organization Identifier attribute "*

3.1.1.1. Certificate field completion guide

According to RFC 5280, which uses UTF-8 string, since it encodes groups of international characters including characters from the Latin alphabet with diacritics ("Ñ", "ñ", "Ç", "ç", "Ü", " ü ", etc.). For example, the character eñe (ñ), which is represented in Unicode as 0x00F1.

For all variable literals:

- All literals are entered in uppercase, with the exceptions of the domain / subdomain name and email which will be in lowercase.
- Do not include accents in 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 simplification is allowed, as long as they do not imply difficulty in interpreting the information.

According to RFC 5280, which uses UTF-8 *1 string, since it encodes groups of international characters including characters from the Latin alphabet with diacritics ("Ñ", "ñ", "Ç", "ç", "Ü", "ü", etc.). For example, the character eñe (ñ), which is represented in Unicode as 0x00F1.

DNI / NIE

The term NIF covers both DNI and NIE.
If you opt for the DNI or NIE label, instead of the NIF, the corresponding one will be used.

3.1.2. Need for names to be meaningful

In all cases the distinguished names must make sense.

3.1.3. Pseudonyms or anonymous

They are not allowed.

3.1.4. Rules used to interpret 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 related to names and brands

ANF AC does not assume any commitment regarding the use of trademarks in the issuance of the Certificates issued under this Certification Policy. ANF AC is not obliged to verify the ownership or registration of registered trademarks and other distinctive signs.

Certificate subscribers will not include names in requests that may be infringing.

The use of distinctive signs whose right to use is not owned by the subscriber or is duly authorized is not allowed.
ANF AC reserves the right to refuse a certificate request due to a name conflict.

3.2. Initial identity validation

3.2.1. Proof of private key possession

As defined in the CPS of ANF AC.

3.2.2. Identity authentication

The Certificates issued under this Certification Policy identify the subject in whose name the issuance of the certificate is requested and the subscriber of the certificate.

The Responsible for Issuance Reports will use the appropriate means to ensure the veracity of the information contained in the certificate. Among these means are external registry bases and the possibility of requesting additional information or documentation from the subscriber.

The tax identifiers of the subject and the subscriber will be incorporated into the certificate. In addition, the subscriber must provide a mobile phone number and an email address that they trust. The email address and the SMS or WhatsApp service associated with your mobile phone will have the

consideration of authorized mailboxes so that ANF AC can deliver certified electronics,
even double authentication in the case of centralized electronic seal certificate service, or any other that is deemed necessary. The user assumes the obligation to inform ANF AC of any change in email address or mobile phone number.

In accordance with Art. 13.3 of Law 59/2003 on Electronic Signature, when the recognized (qualified) certificate contains other personal circumstances or attributes of the subscriber, such as their status as the holder of a public office, their membership in a professional association or their qualification, these must be verified by means of the official documents that accredit them, in accordance with their specific regulations.
The type of documentation, processing procedures, authentication and validation procedures are specified in this document.

3.3. Key renewal

In the case of renewal of the key, ANF AC will previously inform the subscriber about the changes that have occurred in the terms and conditions with respect to the previous issuance.

A new certificate may be issued keeping the previous public key, provided that it continues to be considered cryptographically secure.

3.4. Revocation Request

All revocation requests must be authenticated. ANF AC will verify the capacity of the subscriber to process this request.

4. Operational Requirements

4.1. National Interoperability Scheme and National Security Scheme.

4.1.1 Operation and management of the Public Key Infrastructure

The operations and procedures carried out for the implementation of this Certification Policy are carried out following the controls required by the recognized standards for this purpose, these actions being described in the sections “Physical Security, Facilities, Management and Operational Controls” and “Controls of Technical Security ”of the Declaration of Certification Practices of ANF AC.

The ANF AC Certification Practices Statement 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 the Resolution of November 29, 2012, of the Secretary of State for Public Administrations, which publishes the Agreement for the approval of the Electronic Signature Policy and Certificates of the General Administration of the State and their publication is announced in the corresponding headquarters, and specifically the profile of this type of certificates is in accordance with the profile approved by the Superior Council of Electronic Administration, in a meeting of the Permanent Commission of May 30, 2012 and published in Annex II of the aforementioned Resolution.

4.2. Certificate request

ANF AC only admits application for certificate issuance processed by a natural person of legal age, with full legal capacity to act.

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

to) **In person:** The subscriber may appear before a Recognized Registration Authority, in whose presence they will proceed to sign the application form, which must be duly completed.

b) **By ordinary mail:** Certificate request form handwritten by the subscriber and signed by a Notary Public. Documentation sent by ordinary mail.

4.3. Processing procedure

4.3.1. Identity Authentication

4.3.1.1. Subscriber

When the processing is carried out in person before a Recognized Registration Authority, you must prove your identity and present, in force, an original or authentic copy of the following documentation:

a) Physical address and other data that allow contact with him. If the ARR or RDE deems it necessary, they can request additional documents to verify the reliability of the information, such as recent utility bills or bank statements. If the ARR or the RDE know the subscriber personally, they must issue and sign a Declaration of Identity[2].

b) The ARR, as proof of the face-to-face act and in order to prevent the repudiation of the procedure carried out, may obtain a set of biometric evidence: photography and / or fingerprints.

c) Identification card or passport in the case of national citizens, whose photograph allows the identity of the person appearing to be verified. In case of poor sharpness, another may be requested document official that incorporate Photography (e.g., license of lead).

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

I. To members of the European Union or of States that are part of the European Economic Area:

- National identity document (or equivalent in your country of origin), or NIE card (issued by the Registry of Union Citizens), or passport. The physical identification must be carried out taking as a reference one of these documents that includes a photograph of the person appearing. In case of poor sharpness, another may be requested official document incorporating photography (e.g. license of lead).
- Certificate issued by the Registry of Citizen Members of the Union.

II. To non-EU citizens:

- Passport or permanent residence card, which includes a photograph that allows the identity of the person appearing to be verified. In case of poor clarity, another official document that incorporates a photograph may be requested (eg, driver's license).

e) The Representative must have sufficient power of representation.

f) In the event that the subscriber requires to include other personal circumstances, these must be verified by means of the official documents that accredit them in accordance with their specific regulations.

[2] ***Declaration of Identity:*** *It consists of a formal sworn statement, in which the declarant states that he / she knows personally and directly a certain natural person or a legal person. In addition, it states, as far as its direct knowledge reaches, that it has verified the affiliation data outlined in the Application Form: address, telephone and email, and that they are true.*

The Declaration of Identity incorporates the identity of the declarant, his identity card, the information that has been validated, the date and time of the verification, the signature of the declarant and the corresponding legal warnings in case of perjury.

Appearance before the Registration Authority may be dispensed with in any of the following cases:

1. If the corresponding forms have been duly completed, and the signature of the subscriber has been legitimized in the presence of a notary public, attaching certified copies of the identity, authorization and legal representation documents.

2. Processing via telematics. On the websitehttps://www.anf.esThe interested parties have the application form, which must be completed and signed electronically by means of a recognized (qualified) certificate in accordance with the provisions of Law 59/2003, of December 19, on electronic signature. The certificate used must have been issued by a CA supported by ANF AC.

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 (LFE 59/2003, Art. 13.1).

4.3.1.2. Responsible for the certificate

The same procedure as that specified in the previous section “4.3.1.1 Subscriber” will be followed, with the particularity that, in this case, the power of representation required of the subscriber will be replaced by the signing of the Authorization and Acceptance of Responsibility Act included in this document. The minutes must be signed by the Legal Representative and by the Certificate Manager.

4.3.1.3. Subject

The subscriber who processes the certificate request must present an original or an authentic copy of the following current documentation:

1.- According to legal form:

- Mercantile companies and other legal persons whose registration is mandatory in the Mercantile Registry will certify the valid constitution by providing an authentic copy of 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 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 Proxy, an authentic copy of the power of attorney.
- Associations, Foundations and Cooperatives will certify the valid constitution by providing an original or authentic copy of a certificate from the public registry where they are registered, relative to their constitution.

- Civil societies and other legal persons shall provide an original or authentic copy of the document that reliably proves their constitution.

- Public Administrations and entities belonging to the public sector:

  - Entities whose registration is mandatory in a Registry will certify the valid constitution by providing an original or authentic copy of a certificate relating to the incorporation data and legal personality of the same.

  - Entities created by regulation will provide reference to the creation regulation.

4.3.2. Approval or rejection of certificate requests

The Responsible for Issuance Reports (RDE) assumes the ultimate responsibility of verifying the information contained in the Request Form, assessing the sufficiency of the documents provided and the adequacy of the request in accordance with the provisions of this Certification Policy.

In addition, it will determine:

- That the subscriber has had access to the information that establishes the terms and conditions relating to the use of the certificate, as well as the issuance fees thereof.

- That the subscriber has had access and has permanent access to all the documentation related to the obligations and responsibilities of the CA, the subscriber, subject, responsible for the certificate and third parties that they trust, especially the CPS and the Certification Policies.

- It will supervise that all the requirements imposed by the applicable legislation on data protection are met, following what is established in the security document included in the CPS, for the purposes of the LOPD as provided in article 19.3 of Law 59/2003 , of December 19, electronic signature.

The certificate issuance process will not start as long as the Issuance Report Manager has not issued the corresponding compliance report. The maximum term established for the issuance of the report will be 15 days. After this period has elapsed without issuance of the mandatory report, the subscriber may cancel the order and receive the fees that he has paid.

The RDE may require additional information or documentation from the subscriber and the subscriber will have 15 days to deliver it. After this period has elapsed without this requirement having been fulfilled, the RDE will issue a report denying the issue. In case of meeting the request, the RDE will have 7 days to issue a final report.

In the event that the RDE verifies that the information provided by the subscriber is not true, it will deny the issuance of the certificate and generate an incident informing the Security Coordinator, in order to determine whether or not the subscriber is blacklisted people and entities with OID 1.3.6.1.4.1.18332.56.2.1.

The validation procedure according to the type of certificate is:

- The RDE will check the documentation provided by the subscriber and by the Registration Authority.

- In the validation process, the Legal Department and the Technical Department will intervene giving support, which will review and technically validate the PKCS # 10 petition certificate.

- In the process of verifying the information and documentation received, the following means may be used:

- Consultation of the official public records in which the entity must be registered in order to verify existence, validity of positions and other legal aspects, such as activity and date of incorporation.

  or In the PSD2 electronic seal certificate, ANF AC will verify, using information authenticity 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.

  or Official Gazettes of national or regional scope of the public organisms to which public bodies and companies belong to.

- It is verified that none of the natural or legal persons associated with the request is on the black list managed with the OID identifier 1.3.6.1.4.1.18332.56.2.1.

4.3.3. Time to process the issuance of certificates

The issuance of a certificate implies the final and complete approval of an application by the Responsible for Issuance Reports. The certificate must be issued within a maximum period of 48 hours, once the RDE report has been issued 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 certificates of the CA that issued them.

4.4.1. Actions of the Certification Entity during the issuance process

As defined in the CPS of ANF AC.

Once the electronic certificate has been issued, the certificate is always delivered electronically.
The same cryptographic device must be used that was used for the generation of the cryptographic key pair and the PKCS # 10 request certificate.

The cryptographic device establishes a secure connection with the trusted servers of ANF AC. The system automatically performs the corresponding security checks. In case of confirmation, the certificate is downloaded and installed automatically.

4.4.2. Subscriber notification

ANF AC, by email, notifies the subscriber of the issuance and publication of the certificate.

4.5. Certificate acceptance

4.5.1. Acceptance

As established in the Certification Practices Statement of ANF AC.

4.5.2. Return

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

In the event of malfunctions due to technical causes or errors in the data contained in the certificate, the subscriber or the person responsible for the certificate can send an electronically signed email to ANF AC, informing of the reason for the return. ANF AC will verify the causes of return, revoke the certificate issued and proceed to issue a new certificate within a maximum period of 72 hours.

4.5.3. Follow-up

ANF AC is not responsible for the monitoring, investigation or confirmation of the accuracy of the information contained in the certificate after its issuance. In the case of receiving information about the inaccuracy or current non-applicability of the information contained in the certificate, it may be revoked.

4.5.4. Certificate publication

The certificate is published in the repositories of ANF AC, within a maximum period of 24 hours from its issuance.

4.5.5. Notification of the issuance of the certificate by the CA to third parties

No notification is made to third parties.

4.6. Denial

As established in the Certification Practices Statement of ANF AC.

4.7. Certificate renewal

In general, as established in the ANF AC Certification Practices Statement.

4.7.1. Valid certificates

ANF AC notifies the subscriber by email of the expiration of the certificate, sending the application form, in order to proceed with its renewal. These notifications are sent 90, 30 and 15 days before the expiration date of the certificate.

Only valid certificates can be renewed as long as the identification made has not exceeded the five-year period.

4.7.2. Persons authorized to request renewal

The renewal request form must be signed by the subscriber himself, either the subscriber himself or the legal representative who processed the certificate request.

The subscriber's personal circumstances must not have changed, especially his capacity for legal representation.

4.7.3. Identification and authentication of routine renewal requests

The identification and authentication for the renewal of the certificate can be carried out either in person, using any of the means described in this section, or by processing the renewal request electronically by completing the corresponding form and signing electronically with a valid certificate issued with the qualification of qualified. , and in which the subscriber of the certificate for which renewal is requested appears as the holder.

In accordance with the provisions of article 13.4 b) of Law 59/2003, of December 19, on Electronic Signature, the renewal of the certificate through electronically signed applications will require that a period of time has elapsed since the personal identification of less than five years.

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

- ANF AC certificates are always generated using a token that must be used to carry out any renewal procedure.
  This token is unique to any other provided by ANF AC and is programmed so that the user can perform a single renewal. This technical procedure makes automatic processing impossible once 5 years have elapsed from the first identification.

- ANF AC follows an application registration system, distinguishing the application date - which coincides with the identification- and the issuance of the certificate. This control allows a second renewal if the period of 5 years from the initial identification has not been reached.
  The technical system requires an express request from the user, the direct intervention of an ANF AC operator which, in turn, needs to validate the request by applying a consistency security control. If the 5 years have been exceeded, the application itself blocks the process. Otherwise, it facilitates the operator the process until the renewal of the certificate.

- Before the renewal of the PSD2 certificates, ANF AC will repeat the verification of the specific PSD2 attributes 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. Renewal of certificates that have exceeded 5 years from the initial identification.

The formalization of the request is required through the subscriber's handwritten signature, a procedure carried out with the interested party's physical presence and using sufficient original documentation. The procedures may be carried out before:

- **Recognized Registration Authority** that, according to the definition of the CPS of ANF AC, are the natural or legal persons to whom ANF AC has provided the necessary technology to perform the functions of registry entity, having formalized the corresponding contract of assumption of responsibilities and agreement of collaboration.

- **Collaborating Registration Authority** that, according to the definition of the CPS of ANF AC, they are people who, in accordance with current legislation, have attributions of notary public.

- **Trusted Entity** that, according to the definition of the CPS of ANF AC, are entities that, at the discretion of ANF AC, have the necessary capacity to determine the identity, capacity and freedom of action of the subscribers.

4.7.5. Approval or rejection of renewal requests

The same procedure will be followed as that performed in the issuance process specified in this document.

4.7.6. Notification of certificate renewal

The same procedure will be followed as that performed in the issuance process specified in this document.

4.7.7. Acceptance of certificate renewal

The same procedure will be followed as that performed in the issuance process specified in this document.

4.7.8. Publication of the renewed certificate

The same procedure will be followed as that performed in the issuance process specified in this document.

4.7.9. Notification to other entities

It is not contemplated.

4.7.10. Identification and authentication of key renewal requests after a revocation -Key not compromised-

The renewal of expired or revoked certificates is not authorized.

4.8. Certificate modification

Non applicable.

4.9. Certificate revocation and suspension

In general, as established in the Certification Practices Statement of ANF AC.

4.9.1. Reasons for revocation

In addition to the provisions of the Certification Practices Statement, ANF AC:

- It will provide instructions and provide legal support for the presentation of complaints or suspicions of compromise of the private key, the misuse of certificates or any type of fraud, or improper conduct.

- It will investigate the incidents of which it has knowledge, within the twenty-four hours following its reception. The Security Coordinator, based on the inquiries and verifications carried out, will issue a report to the Responsible for Issuance Opinions, which will determine the corresponding revocation by means of a substantiated Act, which will include:
  - or The nature of the incident.
  - or Information received.

- In PSD2 certificates, if the Competent National Authority, as the owner of the specific PSD2 information, notifies ANF AC that relevant information has changed, 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 assessment within a maximum period of 72 hours, except for just cause.

  The Competent National Authorities, to notify the changes in the relevant PSD2 regulatory information of the Payment Service Provider (PSP), can send email to,

  info@anf.es

4.9.2. Identification and authentication of revocation requests

They may request the revocation of a certificate:

- The certificate subscriber.
- The legal representative of the subscriber.
- A duly authorized representative.
- ANF AC.
- The Recognized Registration Authority that intervened in the processing of the request for issuance of the certificate.

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

- **Telematics:** By means of the electronic signature of the revocation request by the certificate subscriber or the person responsible for it on the date of the revocation request.
- **Telephone:** by answering the questions made from the telephone support service available at the number 902 902 172 (calls from Spain) International +34 933 935 946
- **In person:** The subscriber or the legal representative of the certificate holder will appear in person at any of the ANF AC offices published at the web address https://www.anf.es/sedes.html; proving your identity through original documentation, and handwritten signing the corresponding form.

ANF AC, or any of the Recognized Registration Authorities that make up its National Proximity Network, may ex officio request the revocation of a certificate if they are aware of or suspect the compromise of the private key associated with the certificate, or of any other fact that it will recommend take such action.

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

Said requests and reports will be confirmed by complying with the procedures established in the Certification Practice Statement.

4.9.3. Procedure for revocation request

The subscriber of the Revocation must complete the Revocation Request Form and process it before ANF AC by any of the means provided in this document.

The revocation request must contain, as a minimum, the following information:

- Revocation request date.
- Subscriber identity.
- Detailed reason for the revocation request.

- Name and title of the person requesting the revocation.
- Contact information of the person requesting the revocation.

The revocation request will be processed upon receipt.

The request must be authenticated, in accordance with 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 person responsible for the certificate about the change in the status of the certificate.

In the case of PSD2 certificates, the Competent National Authority, as the owner of the specific information of PSD2, can request the revocation of the certificate following the procedure defined in this document. This procedure allows the Competent National Authority to specify the reason for the revocation.

ANF AC will process such requests and validate their authenticity. If a reason is not provided or the reason is not in the area of responsibility of the Competent National Authority, 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:

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

4.9.4. Revocation request grace period

As defined in the CPS of ANF AC.

4.9.5. Maximum period for processing the revocation request

As defined in the CPS of ANF AC.

4.9.6. CRL check requirements

Trusting third parties should check the status of the certificates they are going to trust. For this, they can consult the last CRL issued within the validity period of the certificate of interest.

4.9.7. Frequency of issuance of CRL lists

As defined in the CPS of ANF AC.

4.9.8. Availability of online verification of the revocation

ANF AC makes available to third parties who entrust an online revocation checking service, which is available 24 hours a day, 7 days a week.

4.9.9. Requirements for online verification of revocation

Trusting third parties can check the revocation of a certificate online through the website https://www.anf.es
.

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

This service complies with the established requirements regarding the Protection of Personal Data, and only provides copies of these certificates to duly authorized third parties.

Access to this certificate consultation system is free.

4.9.10. Certificate suspension

Non applicable.

4.9.11. Identification and authentication of suspension requests

The suspension of the certificate is not allowed.

4.10. Key deposit and recovery

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

5. Physical Security, Facilities, Management and Operational Controls

ANF AC maintains the following criteria in relation to the information available for audits and analysis of incidents that may exist with the certificates.

a) Incident Detection and Control

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

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

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

b) Incident Record

ANF AC has an Incident Registry in which all incidents that have occurred with the certificates issued, and the evidence obtained, are registered. These incidents are recorded, analyzed and solved according to the procedures of the Information Security Management System of ANF AC.

The Security Coordinator determines the severity of the incident and appoints a person responsible and, in the event of relevant 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 Profiles, CRL Lists and OCSP

7.1. Certificate profiles

As defined in the technical profile document.

In order to identify the certificates, ANF AC has assigned them the following object identifiers (OID):

Guy	Medium		OID
Certificate of Electronic seal	QSCD Cryptographic Software		1.3.6.1.4.1.18332.25.1.1.1
	Token		1.3.6.1.4.1.18332.25.1.1.4
	Centralized Service		1.3.6.1.4.1.18332.25.1.1.9
	Distributed key management software		1.3.6.1.4.1.18332.25.1.1.10
Certificate of Electronic seal AAPP	Level half	Token cryptographic software	1.3.6.1.4.1.18332.25.1.1.3
		Distributed management software of keys	1.3.6.1.4.1.18332.25.1.1.12
	High level	QSCD (High level)	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 of Electronic seal PSD2	QSCD Cryptographic Software		1.3.6.1.4.1.18332.25.1.1.5
	Token		1.3.6.1.4.1.18332.25.1.1.6
	Centralized Service		1.3.6.1.4.1.18332.25.1.1.7
	Distributed key management software		1.3.6.1.4.1.18332.25.1.1.8

7.2. CRL Profile

As defined in the CPS of ANF AC. and technical profile document

7.3. OCSP Profile

As defined in the CPS of ANF AC. and technical profile document

8. Compliance Audit

As defined in the CPS of ANF AC.

9. General disposition

As defined in the CPS of ANF AC.