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
Web: www.anf.es/en

Security Level

Public

Important Notice

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

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

Web: www.anf.es/en

Index

1 Introduction

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

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

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

This document is the Certification Policy (CP) corresponding to the certificates issued by ANF AC, of the type "Electronic Seal", "Public Administration Electronic Seal" and "PSD2 Electronic Seal". These certificates are issued with the consideration of qualified in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and with consideration of qualified as defined in the current legislation.

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 www.anf.es/en.

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

1.1 Description of Certificates

These certificates, in accordance with 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, within the framework of its service of qualified certificates of electronic seal, issues the following types:

- **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).

- **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

These certificates can be issued in the following support formats:

- Cryptographic software token, including the key distribution service.

- HSM - QSCD (Qualified Seal Creation Device): Cryptographic Token, exclusively devices specifically certified 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-and-qscds

- Centralized Service of qualified certificates of electronic seal.
  The seal 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 seal creator, and are under the exclusive control of its owner.

This policy, regarding qualified certificates of the type "Public Administration Electronic Seal", follows the definitions set by the Information and Communications Technologies Department (DTIC) in its document "Electronic certificates profiles" of April 2016.

The following assurance levels are defined:

a. Medium level/Substantial:

This level corresponds to a configuration of security mechanisms suitable for most applications.

The expected risk by this level is appropriate to access applications classified by ENS in the levels of Integrity and Authenticity as low or medium risk.

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

The minimum acceptable security mechanisms include X.509 certificates in cryptographic software token. The use of QSCD devices, or centralized service is also allowed.

The maximum validity of these certificates is 5 years.

The expected risk for this level corresponds to the guarantee level 3 provided in the IDABC Authentication Basic Policy *[1].

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

b. High level:

This level corresponds to a configuration of security mechanisms suitable for applications that require additional measures, per the risk analysis performed.

The expected risk for this level is appropriate to access classified applications per the ENS in the levels of Integrity and Authenticity as high risk.

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

The minimum acceptable security mechanisms include X.509 certificates in cryptographic software token. The use of QSCD devices, or centralized service is also allowed.

The expected risk for this level corresponds to guarantee level 4 provided in IDABC Authentication Basic Policy.

The maximum validity of these certificates is 5 years.

1.2 Document name and identification

Name of the document	Certification Policy Certificates for Electronic Seal		
Version	1.7		
Policy status	APPROVED		
OID	1.3.6.1.4.1.18332.25.1.1		
Approval date	30/01/2019	**Publication date**	30/01/2019

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

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

	Support	Technical Specification	OID
Electronic Seal Certificate	Cryptographic software token	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.1
	QSCD	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.4

	Centralized Service	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.9
	Software with distributed key management	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.10
Public Administration Electronic Seal Certificate	Cryptographic software token	High and Medium Level Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.3
	QSCD	High and Medium Level Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.2
	Centralized Service	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.11
	Software with distributed key management	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.12
PSD2 Electronic Seal Certificate	Cryptographic software token	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.5
	QSCD	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.6
	Centralized Service	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.7
	Software with distributed key management	Algorithm SHA-256 and key length 2048 bits.	1.3.6.1.4.1.18332.25.1.1.8

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

In the case of "High Level Public Administration Certificate", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.6.1

In the case of "Medium Level Public Administration Certificate", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.6.2

Furthermore, when the certificate is issued with the consideration of qualified, in the extension CertificatePolicies (2.5.29.32), will include at least one of the following PolicyInformation:

- qcp-legal (0.4.0.194112.1.0). Certificate in token software
- qcp-legal-qscd (0.4.0.194112.1.2). When the qualified seal certificate, is stored in a qualified device per Regulation UE 910/2014.

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

1.3 Parties of the PKI

1.3.1 Certification Authorities

As defined in the CPS of ANF AC.

1.3.2 Registration Authorities

As defined in the CPS of ANF AC.

1.3.2.1 Recognized Registration Authority

As defined in the CPS of ANF AC.

1.3.2.2 Collaborating Registration Authority

As defined in the CPS of ANF AC.

1.3.3 Issuance Reports Manager

As defined in the CPS of ANF AC.

1.3.4 End entities

1.3.4.1 Subject

As defined in the CPS of ANF AC.

1.3.4.1.1 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.

1.3.4.1.2 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.

1.3.4.1.3 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.

1.3.4.2 Subscriber

As defined in the CPS of ANF AC.

1.3.4.3 Certificate Responsible

As defined in the CPS of ANF AC.

1.3.4.4 Relying parties

As defined in the CPS of ANF AC.

1.4 Certificates usage

1.4.1 Allowed usage

The electronic seal certificate, in accordance with the eIDAS regulation, can have three uses:

(1) "documents sealing" *(key usage will have the bit "ContentComitment"),*
(2) "code sealing" (*keyusage will have the bit "digitalSignature" combined with the extendedkeyusage ("codeSigning"),* and
(3) "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").*

This certificate should never be used exclusively for encryption, nor as web server authentication certificate.

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":

> *"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 organizationIdentifier attribute"*

Attributes	Content	Example
organizationName	Company name, as stated in the official records.	Company name. S.L.
organizationIdentifier	VAT number, as contained in the official records. Coded per the European ETSI EN 319 412-1 Standard	VATES-B0085974Z

In the case of certificates with PSD2 attribute, the authorization number is included in the "organizationIdentifier" attribute, as indicated by ETSI TS 119 495:

Field	Content	Example	Size *
Literal	PSD	PSD	3
Country code	Country code according to ISO 3166	ES	2
Literal	Guion (0x2D (ASCII), U+002D (UTF-8))	-	

National Competent Authority Identifyer	Identifier of the Competent National Authority in Capital letters, without spaces	BDE	2-8
Literal	Guion (0x2D (ASCII), U+002D (UTF-8))	-	
PSP Identifyer	Authorization number of Payment Service Provider	3DFD21	Size is stablished by the National Competent Authority

Any space in the ANC identifier shall be eliminated (ETSI 119495 Clause 5.2.1)

Example *= "PSDES-BDE-3DFD21"*

Certificate issued to a PSP with authorization number 3DFD21 issued by the Spanish National Competent Authority "Banco de España" (BDE).

3.1.2 Specific fields completion guide

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

For all literal variables:

- All literals are entered in capital letters, with the exceptions of the domain name/subdomain and email that will be in lowercase.
- Do not include accent marks in the alphabetic literals
- Do not include more than one space between alphanumeric strings.
- Do not include blank characters at the beginning or end of alphanumeric strings.
- The inclusion of abbreviations based on a simplification is admitted, provided they do not difficult the interpretation of information.

*[1] *For more information see RFC 2279 improved in 3629 (UTF-8, a transformation format of ISO 10646)*

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

The term tax identification number covers both, the National Citizens ID Card, and the Foreign Citizens ID Card.

In case of opting on a specific ID card, instead of the tax identification number, the corresponding ID card will be used.

The following coding is allowed:

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

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

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

e.g.: IDCES-00000000G.

2.- Basic semantics. Consisting in:

The number and letter as stated in the ID card.
e.g.: ID00000000G.

3.1.3 Need for names to be meaningful

In all cases the distinguished names must make sense.

3.1.4 Anonymous or pseudonyms

Are not allowed.

3.1.5 Rules for interpreting various name formats

As defined in the CPS of ANF AC.

3.1.6 Uniqueness of names

As defined in the CPS of ANF AC.

3.1.7 Resolution of conflicts in relation to names and trademarks

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

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

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

a) **In person**: the subscriber may appear before a Recognized Registration Authority, in whose presence will proceed to sign the application form, which shall be dully fill out.
b) **By mail**: certificate request form handwritten signed by the subscriber and his/her signature legitimized by public notary. Documentation sent by ordinary mail.

4.3 Processing procedure

4.3.1 Identity authentication

4.3.1.1 Subscriber

When the application is done before a Recognized Registration Authority, the subscriber must prove his/her identity and submit valid original or certified copies of the following documents:

a) Physical address and other contact details of the subscriber. If deemed necessary by the Registration Authority or the Issuance Reports Manager, additional documents may be solicited to verify the reliability of the information, such as recent utility bills or bank statements. In case the RRA or the IRM know the subscriber personally, they shall issue and sign a Declaration of Identity *[1].

b) The RRA, as proof of attendance and to preclude the repudiation of the procedure done, can get a set of biometric evidence: photography and/or fingerprints.

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

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

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

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

- Certificate issued by the Registry of Citizens of Members of the European Union.

II. To non-EU citizens:

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

e) The representative must have sufficient powers of attorney.
f) In case the subscriber requires including other personal circumstances, these shall be verified with official documents in accordance with the applicable regulation.

The subscriber may be waived of appearing before the Registration Authority in any of the following cases:

1. If the appropriate forms have been duly filled, and the signature of the subscriber has been legitimized before a notary, and certified copies of the identity, authorization and legal representation documents have been attached.

2. Online Procedure. The https://www.anf.es/en website includes an application form that should be filled and electronically sign with a qualified certificate, per the Spanish Law 59/2003, of December 19th, on Electronic Signature. The certificate used must has been issued by a CA approved by ANF AC.

***[1] 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 has verified the filiation data outlined in the Application Form are true: the address, telephone and e-mail.

The Declaration of Identity incorporates the identity of the declarant, his 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.

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

4.3.1.2 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:

1.- Per legal form:

- Trading companies and other legal persons which registration is required in the Mercantile Register, shall certify the valid incorporation by providing the authentic copy, the deed of incorporation registered in the Mercantile Registry, or certification issued by the Mercantile Registry.
  To prove the representation:
  - in the case of Administrators or the Board of Directors, an authentic copy of the deed of appointment registered in the Mercantile Registry or certification of the appointment issued by the Mercantile Registry,
  - in the case of Representatives, authentic copy of the power of attorney.

- The Associations, Foundations and Cooperatives shall certify their incorporation by providing original or certified copy of their incorporation certificate from the public registry where they are registered.

- Civil and other legal entities shall provide original or certified copy of the document that attests their incorporation irrefutably.

- Public Administrations and entities belonging to the public sector:

  - Entities which registration is mandatory in a Registry, they will certify their incorporation by providing original or certified copy of a certificate stating their incorporation data constitution and legal personality.

  - Entities created by a norm, shall provide the reference to such norm.

4.3.2 Approval or rejection of certificate applications

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

Moreover, he/she will determine:

- That the subscriber has had 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 duties and responsibilities of the CA, the subscriber, subject, those responsible for the certificate and relying parties, especially the CPS and Certification Policies.

- Shall monitor compliance with any requirement imposed by the legislation on data protection, as established in the security document included in the CPS, per the LOPD as provided in article 19.3 of the Spanish Law 59/2003, of December 19th, on Electronic Signature.

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

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

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

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

- The IRM shall verify the documentation provided by the subscriber and the Registration Authority.

- The validation process will be supported by the Legal and Technical Departments, which will review and technically validate the PKCS#10 certificate request.

- In the process of verification of the information and documentation received, the following means may be used:
    - Consultation of official public registries in which the entity must be registered to verify existence valid management positions and other legal aspects such as activity and date of incorporation.
    - National or regional Official Gazettes of public bodies to which public bodies or companies belong to.

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

4.3.3 Time to process certificate issuance

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

4.4 Certificate issuance

As defined in the CPS of ANF AC.

ANF AC will avoid generating certificates that expire after the CA's certificates that issued them.

4.4.1 Certification entity's actions during the certificate issuance process

As defined in the CPS of ANF AC.

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

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

4.4.2 Notification to subscriber

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

4.5 Certificate acceptance

4.5.1 Acceptance

As 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.

4.7.3.1 Certificate renewal of ones that have exceed 5 years from the initial identification.

The formalization of the application by handwritten signature of the subscriber is required, process done in-situ by the person concerned and using sufficient original documentation. The procedures may be performed before:

- **Recognized Registration Authority**, as defined in the CPS of ANF AC, are natural or legal persons who ANF AC has provided with the technology to perform the functions of a registry entity, having ratified the corresponding assumption of liabilities agreement and collaboration agreement.

- **Collaborating Registration Authority** as defined in the CPS of ANF AC, are people who, per current legislation, have powers of a public notary.

- **Trustworthy entity**, as defined in the CPS of ANF AC, are entities which per ANF AC, have the necessary capacity to determine the identity, capabilities, and freedom of action of the subscribers.

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 Revocation and suspension of certificates

Generally, as defined in the CPS of ANF AC.

4.9.1 Circumstances for revocation

Besides those defined in the CPS, ANF AC shall:

- Provide instructions and legal support for reporting complaints or suspicions regarding the compromise of the private key, of certificate misuse or about any type of fraud or misconduct.

- ANF AC shall investigate incidents of which they become aware within twenty-four hours of their receipt. The Security Manager, based on inquiries and verifications, shall issue a report to the Issuance Reports Manager, whom shall determine, if appropriate, the corresponding revocation in a substantiated minute, which shall include:

    - Nature of the incident.

- Received information.

- In the PSD2 certificates, if the Competent National Authority, 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 Competent National Authorities, to notify 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 applications

The revocation of a certificate may be requested by:

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

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

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

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

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

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

4.9.3 Procedure for revocation request

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

The revocation application shall contain at least the following information:

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

The revocation application shall be processed upon receipt.

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

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

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 these 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:

- 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.

4.9.4 Revocation request grace period

As defined in the CPS of ANF AC.

4.9.5 Maximun processing time of the revocation request

As defined in the CPS of ANF AC.

4.9.6 CRL lists verification requirements

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

4.9.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.9.8 On-line verification availability of the revocation

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

4.9.9 On-line verification requirements of the revocation

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

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

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

Access to this system is free.

4.9.10 Certificate suspension

Not applicable.

4.9.11 Suspension requests identification and authentication

Certificate suspension is not allowed.

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

6.1 Key pair generation and installation

As defined in the CPS of ANF AC.

6.2 Private key Protection

As defined in the CPS of ANF AC.

6.3 Other management aspects of key pair

As defined in the CPS of ANF AC.

6.4 Activation data

As defined in the CPS of ANF AC.

6.5 Informatic security controls

As defined in the CPS of ANF AC.

6.6 Life cycle technical controls

As defined in the CPS of ANF AC.

6.7 Network security controls

As defined in the CPS of ANF AC.

6.8 Time-stamping

As defined in the Time-Stamping Authority Policy and Practice Statement.

6.9 Cryptographic Module Security Controls

As defined in the CPS of ANF AC.

7 Certificates profiles, CRL and OCSP

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

Certificates which are issued as "qualified" comply with the standards:

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI) Certificate Profiles, Part 5: QCStatements
- ETSI TS 119 495 *(PSD2 Certificates)*
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

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

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

Within the certificates, besides the already standardized common fields, there are also included a group of "proprietary" fields which provide information in relation to the subscriber, or other information of interest.

Proprietary fields

Internationally unambiguous identifiers have been assigned. Specifically:

- Fields referenced with OID 1.3.6.1.4.1.18332.x.x are proprietary extensions of ANF AC. The complete list of OID codes and the information associated to the same may be consulted in the section "Proprietary fields of ANF AC" of the Certification Practice Statement of ANF AC.

- Fields with ISO/IANA of MPR 2.16.724.1.3.5.x.x, are proprietary extensions required and identified in the Identification and Electronic Signature Scheme v.1.7.6 published by the High Council of Electronic Administration.

- Fields with OID 1.3.6.1.4.1.18838.1.1 are proprietary of the Spanish State Tax Administration Agency (Agencia Estatal de Administración Tributaria "AEAT").

QCStatements

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

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

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

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

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

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

- **QcSSCD**, determines that the private key associated to the public key contained in the electronic certificate, is in a qualified signature creation device as defined in accordance with Annex II of the Regulation (UE) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing the Directive 1999/93/CE.

- **QcType**, when the certificate is issued with the profile (SIGNATURE), QcType 2 is outlined

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

The certificates issued by ANF AC of type PSD2, in addition to those previously mentioned, include PSD2QcType, in accordance with the provisions of ETSI TS 119 495 clause 5.1:

a) The function of the Payment Service Provider (PSP), which may be one or more of the following:
   - account service (PSP_AS);
   - initiation of payment (PSP_PI);
   - account information (PSP_AI);
   - issuance of card-based payment instruments (PSP_IC).

b) Name of the Competent National Authority where the PSP is registered. This information is provided in two forms: the full name string (NCAName) in English and an abbreviated unique identifier (NCAId).

Subject Alternative Name

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

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

7.1 Certificate Profiles

As defined in the technical background document.

7.2 CRL profile

As defined in the CPS of ANF AC.

7.3 OCSP profile

As defined in the CPS of ANF AC.

8 Compliance Audit

8.1 Frequency of compliance controls for each entity

As defined in the CPS of ANF AC.

8.2 Identification of the personnel in charge of the audit

As defined in the CPS of ANF AC.

8.3 Relationship between the auditor and the audited entity

As defined in the CPS of ANF AC.

8.4 List of items subject to audit

As defined in the CPS of ANF AC.

8.5 Actions to be taken because of a lack of compliance

As defined in the CPS of ANF AC.

8.6 Treatment of audit reports

As defined in the CPS of ANF AC.

9 General Provisions

9.1 Fees

As defined in the CPS of ANF AC.

9.2 Financial liability

As defined in the CPS of ANF AC.

9.3 Confidentiality of information

As defined in the CPS of ANF AC.

9.4 Privacy of personal information

As defined in the CPS of ANF AC.

9.5 Intellectual property rights

As defined in the CPS of ANF AC.

9.6 Obligations and guarantees

As defined in the CPS of ANF AC.

9.7 Disclaimers of guarantees

As defined in the CPS of ANF AC.

9.8 Limitations of liability

As defined in the CPS of ANF AC.

9.9 Interpretation and execution

As defined in the CPS of ANF AC.

9.10 Management of the CP

As defined in the CPS of ANF AC.