Certification Practice Statement (CPS)

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

Telephone: 902 902 172 (Calls from Spain)

International (+34) 933 935 946

Fax: (+34) 933 031 611 · Website: 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

Fax: (+34) 933 031 611. Web: www.anf.es/en/

Index

1 Introduction

ANF Certification Authority (hereinafter, ANF AC) is a corporate entity, constituted under Spanish Organic Law 1/2002 of March 22nd, and registered in the Spanish Ministry of Internal Affairs with national number 171.443 and VAT number G-63287510.

This document is ANF AC's Certification Practice Statement (CPS).

In accordance with article 19 of Spanish Law 59/2003, of December 19th, on Electronic Signature of Spain (LFE), this CPS details the general terms and conditions of ANF AC's certification services in relation to the management of the creation data, signature verification and extinction of certificates' validity; technical and organizational security measures; profiles and information mechanisms regarding the validity of certificates; and especially the verification processes to which data provided by subscribers is subjected in order to establish its veracity.

ANF AC protects its personal data files in accordance with the provisions of Spanish Law 15/1999, of December 13th, on the Protection of Personal Data (LOPD), Spanish Royal Decree 1720/2007 of December 21st, by which it is approved the implementing Regulation of the Spanish Organic Law 15/1999, of December 13th, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In accordance with article 19.3 of the Spanish Law 59/2003, this CPS is the security document for the purposes provided in the applicable legislation on data protection.

The Public Key Infrastructure (PKI) of ANF AC follows the directives 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 repealing Directive 1999/93/EC (hereinafter eIDAS), and Spanish Law 59/2003, of December 19th, on Electronic Signature of Spain (LFE).

The identification mechanisms offered by ANF AC are defined following the guidelines of Commission Implementing Regulation (EU) 2015/1502 of 8 September 2105 on setting minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

For the development of its activity, ANF AC has implemented an information security management system for the operation processes and maintenance of the infrastructure, issuance, validation, and revocation of electronic certificates per the ISO 27001 standard. ANF AC has the certifications ISO/IEC 27001 "Information technology - Security techniques - Information security management systems - Requirements", and 9001:2008 "Quality Management System".

This CPS constitutes a general compendium of standards applicable to the entire activity of ANF AC as Qualified Trust Service Provider, in accordance to eIDAS.

ANF AC issues various types of certificates, for which specific Certification Policies (CPs) exist. Consequently, the subscriber of any type of certificate must know this CPS and the CP that in each case is applicable for him/her to be able to request and use correctly the electronic certificate and the trust services provided by ANF AC. The provisions of the specific Certification Policies shall prevail over what is stated in this CPS.

In this CPS and related CPs, it is established the delimitation of responsibilities of the different parties involved, as well as the limitations of liabilities before potential damages.

ANF AC is certified per the WebTrust for EV under the guidelines for the issuance and management of Extended Validation SSL Certificates (CA/Browser Forum guidelines for the issuance and management of extended validation certificates). These guidelines, defined by the CA/Browser Forum, specify the minimum requirements to apply by Certification Authorities in order to issue EV-SSL certificates, with the aim of providing reliability in the identification and control of the identity of the services accessed.

ANF AC is adjusted to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published on https://www.cabforum.org. In the event of any inconsistency between this document and the requirements, the requirements shall prevail over this document, as long as these do not come into contradiction with legal norms.

ANF AC follows the ETSI (European Telecommunications Standards Institute) standards, among other reference standards: EN 319 411-1 for the issuance of certificates, EN 319 411-2 for the issuance of qualified certificates, and EN 319 421 for the issuance of timestamps.

This Certification Practice Statement assumes that the reader understands the PKI, certification, and electronic signature concepts. If this is not the case, the reader is recommended to study the above-mentioned concepts before continuing with this document.

1.1 Presentation

ANF AC, as a Qualified Trust Service Provider, manages a Public Key Infrastructures to provide the following qualified services:

- **Service of certification, issuance, revocation and renewal of qualified certificates**, and ordinary certificates without the legal consideration of qualified certificates, in accordance with Spanish Law 59/2003, of December 19th, on electronic signature.

- **Electronic time-stamp service**, which allows its users to obtain a guarantee that determines with complete certainty that the information existed at a specific moment of the time.

- **Service of creation, verification, and validation of electronic seals**.

- **Certificate Validation Service**, which allows its users and relying parties to verify the validity, integrity and authenticity of the certificates issued.
- **Electronic signature conservation service**, which aims to increase the reliability of electronic signature data beyond the technological validity period.
- **Certified electronic delivery service**, which allows the transmission of data between third parties by electronic means.
- **Website authentication service**, issuance of a web site authentication certificate.

The specifics related to each type of certificate issued by ANF AC are regulated in a specific Policy, published on the corporate website of ANF AC:

https://www.anf.es/en

ANF AC issues the following types of certificates:

TYPE	CERTIFICATE	STORAGE	OID IDENTIFIER
Natural Person Class 2	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.3.4.1.2.22
		HSM Token	1.3.6.1.4.1.18332.3.4.1.4.22
	Authentication	In all cases	1.3.6.1.4.1.18332.3.4.1.1.22
	Encryption	In all cases	1.3.6.1.4.1.18332.3.4.1.3.22
	Centralized service	HSM Token	1.3.6.1.4.1.18332.3.4.1.5.22
Legal Representative of a Legal Person	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.2.5.1.3
		HSM Token	1.3.6.1.4.1.18332.2.5.1.10
	Authentication	In all cases	1.3.6.1.4.1.18332.2.5.1.1
	Encryption	In all cases	1.3.6.1.4.1.18332.2.5.1.2

	Centralized service	HSM Token	1.3.6.1.4.1.18332.2.5.1.14
Legal Representative for Sole and Joint and Several Directors	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.2.5.1.9
		HSM Token	1.3.6.1.4.1.18332.2.5.1.12
	Authentication	In all cases	1.3.6.1.4.1.18332.2.5.1.7
	Encryption	In all cases	1.3.6.1.4.1.18332.2.5.1.8
	Centralized Service	HSM Token	1.3.6.1.4.1.18332.2.5.1.13
Legal Representative of an Entity without Legal Personality	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.2.5.1.6
		HSM Token	1.3.6.1.4.1.18332.2.5.1.11
	Authentication	In all cases	1.3.6.1.4.1.18332.2.5.1.4
	Encryption	In all cases	1.3.6.1.4.1.18332.2.5.1.5
	Centralized Service	HSM Token	1.3.6.1.4.1.18332.2.5.1.15
Public Employee	High Level Signature	HSM Token	1.3.6.1.4.1.18332.4.1.3.22
	High Level Authentication	HSM Token	1.3.6.1.4.1.18332.4.1.1.22
	High Level Encryption	HSM Token	1.3.6.1.4.1.18332.4.1.4.22
	Medium Level	Soft Token. Cryptographic	1.3.6.1.4.1.18332.4.1.2.22
Public Administration Electronic Seal	High Level	HSM Token	1.3.6.1.4.1.18332.25.1.1.3
	Medium Level	Soft Token. Cryptographic	1.3.6.1.4.1.18332.25.1.1.2
Electronic Seal	Signature	HSM Token	1.3.6.1.4.1.18332.25.1.1.1

		Soft Token. Cryptographic	
RA Operator	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.22.1.3.22
		HSM Token	
	Authentication	Soft Token. Cryptographic	1.3.6.1.4.1.18332.22.1.1.22
		HSM Token	
	Encryption	Soft Token. Cryptographic	1.3.6.1.4.1.18332.22.1.2.22
Issuance Reports Manager	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.4.22
		HSM Token	
	Authentication	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.1.22
		HSM Token	
	Encryption	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.3.22
PKI Operator	Signature	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.6.22
		HSM Token	
	Authentication	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.2.22
		HSM Token	
	Encryption	Soft Token. Cryptographic	1.3.6.1.4.1.18332.23.1.5.22
Secure Server SSL		Soft. Cryptographic	1.3.6.1.4.1.18332.55.1.1.1.22
EV Secure Server SSL		Soft. Cryptographic	1.3.6.1.4.1.18332.55.1.1.2.22
Electronic Headquarters	High Level	HSM Token	1.3.6.1.4.1.18332.55.1.1.4.22
	Medium Level	Soft. Cryptographic	1.3.6.1.4.1.18332.55.1.1.3.22
Electronic Headquarters	High Level	HSM Token	1.3.6.1.4.1.18332.55.1.1.6.22
	Medium Level	Soft. Cryptographic	1.3.6.1.4.1.18332.55.1.1.5.22

The specifics related to each type of certificate, per its OID, are regulated in the Specific Policy for each certificate, published on the corporate website of ANF AC:

https://www.anf.es/en

1.2 Identification

ANF Certification Authority uses Object Identifiers (OID) defined in the ITU-T Rec. X.660 and 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 company private 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-)*.

To individually identify each type of certificate issued in accordance with the present Certification Practice Statement, and the Certification Policy to which it is subjected, an object identifier (OID) is assigned. This OID appears in the corresponding section of the "CertificatePolicies" and begins with the following sequence:1.3.6.1.4.1.18332.

The certificate profile document can be consulted in:

https://www.anf.es/en

Furthermore, per the definition of the ETSI EN 319 412-5, the following identifiers are included:

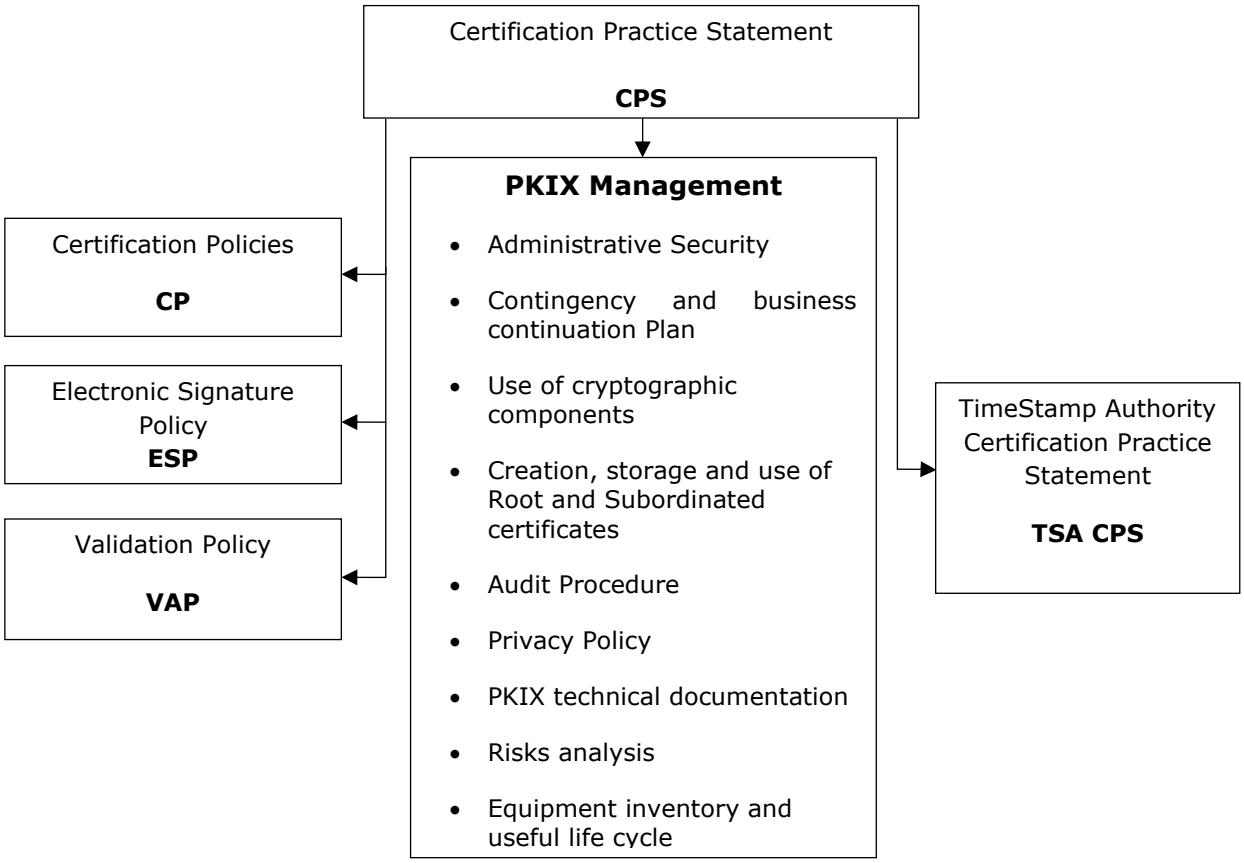
- QcCompliance: qualified certificate per eIDAS
- QcSSCD: certificate issued in a qualified signature creation device
- QcRetentiodPeriod: retention period of documentation
- QcPDS: route to the usage conditions
- Qctype: indicates the type of signature per eIDAS (seal, signature, web)

1.2.1 Document name

This document is known as ANF AC's Certification Practice Statement, hereinafter shall be cited by its acronym "CPS".

1.2.2 Document structure

The document structure of the Policies, the CPS and other documents related to ANF AC's certification services is described in the following scheme:



1.2.3 OID identifiers

The meaning of the OID with the arc "1.3.6.1.4.1.18332.1.9.1.1" is the following:

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- ANF Certification Authority (18332)
- Certification Practice Statement (1.9.1.1)

1.2.4 Specifications

Document name	Certification Practice Statement of ANF AC
Version	23

Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18332.1.9.1.1
Publication date	March 22nd, 2017
Expiration date	Not applicable
Location	https://www.anf.es/en/

This document has as an objective to determine the means and procedures that ANF AC uses to meet the requirements and levels of security imposed by the Certification Policies. The conditions of use, limitations, responsibilities, properties, and any other information that is considered specific of each type of certificate, is reflected in each of the Certification Policies to which its respective issuance is submitted.

The Governing Board of the PKI is responsible for the administration of this CPS and the Certification Policies of ANF AC. The date of publication is the date of entry into force.

The publication of a new document entails the repeal of the previous one. The identifier of this document will only be changed if there are substantial changes that affect its applicability.

1.3 PKI Parties

1.3.1 Intervening persons and entities

- Certification Entity
  - Certification Services Provider
  - PKI Governing Board
- Certification Authority
  - Root Certification Authority
  - Intermediate Certification Authorities
  - Associated CA (International Mutual Recognition Agreements)
- Issuance Reports Managers
- Recognized Registry Authority
- Certificates Issuance Managers
- Validation Authority
- Time Stamp Authority
- End entities
  - Subscribers
  - Subjects
  - Relying Parties

1.3.1.1 Certification entity

ANF Autoridad de Certificación (hereinafter, ANF AC) with registered office in Paseo de la Castellana, 79, Madrid (28046) Spain, and VAT number G-63287510

1.3.1.1.1 Trust Service Provider (TSP)

ANF AC is the Qualified Trust Service Provider (QTSP) of this PKI, which provides qualified trust services to which this CPS is applied.

ANF AC is responsible that the CA Hierarchies, which constitute its public key infrastructure, comply with what is established in the CPS and addendum.

1.3.1.1.2 PKI Governing Board

The Governing Board of ANF AC's PKI is the body that manages executively the PKI and is responsible for the approval of this Certification Practice Statement and Policies that conform its addendum, as well as their compliance to applicable law, technical standards that affect this subject, and their harmonization with the Certification Policies.

1.3.1.2 Certification Authority

It is the trusted authority of the users of the certification services (for example, subscribers, subjects and relying parties), which creates and assigns certificates, and it's called Certification Authority (CA). The CA has the overall responsibility for providing trusted services, which is identified in the certificate as issuer, and whose private key is used to sign certificates.

The CA may use other parties to provide certification services. However, the CA always maintains the overall responsibility and ensures that regulatory requirements, both technical and legal, are met.

ANF AC, as Qualified Trusted Services Provider, has a hierarchy of CAs, and ensures that subordinate CAs comply with regulatory requirements, both technical and legal.

ANF AC has the following Certification Authorities,

- Root Certification Authority
- Intermediate Certification Authorities

1.3.1.2.1 Root Certification Authorities

This is the root entity whose public key certificate has been self-signed. It issues intermediate

certification authorities' certificates. In the scope of the PKI, it is the part in which ANF AC currently has the following Root Certification Authorities:

CN Root Certificate = **ANF Global Root CA** with serial number 01 64 95 ee 61 8a 07 50, which expires on May 15th, 2036.

The identification data of this Root Certificate is:

With SHA-256 algorithm:

Serial Number	01 64 95 ee 61 8a 07 50
Subject	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Validity Period	From 2016-05-20 to 2036-05-15
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	fc 98 43 cc 99 22 61 50 01 a1 73 74 ce 8a 3d 79 58 0f ea 51

This certificate was issued to replace the Root Certificate with CN = **ANF Global Root CA** issued with SHA-256 with serial number 01 3f 2f 31 77 e6 that expires on June 5th, 2033. The PKI's Governing Board on January 1, 2017, approved the creation of a centralized certificate platform. This system will allow access to centralized signature services using qualified electronic signature devices, based on centralized qualified electronic certificates.

The certificate was issued without renewal of keys, and it's valid until its expiration date. It uses the same private key, the same public key, and the same CA name. This certification model with shared key is called "Cross-Certification" *[1].

Whenever possible, it will gradually be abandoned, and in an amicably manner with the institutions that have it approved, the use of the hierarchy with expiration 2033.

*[1] *The "Cross-Certification" is a mechanism that allows creating multiple certification paths. In this case, it is used for a single certificate to be validated interchangeably in two certification hierarchies ending in different CA roots. (See "RFC4949: Internet Security Glossary, Version 2": cross-certification).*

The identification data of the CN root certificate = **ANF Global Root CA** with expiration date June 5th, 2033, are:

With SHA-256 algorithm:

Serial Number	01 3f 2f 31 77 e6
Subject	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Validity Period	From 2013-06-10 to 2033-06-05
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	26 ca ff 09 a7 af ba e9 68 10 cf ff 82 1a 94 32 6d 28 45 aa

- CN Root Certificate = **ANF Server CA** with Serial Number 01 34 4b, which expires on December 1st, 2021.

The identification data of this Root Certificate are:

Serial Number	01 34 4b
Subject	CN = ANF Server CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Validity Period	From 2009-12-01 to 2021-12-01
Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Fingerprint	ce a9 89 0d 85 d8 07 53 a6 26 28 6c da d7 8c b5 66 d7 0c f2

This certificate was issued to replace the CN Root Certificate = **ANF Server CA** with Serial Number: 29, which expired on April 3rd, 2015.

CN Root Certificate = **ANF Server CA** with Serial Number 29, which expired on April 3rd, 2015 replaced, with key renewal, the root certificate that expired on February 1st, 2010.

The identification data of this Root Certificate is:

Serial Number	29
Subject	CN = ANF Server CA SERIALNUMBER = G-63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Validity Period	From 2005-04-05 to 2015-04-03
Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	b5 f8 84 ad eb 80 d6 9b 20 3e e3 91 01 21 1f 47 fa 77 44 59

- CN Root Certificate **=ANF Root CA** with serial number: 05 which expired on February 26th, 2015.

The identification data of this Root Certificate are:

Serial Number	05
Subject	CN = ANF Root CA SERIALNUMBER = G-63287510 OU = ANF Public Primary Certification Authority O = ANF Autoridad de Certificacion C = ES
Validity Period	From 2005-02-28 to 2015-02-28
Public Key	RSA (2048 Bits)
Signature Algorithm	sha512RSA
Fingerprint	d6 06 de eb 90 05 f5 f0 8c de d2 a9 5e 46 37 24 d6 90 8a b5

- The CN Root Certificate**= ANF Server CA** with Serial Number: 01 which expired on February 1st, 2010. This certificate was replaced by a new Root Certificate, with expiration date 2015, with key

renewal.

The identification data of this Root Certificate is:

Serial Number	01
Subject	CN = ANF Server CA SERIALNUMBER = G-63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificación C = ES
Validity Period	From 2000-02-01 to 2010-02-01
Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Fingerprint	a3 05 94 e9 3c f3 90 49 53 71 37 e2 5d cf 8d c0 c6 90 9d b1

1.3.1.2.2 Intermediate Certification Authorities

They are the entities, that within the certification hierarchy, issue end-entity certificates, and whose public key certificate has been digitally signed by the Root Certification Authority.

All Intermediate Certification Authorities (iCA) can issue OCSP Responder certificates. This certificate is used to sign and verify the responses of the OCSP service on the status of the certificates issued by these CAs. The OID of the certificates issued by each Intermediate Certification Authority for the issuance of OCSP responder certificates is 1.3.3.1.4. 1.18332.56.1.1

ANF Global Root CA, which expires on 2036, currently has the following Intermediate Certification Authorities:

- **ANF Assured ID CA1**

  With SHA-256 algorithm:

Serial Number	07 71 c1 14 00 1a e5 00

Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF Assured ID CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de Identidad O = ANF Autoridad de Certificacion C = ES
Validity	From the 2016-05-20 to 2026-05-18
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Fingerprint	cb df 3e 06 86 f1 b1 c1 f8 83 49 41 69 ef ed 52 f6 94 14 b9

This certificate was issued to replace the CN intermediate CA certificate = **ANF Assured ID CA1** issued with SHA-256 with serial number: 06 40 0c a5 29 ce 79 80 that expires on February 29th, 2024.

This certificate was issued without renewal of keys, and it is valid until its expiration date. It uses the same private key, the same public key, and the same name of CA. This certification model with shared key is called "Cross-Certification".

Whenever possible, it will gradually be abandoned, and in an amicably manner with the institutions that have it approved, the use of the hierarchy with expiration 2033.

The Intermediate Certification Authority **ANF Assured ID CA1** issues end entity electronic certificates of identity stored in HSM token, cryptographic software and centralized device.

- **ANF High Assurance AP CA1**

With SHA-256 algorithm:

Serial Number	0c 68 fc 7d c4 8d 83 80

Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance AP CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de AP O = ANF Autoridad de Certificacion C = ES
Validity	From 2016-05-20 to 2026-05-18
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	1e 8f 04 25 22 80 bb 73 f4 51 ec 45 8d 87 b5 b8 0e a6 e1 a1

This certificate was issued to replace the CN intermediate CA certificate = **ANF High Assurance AP CA1** issued with SHA-256 with serial number: 0a aa dc 2e eb a2 92 00 which expires on February 29th, 2024.

This certificate was issued without renewal of keys, and is valid until its expiration date. It uses the same private key, the same public key, and the same name of CA. This certification model with shared key is called "Cross-Certification".

Whenever possible, it will gradually be abandoned, and in an amicably manner with the institutions that have it approved, the use of the hierarchy with expiration 2033.

Intermediate Certification Authority **ANF High Assurance AP CA1** issues end-entity electronic certificates for Public Administrations.

- **ANF High Assurance EV CA1**

With SHA-256 algorithm:

Serial Number	06 5d 66 65 46 a4 59 00
Issuer	CN = ANF Global Root CA

	SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance EV CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia Tecnicos O = ANF Autoridad de Certificacion C = ES
Validity	From 2016-05-20 to 2026-05-18
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	67 93 9b 3c a7 7e 5f 6f de c0 7e c9 63 71 a8 7c 77 19 79 62

This certificate was issued to replace the CN intermediate CA certificate = **ANF High Assurance EV CA1** issued with SHA-256 with serial number: 0b e6 86 56 59 db bc 00 which expires on February 29th, 2024.

This certificate was issued without renewal of keys, and is valid until its expiration date. It uses the same private key, the same public key, and the same name of CA. This certification model with shared key is called "Cross-Certification".

Whenever possible, it will gradually be abandoned, and in an amicably manner with the institutions that have it approved, the use of the hierarchy with expiration 2033.

Intermediate Certification Authority **ANF High Assurance EV CA1** issues technical electronic certificates for authentication services SSL, EV SSL, Encryption, Code Signature and TSU Electronic Time Stamp.

- **ANF Global CA1**

With SHA-256 algorithm:

Serial Number	06 6b 6d 11 a4 5f c1 80

Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF Global CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia PKI O = ANF Autoridad de Certificacion C = ES
Validity	From 2016-05-20 to 2026-05-18
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	bb a1 aa 14 07 d4 1f 68 d3 e0 39 78 a3 de 20 d8 95 40 61 b2

This certificate was issued to replace the CN intermediate CA certificate = **ANF Global CA1** issued with SHA-256 with serial number: 00 ba 8e 3c 10 62 ff 18 which expires on February 29th, 2024.

This certificate was issued without renewal of keys, and its valid until its expiration date. It uses the same private key, the same public key, and the same name of CA. This certification model with shared key is called "Cross-Certification".

Whenever possible, it will gradually be abandoned, and in an amicably manner with the institutions that have it approved, the use of the hierarchy with expiration 2033.

Intermediate Certification Authority **ANF Global CA1** issues electronic certificates for the management and administration of ANF AC's PKI.

ANF Global Root CA, with expiration date 2033, currently has the following Intermediate Certification Authorities:

- **ANF Assured ID CA1**

  With SHA-1 algorithm:

Serial Number	01 40 15 8c d1 bc
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF Assured ID CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de Identidad O = ANF Autoridad de Certificacion C = ES
Validity	From 2013-07-25 to 2023-07-23
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	60 14 72 d6 58 ce 79 25 fd 81 ae 46 05 4c a3 42 de 11 2e 8b

With SHA-256 algorithm:

Serial Number	06 40 0c a5 29 ce 79 80
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF Assured ID CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de Identidad O = ANF Autoridad de Certificacion C = ES
Validity	From2014-03-03 to 2024-02-29
Public Key	RSA (4096 Bits)

Signature Algorithm	Sha256RSA
Digital Fingerprint	ab da 03 79 f0 2e ba e8 2e fb 93 41 f2 ad d6 c0 14 9b 58 14

Intermediate CA **ANF Assured ID CA1** issues end entity electronic certificates of identity in accordance with what is established in the Spanish Law 59/2003, December 19th, 2003.

- **ANF High Assurance AP CA1**

With SHA-1 algorithm:

Serial Number	01 40 15 92 25 0a
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance AP CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de AP O = ANF Autoridad de Certificacion C = ES
Validity	From 2013-07-25 to 2023-07-23
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	e9 cd c2 dd 9a 82 38 c2 46 35 90 d9 46 49 47 ef 56 52 da d0

With SHA-256 algorithm:

Serial Number	0a aa dc 2e eb a2 92 00

Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance AP CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia de AP O = ANF Autoridad de Certificacion C = ES
Validity	From 2014-03-03 to 2024-02-29
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	68 d1 5d a0 1c 93 dc 54 2a 3c 7b 6d c0 19 35 68 78 bd 31 61

Intermediate CA **ANF High Assurance AP CA1** issues end entity electronic certificates for Public Administrations.

- **ANF High Assurance EV CA1**

With SHA-1 algorithm:

Serial Number	01 40 15 93 1e 6b
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES

Subject	CN = ANF High Assurance EV CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia Tecnicos O = ANF Autoridad de Certificacion C = ES
Validity	From 2013-07-25 to 2023-07-23
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	b6 80 2f ad b3 e6 f9 fc 06 89 20 79 c6 af 35 0a f9 b7 a4 bf

With SHA-256 algorithm:

Serial Number	0b e6 86 56 59 db bc 00
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance EV CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia Tecnicos O = ANF Autoridad de Certificacion C = ES
Validity	From 2014-03-03 to 2024-02-29
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	ce e5 c6 6f 66 21 7b 2f ec ba e4 04 87 66 3a 5b 5a 0c 2a 49

Intermediate Certification Authority **ANF High Assurance EV CA1** issues technical electronic certificates for authentication services SSL, EV SSL, Code Signature, Encryption and TSU Electronic Time Stamp.

- **ANF Global CA1**

  With SHA-1 algorithm:

Serial Number	01 40 15 8f 88 d6
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF Global CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia PKI O = ANF Autoridad de Certificacion C = ES
Validity	From 2013-07-25 to 2023-07-23
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	18 21 7f f3 df 4e af 55 56 82 01 75 4c 83 83 97 da 38 71 9e

With SHA-256 algorithm:

Serial Number	00 ba 8e 3c 10 62 ff 18
Issuer	CN = ANF Global Root CA SERIALNUMBER = G63287510 OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES

Subject	CN = ANF Global CA1 SERIALNUMBER = G63287510 OU = ANF Autoridad Intermedia PKI O = ANF Autoridad de Certificacion C = ES
Validity	From 2014-03-03 to 2024-02-29
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Digital Fingerprint	50 95 4d 42 a9 5e 39 e7 d6 1f a0 7a 6f 9c 5f 46 50 06 e9 e9

Intermediate Certification Authority **ANF Global CA1** issues electronic certificates for the management and administration of the ANF AC PKI.

ANF Server CA, with expiration date on 2021, has the following Intermediate Certification Authorities:

- **ANF EC 1**

Serial Number	01 6a d0
Issuer	CN = ANF Server CA OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF EC 1 OU = ANF Autoridad Intermedia O = ANF AC C = EC
Validity	Valid from Monday, December 20th, 2010 16:43:21 To Saturday, November 27th, 2021 16:43:21
Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	8d eb ff fb 15 66 c6 2b e2 e4 46 7b b7 07 10 41 3d d6 b1 bd

Intermediate Certification Authority **ANF EC 1** issues end entity electronic certificates for Ecuador.

- **ANF SSL Sede CA1**

Serial Number	07 ae 2d
Issuer	CN = ANF Server CA OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF SSL Sede CA1 OU = CA Intermedia SSL Sede O = ANF Autoridad de Certificacion C = ES
Validity	Valid from 2010-20-12 to 2020-17-12
Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	c1 5a 0c f3 be e2 25 f0 78 aa b2 41 8b da 98 ab 36 81 9d 49

Intermediate Certification Authority **ANF SSL Sede CA1** issues electronic certificates for SSL and Electronic Headquarters.

- **ANF High Assurance EV CA1**

Serial Number	03 8b 16
Issuer	CN = ANF Server CA OU = ANF Clase 1 CA O = ANF Autoridad de Certificacion C = ES
Subject	CN = ANF High Assurance EV CA1 OU = CA Intermedia SSL Sede EV O = ANF Autoridad de Certificacion C = ES
Validity	Valid from 2010-20-12 to 2020-17-12

Public Key	RSA (2048 Bits)
Signature Algorithm	Sha1RSA
Digital Fingerprint	a2 ee 86 d1 88 2c 29 23 10 49 59 8b 19 f5 05 bc 95 35 c7 8b

Intermediate CA **ANF High Assurance EV CA1** issues electronic certificates for SSL with Extended Validation.

- Intermediate CAs of **ANF Root CA** root have ceased issuing certificates. There are currently no valid certificates issued by this intermediate CA.

- Intermediate CAs of **ANF Server CA** which expired on **2015**, have ceased issuing certificates. There are currently no valid certificates issued by this intermediate CA.

- Intermediate CAs of **ANF Server CA:**

  - **ANF Cripto SubCA1**

  - **ANF ES CA1**

  have ceased issuing certificates. There are currently no valid certificates issued by this intermediate CA.

1.3.1.3 Registration Authorities

This Certification Practice Statement applies to the Registration Authorities that ANF AC employs to attend in-situ subscribers of certificates.

The Registration Entities carry out the tasks of the identification of the subscribers and holders of the keys of the certificates, the verification, and the certified digitization of the supporting documentation of the circumstances that appear in the certificates, as well as the revocation and the procedures of the renewal of certificates.

1.3.1.3.1 Recognized Registration Authorities

These are legal or natural persons to whom ANF AC has provided with the necessary technology to carry out the functions of a registration authority, after formalizing the corresponding assumption of responsibilities and collaboration agreement.

To perform their duties. The registration entities carrying out these functions use natural persons who have completed the training course of "RA Operator" of ANF AC, and have passed the training tests as "RA Operator"; it is a mandatory requirement for the performance of these duties. The RA Operators of the Recognized Registration Authority are under the supervision, control, and management thereof, and are of their sole responsibility.

ANF AC entrusts these officially recognized operators with identifying and verifying the personal circumstances of certificate subscribers.

With this objective, the operators:

- Guarantee that the application is made in person by the persons involved in the application, custody of use of the certificate requested.
- Guarantee that the documents provided for identifying and verifying the representation capacity are originals and sufficient for performing this process.
- To the extent of their possibilities, they ensure that:
    - the subscriber, and any other intervening party in the application process, performs it without coercion;
    - the subscriber, and any other intervening party in the application process, are of legal age and have mental capacity to act;
    - the subscriber, and any other intervening party in the application process, have sufficient intellectual capacity to assume the responsibility and correct use of the certificates and associated instruments that are requested.
- Deal with requests and clarify doubts on any queries in relation that are asked.
- Put at the disposal of the subscriber, and any other intervening party in the application process, the CPS, the corresponding Certification Policies, Electronic Signature Policy, and service fees, as well as information related with the renewal and revocation processes: causes, obligations and procedure.
- Inform the subscribers of the exact conditions for the usage of the certificate and its limitations.
- Verify that the data owner gives his consent to the use of the personal data, and is informed about the purpose it is going to be given and regarding its storage in the file declared by ANF AC, as well as his/her rights of access, rectification, cancellation, and opposition, and how to exercise said rights.
- Physically provide the Electronic Signature Cryptographic Device to the subscriber, among other utilities, for:

- The generation of the key pair,
- The generation of the activation data;
- The generation of the request certificate;
- The connection to the trusted ANF AC servers through a secure communications protocol;
- The certificate download once it has been issued, the generation of electronic signature;
- The electronic signature and the carrying out of verification processes;
- The authentication processes before computer applications, and encryption processes;

This device gives the user access, storage, control and management of their certificates and private keys. As such, its destruction implies the destruction of the certificate and its keys.

- Deliver to the subscriber their identification certificate, electronically signed by the RA operator.
- Verify that all documentation submitted by the subscriber, and any other intervening party in the application process, is original, obtaining a copy of the same which is signed electronically by the RA operator. This documentation, along with other information collected and compiled by the RA operator (application form, statement of identity, biometrics...etc.), constitutes the "application file". The application file is sent, by electronic means, to ANF AC's trusted servers.

  The process of digitalization and transmission of the application file is made by the "RA Manager" application of ANF AC, which guarantees the security and privacy of information. The RA Manager incorporates the following security measures for the correct completion of the forms:

  - It verifies that e-mail addresses given are properly formatted, and its validity is verified.
  - It does not allow the e-mail address of the certificate to be the same as the RA Operator.
  - It verifies that the tax identification number is properly formatted.
  - It verifies that the National/Foreign Citizens ID card is properly formatted, and if appropriate, the Passport number.
  - It verifies that the bank accounts listed are properly formatted.
  - It verifies that the necessary documents are attached, per the certificate type requested.
  - All alphanumeric fields are capitalized, except for electronic mail addresses and URLs.
  - It is not allowed the introduction of blanks at the beginning or end of any displayed value, as well as several blank spaces in a row.

- At the end of the application process, the RA Operator generates and signs the Identification Minute, transferring it to the Electronic Signature Cryptographic Device, and generating in paper the Activation Letter; all of which is given to the certificate subscriber. These documents contain:
    - The Identification Minute incorporates in a structured manner, all the information that enables the subscriber to elaborate the PKCS #10 Certificate petition. This Minute is previously encrypted with double key.
    - The Activation Letter contains one of the passwords necessary to decipher the Identification Act. The second password is sent by e-mail to the account given in the application.
- Based on the accredited data, they proceed to:
    - Complete the certificate application form and the subscription agreement.
    - Print these documents, which will be signed in manuscript form by the RA operator who performs the process and by the subscriber; one of these documents is the Certificate Application Form.
    - Submit to ANF AC all the documentation for the processed application.
    - Generate the Identification Minute.

ANF AC has initiated a technological renewal plan that includes the incorporation of new identification instruments, specifically:

- Subscriber's image capture.
- Subscriber's fingerprint capture
- National/Foreign Citizens ID card reader that incorporates authenticity validator.

Those RRA already equipped with these instruments, assume the obligation of carrying out the corresponding processes of biometric data capture and validation of National/Foreign Citizens ID cards, always with express authorization from the user to process and transmit this information to ANF AC's Trusted Servers.

Once documents are formalized, the subscriber must be provided with:

- Signature Creation Data Generation Device.
- Electronic Signature Creation Device.
- Verification Device.

- Identification Minute which allows the generation of the "requested certificate".
- Activation Keys of the minute.

The certificate application form is a document in which the subscriber agrees to an explicit statement of his knowledge on the use of the Electronic Signature Device and Electronic Certificate, as well as the duties, limitations, and obligations as a user of the same. The obligations referred to are:

- Generating the signature creation data without third party mediation, and that only the user knows the activation password.
- Understanding the obligations of safeguarding the signature data creation and activation password.
- Knowing the means for reporting the loss or potential misuse of certificate data and electronic signature, as well as the obligation to revoke the certificate if such event occurs.
- Understanding how to use the certification device that has been delivered.

The Certificate Application forms, of the corresponding certificates can be found on the following link:

https://www.anf.es/en

In the case of delivery of a cryptographic device that incorporates biometric reader, the Recognized Registration Authority must ensure that, in its presence, the subscriber proceeds to identify himself/herself before the device with his/her fingerprints. With this method, the device becomes activated and personalized. Only the subscriber may, after undergoing the corresponding biometric verification, activate the certification system.

It should also be required, prior to the execution of the request for issuance of the certificate, that a reading of their Rights and Obligations be performed, answering any doubts the subscriber may have. The certificate issuance request cannot be formalized until the subscriber considers that he/she has full understanding of the documents. With the signing of the certificate application form, the subscriber acknowledges that he/she understands and accepts all the Rights and Obligations set forth in this PKI.

In any case, if the RA Operator deems that the consultations held by the subscriber fall outside the scope of his/her knowledge or obligations, or fails to resolve the doubts that may arise, he/she will instruct the subscriber to contact ANF AC's Customer Service Office, which shall freely assist and provide the advice required.

The RRA assumes the obligation to revoke the certificates processed, or to deny a pending certificate whenever:

- It is known that the circumstances of the holder or legal representative, where appropriate, have changed.
- It is known that there has been a breach affecting the safety of the signature creation data.

- In any case where he/she considers that its validity can adversely affect the reliability of ANF AC's PKI; its use is not framed in good faith; or it is used to the detriment of third parties or in illegal operations.

The assessment criteria that follows the RRA on the documentation submitted by the subscriber to prove his/her identity or other data to be included in the certificate, are those normally accepted in Law. The Recognized Registry Authority always requires the physical presence of the subscriber.

All processing made by the RRA are electronically signed by the operators performing them, thus taking full responsibility for the process.

The RRA have the authorization to charge the fees of identification, application, activation, and inclusion of attributes in the requested certificate.

The final assessment of the adequacy or otherwise of the investigation carried out by the RRA, as well as the documents provided, shall be always be performed by staff of ANF AC.

Once the certificate is issued, the Registration Authority receives an acknowledgment of the issuance via e-mail.

1.3.1.3.2 Collaborating Registration Authorities

These are persons who, in accordance with the applicable legislation, have the powers of a public notary.

1.3.1.3.3 Trustworthy entities

These are in-situ verification offices under the authority of a Recognized Registration Authority. They have the necessary capacity to determine the identity, capacity, and freedom of action of the subscribers. Their intervention shall be carried with physical presence of the subscriber, comparing original documents with copies thereof provided by the user, or information included on processing forms.

The subscriber shall sign on paper the processing forms. The Trustworthy Entity will issue and sign a Certificate of Proof of Life. The original documentation shall be submitted to the Issuance Report Manager (IRM).

The Issuance Report Manager will assess the adequacy of the capacity of the Trustworthy entity based on their prestige, independence, and prior relationship it may have with the user. It can order new arrangements, inquiries or even reject the processing performed for insufficient guarantees.

The intervention of Trustworthy Entities is limited to the renewal process of electronic certificates which may have passed, or not, the term of 5 years from the initial identification process.

1.3.1.4 Issuance Report Managers

These are staff assigned to ANF AC's Legal Department, responsible for verifying the documentation provided by the Registration Authorities. They determine whether the documents are sufficient or not, they verify the reliability of the information provided by the subscriber, and, if they consider it necessary, order further investigations.

The Issuance Report Managers will determine the need for completing these verifications in each case through telecommunication consultations directly with the registries, or through third party services.

The Issuance Report Managers' responsibilities are to:

- Ensure that the certificate application contains verifiable and complete information.
- Verify that the application meets all the corresponding CP requirements per the certificate requested.
- Verify the powers of attorney and public deeds.
- Verify that all the documents have been signed, and that all formalities demanded by this CPS and its corresponding certification policies have been met.
- Analyze powers of attorney and other public documents.
- Verify that information contained in the certificate is exact and that no typing errors have been made.
- Verify that all the information included in the certificate is exact, and no typewriting errors have been made.
- Verify that all the information required has been included and, if information which is not required is included, that the subscriber authorizes its inclusion in the certificate.
- Apply the corresponding cryptographic verification process on the requested certificated to verify the integrity of the certificate's contents and that the signing party is in possession of the signature creation details.

Based on all the tasks performed, the Issuance Report Managers decides:

- To issue the certificates, generating and signing a favorable issuance report, or
- Refuse to the issuance, generating an unfavorable report, or
- requesting further accrediting documents or the signature of complementary certificates.

1.3.1.5 Certificate Issuance Managers

There is a minimum of three operators who have the capacity to access and activate ANF AC's certificate issuance devices.

To activate the issuance service, the presence of at least two of these operators is required.

1.3.1.6 Validation Authority

A Validation Authority is a Certification Services Provider which provides certainty on the validity of electronic certificates.

ANF AC is a Validation Authority (VA) which acts as a trusted third party, validating electronic certificates.

ANF AC manages an IT system formed by a combination of Trusted Servers, that access in real time the status of all certificates issued by ANF AC.

These servers are given the name of OCSP Responder and answer validation requests through the Online Certificate Status Protocol (OCSP). They determine the status of an electronic certificate and all its trust chain, issuing a signed validation report. The repositories that access the OCSP Responder servers are permanently kept up to date and comply with IETF RFC 6960, Online Certificate Status Protocol Algorithm Agility.

OCSP requests can be performed 24/7/365 completely free. These requests must be made in accordance with IETF RFC 6960. This validation process is complementary to the publication of the Certificate Revocation Lists (CRLs) and the AEAT web service.

1.3.1.7 Time Stamp Authority

A Time Stamp Authority is a Certification Services Provider which provides certainty about the existence of certain electronic documents before a given moment in time. The Time Stamping Authority signs the time stamp of such moment, along with the hash of the associated document.

ANF AC is a Time Stamp Authority (TSA) which manages an IT System formed by a combination of Trusted Services whose time system is synchronized with a safe time source.

These servers are given the name Time Stamp Units (TSU), and their function is to stamp electronic time stamps on requests made by ANF AC's users. They allow to determine the existence of a certain object in time.

The ANF AC Time Stamping Services are specified in the TSA CPS with OID 1.3.6.1.4.1.18332.5.1.1, and comply with the IETF RFC 5816, updated by RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) and RFC 3339 Date and Time on the Internet: Timestamps standards.

1.3.1.8 End entities

These are the natural persons and organizations that are the target of the issuance, management and use of electronic certificates services

The final entities of this PKI are:

- Subscriber
- Subject
- Relying Parties

1.3.1.8.1 Subscriber

These are the natural persons, with full legal capacity to act, in their own name or on behalf of third parties, that request to the Certification Authority the issuance of a certificate and with whom they sign the subscription agreement. In case of assuming the representation of a third party, this representation must be supported with powers of attorney, with the sufficient scope for legal purposes, and in case of being the representative of a legal person, the powers of attorney must be inscribed in the corresponding registry.

Article 6.2 of the Spanish law 59/2003, of electronic signature, alludes to the signatory, who, in agreement with ETSI EN 319 411, is the subscriber.

> *"The signatory is the person who has a signature creation device and acts in his own name or on behalf of a natural or legal person that he represents."*

The Subscribers are responsible before the CA for the use of the private key associated with the public key certificate, their identity will be included in the certificate and only the issuance of a certificate can be requested in the following cases:

a) To request a certificate of natural person, the subscriber is:

   i. The same natural person. When the subscriber and the subject are the same person, this person shall be held directly responsible for the breach of obligations.

   ii. A natural person with sufficient powers of attorney to represent the natural or legal person.

b) To request a certificate of a legal representative of a legal person or entity without legal personality, the subscriber is:

i. A legal representative of the legal person or entity without legal personality with sufficient powers of attorney.

c) To request a system, server, or web certificate, for example SSL, the subscriber is:

i. The natural person legal representative of the interested entity.

1.3.1.8.2 Subject

The subject is the entity or person to which the certificate is applied, and which is authenticated with the private key. The subject can be:

a) The Subscriber in case of requesting the certificate for himself the certificate.

b) A natural person to whom the Subscriber requests the certificate acting as his/her legal representative.

c) A legal entity, for example, electronic seal, web authentication, etc. to whom the Subscriber requests the certificate.

d) The public employee of a Public Administration to whom the subscriber with sufficient powers of representation, requests for, the issuance of the certificate to be authenticated in their telematic relations and be used for the generation of electronic signatures as officer, employee, or temporary personnel of the Public administration.

1.3.1.8.3 Certificate responsible

The certificate responsible is in possession of the signature creation device and is responsible for its use and custody. The certificate responsible must have an express authorization from the subscriber and his identity will be included in the certificate.

The certificate responsible must be a natural person of legal age, with full capacity to act and must state his/her consent to assume this responsibility.

1.3.1.8.4 Relying Parties

In general, they are all the natural or legal persons, entities, organizations, Public or Corporate Administrations that voluntarily trust in the electronic certificates, in the electronic signatures generated by them, electronic signature service in centralized certificate device of ANF AC, in the electronic time stamps and in the authentication processes performed in the scope of this PKI.

The third-party recipient of certificates or time stamps, assumes its responsibility as a "relying party" when he/she accepts in its relations with subscribers the use of these instruments.

When this use has been made, the third-party receiver assumes that there is no declaration by which it intends to assert that he/she does not trust in the certificates, in the electronic signatures or time stamps, if he/she effectively trusted them and, therefore, acquired the corresponding responsibilities and obligations.

These "relying parties" must perform public key operations satisfactorily to trust in the certificate, as well as assuming the responsibility of verifying the status of the certificate, the authorized scope of use, as well as the limitations of responsibility contained in the certificates and policies to which they are subjected; for this purpose, they must use the means established in this CPS and Policies that make up its addendum.

Relying parties must act on principles of good faith and loyalty, refraining from performing fraudulent or negligent conduct intended to repudiate the processes of identification, electronic signature or time stamp, or any manipulation of electronic certificates.

1.4 Use of the certificates

Certification Policies corresponding to each type of certificate issued by ANF AC are those documents in which the uses and limitations of each certificate are specified and published in

https://www.anf.es/en/show/section/cps_597

Nonetheless, in general, the permitted and prohibited uses of the certificates issued by ANF AC are established hereunder.

1.4.1 Allowed usage

1.4.1.1 Qualified Certificates

Regarding the usage of these certificates:

- The electronic signature qualified certificates ensure the identity of the subscriber and the holder of the private signature key. With the intervention of secure signature creation devices, they are ideal for providing support to the qualified signature, which in accordance to article 3.4 of the Spanish Law 59/2003, of December 19th, on electronic signature, and with eIDAS, it is compared to handwritten signature by legal effect, without having to meet any additional requirements.
- Qualified certificates can also be used, if it is defined in the type of certificate, to sign authentication messages, particularly SSL or TSL client challenges, S/MIME Secure Email,

encryption without key recovery among other. This digital signature has the effect of guaranteeing the identity of the subscriber of the signature certificate.

- The electronic seal certificate links the validation data of a seal with a legal person and confirms the name of such person. They allow the generation of electronic seals, which serve as proof that a legal person has issued an electronic document, providing certainty as to the origin and integrity of the document.

  ANF AC's electronic seal certificates comply with the requirements of Annex III of eIDAS, in order be considered qualified.

- Website authentication certificates allow the authentication of a website and link the website with the natural or legal person to whom the certificate has been issued.

  The web certificates issued by ANF AC comply with the requirements of annex IV of eIDAS, in order to be considered qualified.

- Electronic Headquarters and Seal certificates are issued for identifying administrative offices and sealing electronic documents. Electronic Headquarters certificates in the scope of public administration, per the Spanish Law 39/2015, of October 1st, of the Common Administrative Procedure of Public Administrations.

Per the provisions of article 11.2 a) of Spanish Law 59/2003, on Electronic Signature, for a certificate to be deemed as qualified, it must have been issued with this indication. The Certification Policy specifies how this consideration shall be noted, which in general it is:

All certificates issued with the consideration of qualified, incorporate QCStatements, per the definition of ETSI EN 319 412-5:

- *QcCompliance:* *qualified certificate per eIDAS*
- *QcSSCD certificate:* *if it is issued in a qualified signature creation device*
- *QcRetentiodPeriod:* *documentation retention period*
- *QcPDS:* *route to the conditions of use*
- *Qctype:* *indicates the signature type per eIDAS (seal, signature,* web)

Furthermore, in the certificates it is included the CertificatePolicies extension (2.5.29.32), at least one of the defined PolicyInformation corresponds to:

- *qcp-public-with-sscd* *(0.4.0.1456.1.1)*
- *qcp-public* *(0.4.0.1456.1.2)*
- *qcp-natural* *(0.4.0.194112.1.0)*
- *qcp-legal* *(0.4.0.194112.1.1)*
- *qcp-natural-qscd* *(0.4.0.194112.1.2)*
- *qcp-legal-qscd* *(0.4.0.194112.1.3)*

- *qcp-web* *(0.4.0.194112.1.4)*

ANF AC qualified certificates meet the ETSI EN 319 411-2 technical standard.

1.4.1.2 Non-qualified certificates

Regarding the employment of non-qualified certificates:

- Non-qualified certificates do not guarantee the identity of the subscriber and, where appropriate, the holder of the signature key. In this case, it is not equivalent to the handwritten signature of the signer.

- Non-qualified certificates can also be used, if so is defined in the certificate type, to sign authentication messages, client challenges including SSL or TLS, Secure Email S/MIME encryption without key recovery, or others.

- In addition, such certificates can support various forms of authentication and advanced electronic signature.

  ANF AC guarantees that they have been issued in accordance with the standard ETSI EN 319 411-1.

1.4.1.3 Computer device certificates

Secure Server SSL and Electronic Headquarter certificates are issued.

This type of certificates follow the standards approved by the CA / Browser Forum and are audited per the ETSI EN 319 411-1 technical standard, both for its extended validation policy as for the basic one.

1.4.2 Usage scope of certificates

Regarding their usage scope, the following situations are considered:

- Certificates issued by ANF AC and intended for the public, private companies and corporations, are intended to be used by subscribers for any use not prohibited, respecting the limitations established in the certificate or in the corresponding CP, assuming, and therefore accepting the liability limitations stated by the issuer in the certificate itself, in this CPS and CPs.

- Certificates issued by ANF and intended for persons belonging to public administration bodies, or within the scope of the competencies of the administrative body and of the position or position held in a Public Administration. The key holders must use these certificates for the uses determined in the application, and always within the limits of use indicated in section a) above.

Specifications on the usage scope of each certificate must be consulted in their corresponding Certification Policy.

1.4.3 Limits of the certificate usage

Certificates must be used for their own function and established purpose, without being able to be used for other functions and for other purposes. Likewise, certificates must be used only in accordance with applicable law, especially considering the existing import and export restrictions on cryptography.

In the case of centralized certificates to sign electronically (non repudiation and commitment with the signed), to carry out processes of identification and authentication before computer systems.

The Certification Policies for each type of certificate may determine additional limitations and restrictions on the use of certificates.

1.4.4 Prohibited uses

Certificates issued by ANF AC and services rendered as VA or TSA, are to be used exclusively for the purpose and functions set forth in the corresponding Policies, and in compliance with applicable law, and agreements with current regulations, taking into consideration current import and export restrictions on cryptography.

Certificates, except where specified by the CP, cannot be used to act as a Registration Authority or Certification Authority, neither can they be used to sign other public key certificates, nor certificate revocation lists (CRLs), OCSP validation queries, issuance of time stamps, or for the provision of validation or delegated signature services.

Certification Policies corresponding to each type of certificate can determine limitations and additional restrictions on the use of certificates. It is not the purpose of this CP to determine additional limitations and restrictions.

Certificates have not been designed nor can be assigned to hazardous situations control equipment or uses that require fail-safe performances, such as the operation of nuclear installations, navigation systems or air communications, weapons control systems, where a failure could directly lead to death, personal injury, or severe environmental damage; their use or resale is not authorized for such uses.

The Certification Policies corresponding to each type of certificate may determine additional prohibitions on the use of certificates.

1.5 Certification Entity contact details

1.5.1 Trust Service Provider

Name	ANF Autoridad de Certificación
E-mail address	info@anf.es
Address	Paseo de la Castellana, 79
Locality	Madrid (Spain)
Zip code	28046
Telephone number	902 902 172 (Calls from Spain) International (+34) 933 935 946

1.5.2 PKI Governing Board

Name	PKI Governing Board
E-mail address	juntapki@anf.es
Address	Paseo Castellana, 79
Locality	Madrid (Spain)
Zip code	28046
Telephone number	902 902 172 (Calls from Spain) International (+34) 933 935 946

1.6 Definitions and acronyms

1.6.1 Definitions

Activation data (PIN): Secret key which the subscriber uses to activate signature creation data.

Authentication: The procedure of verifying the identity of a subscriber or holder of a certificate.

Authority Revocation List (ARL): List which exclusively includes all revoked or suspended intermediate or subordinate CA certificates (not including expired ones).

Certificate Revocation List (CRL): List which exclusively includes all revoked or suspended end-entity certificates (not including expired ones).

Certificate serial number: Unique integer number unequivocally associated with a certificate issued by ANF AC.

Certification Authority (CA): The Certification Authority is the entity that issues electronic certificates.

Certification Services Provider (CSP, CA): Natural or legal person which issues electronic certificates or renders other services in relation with the electronic signature.

Device: An instrument which is used to apply signature creation data, complying with the requirements established in article 24.3 of the Spanish Law 59/2003, 19th of December, on Electronic Signature.

Directory: Information repository which follows the ITU-T X.500 standard.

Electronic certificate: A certificate signed electronically by ANF AC which links signature verification data (public key) to the holder and confirms their identity.

Hardware Security Module (HSM): Hardware module used to carry out cryptographic functions and securely store keys.

Hash function (hash or digital fingerprint): Operation run on a group of data of any size, such that the result obtained is another group of data of a fixed size, independent of the original size, which has the property of guaranteeing the integrity of the original data and making its falsification impossible.

Holder: Natural/legal person or computer component for which an electronic certificate is issued and is accepted by himself/herself or legal representative or responsible in case of certificates of technical nature.

HSM (Cryptographic Security Module): it is a security device that generates and protects cryptographic keys.

Identification: The procedure of recognizing the identity of a subscriber or holder of an ANF AC certificate.

IT component (or component): Any software or hardware device suitable for using electronic certificates.

Non-qualified certificates: they are ordinary certificates, without the legal consideration of qualified certificate.

PKCS#10 (Certification Request Syntax Standard): Standard developed by RSA Labs, internationally accepted, which defines the syntax for a certificate request.

Public key and private key: ANF AC's PKI cryptography is based on asymmetrical cryptography. This uses a key pair: whatever is encrypted by one can only be decrypted by the other, and vice versa. One of these keys is called public and is kept in the electronic certificate, while the other is called private and is kept by the certificate's holder.

Public Key Infrastructure (PKI): Group of persons, policies, procedures, and IT systems necessary for providing authentication, encryption, integrity, and non-repudiation services using public and private key cryptography and electronic certificates.

Qualified certificate: A qualified certificate issued by ANF AC as a Qualified Trust Services Provider which complies with the requirements set in eIDAS and allows to guarantee the identity of the subscriber and the holder of the private key of the certificate.

Qualified electronic signature: Advanced electronic signature based on a qualified certificate and generated by a qualified signature creation device.

Qualified signature creation device: Electronic signature creation device that meets the requirements listed in Annex II of eIDAS.

Registration Authority (RA): It is the entity in charge of performing the tasks of identification of the subscribers.

Relying party: Person or entity, different from the holder, who decides to accept and trust in a certificate issued by ANF AC.

Root Certificate: Self-signed certificate whose subscriber is a Certification Authority (CA) belonging to the hierarchy of ANF AC, and which contains the signature verification data of said CA, signed with the signature creation data of the same as Qualified Trust Services Provider.

Session key: Key which establishes encryption for communication between two entities. The key is established specifically for every communication or session; its lifespan lasts until this communication or session ends.

Signature Creation Data (Private Key): It is the private key par associate to the public key pair. It is unique data, private cryptographic key, which the subscriber uses to create the electronic signature.

Signature verification data: This is the public key pair associated with the private key pair. They are unique data, public cryptographic key, used to verify an electronic signature.

Subject: It is the entity and person to whom the certificate is applied, is authenticated with the private key, and has control over it.

Subscriber: Natural person who requests to ANF AC the issuance of a certificate, and who has ratified a Subscription Agreement.

Time Stamping Authority (TSA): It is the entity that issues electronic time stamps.

Trusted hierarchy: Group of certification authorities which keep trust relationships and, thus, a higher-level CA guarantees the reliability of one or more lower-level CAs.

X.500: Standard developed by UIT which defines directory recommendations. It corresponds with the ISO/IEC 9594-1 standard: 1993. This gives rise to the following recommended standards: X.501, X.509, X.511, X.518, X.519, X.520, X.521 and X.525.

X.509: Standard developed by UIT which defines the basic format for electronic certificates.

1.6.2 Acronyms

ARL: Authority Revocation List.

C: Country. Distinguished Name (DN) attribute of an object, within the X.500 directory structure.

CDP: CRL Distribution Point.

CA: Certification Authority.

CEN: European Committee for Standardization (Comité Européen de Normalisation).

CN: Common Name. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

CP: Certification Policy

CPS: Certification Practice Statement.

CRL: Certificate Revocation List.

CSP: Certification Services Provider.

CSR: Certificate Signing Request. A group of data containing holder's information and a public key, all of which is self-signed by the holder using the relevant private key.

CWA: CEN Workshop Agreement.

DN: Distinguished Name. Univocal identification of an entry within the X.500 directory structure.

eIDAS: Regulation (EU) No 910/2014 of the European Parliament of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

ETSI: European Telecommunications Standard Institute.

HSM: Hardware Security Module. Comply with the ISO 15408 standard, (or superior), in accordance with what is established in the CEN CWA 14169.

IETF: Internet Engineering Task Force.

LDAP: Lightweight Directory Access Protocol

O: Organization. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

OCSP: Online Certificate Status Protocol. This protocol allows online checking of an electronic certificate's status.

OID: Object Identifier.

OU: Organizational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

PIN: Personal identification number. In an electronic certificate context, it corresponds to the signature activation data.

PKCS: Public Key Infrastructure Standards. PKI standards developed by RSA Laboratories and internationally accepted.

PKI: Public Key Infrastructure.

PKIX: A workgroup within the IETF (Internet Engineering Task Group) incorporated with the objective of developing specifications related to PKI and the Internet.

RA: Registration Authority.

RFC: Request for Comments (Standard issued by the IETF).

UUID: Universally Unique Identifier. It is a code standardized by the Open Software Foundation (OSF) that enables distributed systems to provide a unique and reliable information identifier that avoids name conflicts.

VA: Validation Authority.

2 Repositories and information publication

2.1 Repositories

For downloading the Root CA and Intermediate Certificates:

- Web: https://www.anf.es/en/show/section/root_ca_certificate

  https://www.anf.es/en/show/section/intermediate_ca_certificate

For downloading the end-entity certificates:

- Web: https://www.anf.es/en/show/section/certificate_search

For downloading the valid version of the CPS:

- Web: https://www.anf.es/en

For downloading the valid versions of the CP:

- Web: https://www.anf.es/en/show/section/cps_597

For downloading the publish documents by ANF AC

- Web: https://www.anf.es/en/show/section/documentary_structure

For accessing the Certificate Revocation Lists (CRL):

- The Certificate Revocation Lists are public and available in CRL v2 format on the following link: https://www.anf.es/en/show/section/crl%27s_%E2%80%93_arl%27s

2.2 Certification Entity information publication

ANF AC's publishing service is a system where all the documents drafted by ANF ACA, in relation to their trust services and complementary ones are published. It also publishes the certificates obtained by the entity and available credentials.

- Ensures availability of information online.

  http://www.anf.es/en

  It is available for anyone interested a paper version of all the document.

- It facilitates the use of a fast and secure service of consultation of the registry of issued certificates which is at the disposal of relying parties of the certificates.

- Maintains an updated system of certificates in which the issued certificates are indicated and if they are in force or if their validity has been suspended or extinguished.
- Issues Certificate Revocation Lists (CRLs) and (ARL's), which are accessible to the public. In addition, it provides real-time verification services for certificates, through Online Certificate Status Protocol (OCSP).

Access to this repository of documents is regulated in accordance to the level of security with which each document is classified as specified in the section "Classification of the documents drafted by ANF AC" of this CPS.

2.3 Publication and notification policy

Changes in the specifications or in the conditions of service shall be communicated by ANF AC to subscribers and relying parties through the website of ANF AC:

www.anf.es/en

2.3.1 Items not published in the Certification Practice Statement

The full list of components, subcomponents and elements that exist but due to their confidential characteristic are not placed at the disposal of the public, are those reported in this Certification Practice Statement, under the sections "Confidentiality of Information" and in "Classification of documents drafted by ANF AC".

2.4 Approval of the publication

Final modifications as well as aspects related to publication and notification are approved by the PKI's Governing Board, after verifying the compliance with the requirements set herein.

2.5 Publication of status of issued certificates

ANF AC provides a fast and safe consultation service of the Registry of Issued Certificates. An updated system of certificates is maintained, which identifies the license and if they are valid or if their application has been suspended or expired.

In the publication of CRLs, safe and quick access to users and subscribers is guaranteed, as indicated in the relevant section of this CPS.

Furthermore, ANF AC provides real-time verification of certificates in the following modalities:

- Through Online Certificate Status Protocol (OCSP) consultation. Information on: https://www.anf.es/en/show/section/ocsp_services

- Web service permanently available for querying the status of a given certificate status.

Unless expressly authorized in writing by the PKI Governing Board of ANF AC, it is prohibited to use any of these publishing service to provide validation services to third parties or to use the information for purposes other those specifically authorized herein.

2.6 Frequency of updates

The Certification Practice Statement and Certificate Policies are published each time they are modified, unless the PKI Governing Board considers the update as minor, in which case, it will publish an annex built to the respective CPS or affected Policy, as stated in the section "Management of CPS and Certification Policies" of this document.

The certificates issued by the CA are published immediately following their issuance. ANF AC adds the revoked certificates to the relevant CRL within the period stipulated in the "Next Update" field.

OCSP queries are performed on permanently updated states.

2.7 Access control

ANF AC's Publishing Service has a security system that allows to adequately control access to information per the Document Classification and Operators Security Level.

This system also prevents unauthorized persons from adding, modifying, or deleting records of this Service, and protects the integrity and authenticity of the information stored, so that:

- Only authorized persons can make entries and modifications.

- The authenticity of the information can be verified.

- The certificates are only available for consultation if the subscriber has formally given consent in the corresponding subscription agreement.

- Any technical change affecting the safety requirements can be detected. ANF AC only allows access to classified information to persons who are specifically authorized. We have implemented security measures that allow to protect, in a reasonable manner, access to information, determining at each visit:
    - Identity of the applicant
    - Accredited Security Level accredited

Servers managed a Log system which:

- Manages an access log
- Manages a denial access log

2.8 Audits

ANF AC performs internal audit processes periodically, and hires independent auditors of maximum prestige to review its public key infrastructure.

2.8.1 Frequencies of audits.

- ISO 27001 Audit, cycle of 3 years with annual revisions.
- ISO 9001 Audit, cycle of 3 years with annual revisions.
- WEBTRUST for CA, WEBTRUST SSL BR, WEBTRUST EV SSL, annually.
- Conformity assessment: EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421. As stated in the eIDAS Regulation, biannual.
- Spanish Data Protection Audit, annual.
- PCI DSS Audit, annually.
- RRA Audit, in a discretionary manner.
- Systems Audit, in a discretionary manner.
- Internal ISO 26000 Audit, annually.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

All certificates contain a DN (DistinguishedName) X.500, in the Subject Name field.

The attributes that make up the distinguished name of the subject field are those included in the section corresponding to the profile of the certificate.

On some types of certificates the subjectAltName field includes information about the subject

In all end-entity certificates of identity, the Common Name field contains the full name of the certificate subscriber.

The profile is based on the IETF RFC 5280 recommendations, and the ITU-T X.509 standard. ETSI has developed European standards in compliance with the European Commission Mandate M/460 to rationalize the standards for electronic signatures. The ETSI EN 319 412 family specifies the content of the certificates issued to natural persons, legal or web sites certificates.

The Certification Policy to which each certificate is submitted determines precise specificities in this respect.

3.1.1.1 Issuer – Requirement of article 11.2 letter c) of Spanish Law 59/2003

This field contains the ANF AC identification which is the Certification Entity which signed and issued the certificate. The field cannot be left blank and always contains a Distinguished Name (DN).

A Distinguished Name (DN) is composed of a combination of attributes, consisting of a name or label and an associated value. In the certificates issued by ANF AC, every single Subject field make the Distinguished Name (DN).

The issuer of the intermediate CAs matches the Subject of the CA that issued the certificates.

3.1.1.2 Subject - Requirement of article 11.2 letter c) of Spanish Law 59/2003

This field contains the identification of the subscriber or holder of the certificate. The field cannot be left in blank and shall always contain a Distinguished Name (DN).

A Distinguished Name is composed of a combination of attributes, consisting of a name or label and an associated value.

The Certification Policy to which each certificate is submitted, establishes the detailed profile of each certificate. Need for names to be meaningful.

As stated in the Certification Policy to which the electronic certificate is subjected.

3.1.2 Interpretation of name formats

As stated in the reference X.500 standard in ISO/IEC 9594.

The subject and the issuer identify the person (natural or legal) or device, and must have meaning in the sense that the Issuing Entity has evidence of the association between these names or pseudonyms and the entities to which they are assigned.

Names cannot be misleading.

3.1.3 Uniqueness of names

The DN of the certificates must be unique.

Within a same hierarchy, it cannot be reassigned a subscriber name that has been used by another subscriber. To avoid duplication of names between different people it shall be incorporated the unique tax identification into the chain of the name that distinguishes the certificate holder.

In the Common Name (CN) the uniqueness and space requirements must be met in the name. In no case are anonymous certificates issued, although ANF AC may issue pseudonym certificates, but these cannot be CA or subordinate CA certificates.

The Certification Policy to which each certificate is submitted sets out the detailed profile of each certificate.

3.1.4 Dispute resolution concerning names and trademarks

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

Certificate subscribers will not include names in applications that may involve infringements of third-party rights.

Conflicts of names of certificate responsible that are identified in certificates with their real name are solved by including, in the certificate's name, the National/Foreign Citizen ID Card of the certificate responsible or other identifier assigned by the subscriber.

3.1.5 Recognition, authentication, and role of trademarks

The distinguished names are the property of the persons who own the corresponding trademark rights on them, if any. If this circumstance is not known, ANF AC will use the name proposed by the user, under the full responsibility and liability of the user.

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

3.2 Identity initial validation

3.2.1 Proof of private key possession

In ANF AC's PKI, the keys are always generated by the certificate's own subscriber, which determines the signature activation data independently and without the intervention of third parties. The possession of the private key, corresponding to the public key for which it is requested the generation of the certificate, will be proven by sending the Certificate Signing request (CSR), per the RSA PKCS#10 standard, in which it will be included the public key signed by the associated private key.

This certificate request is sent to ANF AC for processing, which makes it possible to detect errors in the generation of the certificate and proves that the subscriber already has the key pair in his/her possession, and can make use of them.

3.2.2 Authentication of a legal person's identity

ANF AC is based on the specifications of the Commision Implementing Regulation (EU) 2015/1502 of 8 September 2105 on setting minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Each Certification Policy establishes the procedure for authenticating the identity of a legal person, generally determining the following aspects:

- Types of documents valid for identification.
- Identification procedure to be carried out by the RRA.
- Necessity or not to process identification in-situ.
- Form of attesting the membership to a given organization and sufficient legal powers of attorney.

3.2.3 Authentication of a natural person's identity

ANF AC is based on the specifications of the Commision Implementing Regulation (EU) 2015/1502 of 8 September 2105 on setting minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Each Certification Policy establishes the procedure for authenticating the identity of a legal person, generally determining the following aspects:

- Types of documents valid for identification.
- Identification procedure to be carried out by the RRA.
- Necessity or not to process identification in-situ.
- Form of attesting the membership to a given organization and sufficient legal powers of attorney.

3.2.4 Non-verified information regarding the subscriber

Non-verified information is not included on certificates issued by ANF AC.

3.2.5 Verification of powers of attorney

The Issuance Reports Manager is responsible for verifying the powers of attorney, determining their validity in the public records where they must be registered, and assessing their sufficiency.

3.3 Identification and authentication of re-key requests

3.3.1 Identification and authentication for routine re-key

Each Certification Policy establishes the authentication procedure of a subscriber's identity.

ANF AC verifies the existence and validity of the certificate for which the re-key is solicited, and that the information used to verify the identity and attributes of the subscriber/subject are still valid. On the other hand, if the terms and conditions governing the relationship between the subscriber/subject and the CA have been modified at the date of re-key, the valid terms and conditions must be transmitted.

3.3.2 Identification and authentication for re-key after revocation

The re-key of revoked certificates is not authorized.

4 Certificate life-cycle operational requirements

This section establishes the common operational requirements to the different types of certificates issued by ANF AC. If ANF AC performs "cross-certification" with an external Certification Service Provider, ANF shall require compliance with all requirements defined in this Certification Practice Statement and related Certificate Policies.

The specific regulations for each type of certificate should be consulted in the corresponding Policy.

4.1 Certificates application

Once the identity of the subscriber is attested before the Registration Authority, or having his/her signature been authenticated by a public notary, any subscriber desiring a certificate must:

- Complete the certificate application form with all required information and proceed in signing it. Nonetheless, not all required information will be written in the certificate; it is only required for various obligations which ANF AC must meet to correctly issue the certificate and manage its PKI. This information will be kept confidentially by ANF AC in accordance with the applicable law regarding Personal Data Protection.
- Sign the corresponding subscription agreement, adhering to the contractual terms and conditions, and paying the appropriate fees. The signing of these documents presupposes the acceptance of the electronic certificate, and of all obligations and responsibilities specified in this CPS and in the corresponding Certification Policy.

A new "Issue Request" will not be necessary in the case of emissions made because of a revocation due to technical failures in the issuance and/or distribution of the certificate or related documentation.

The data that identifies the key holder in the certificate and in the request, is the one appearing in the required identification documents. This information is accurately recorded, within the limits of length derived from the technical conditions established in the content of the certificate.

Any modification relating to the information contained in the certificate or documents filled out to process the request, produced after the issuance of the certificate, must be communicated to ANF AC, as it may lead to a revocation of the certificate.

On the other hand, in the scope of electronic certificates of centralized signature, the identification and authentication functions described in this section will also be performed by an operator of a Registration Authority or by authentication of signature performed by a public notary.

4.1.1 Who can process an application

Each Certification Policy specifies who can be a certificate holder, who can apply for one and the documentation that must be submitted.

4.1.2 Registration of certificate applications

The Recognized Registration Authority will advise the subscribers on the adequacy of the type of certificate to the characteristics of use and profile of the holder. The Recognized Registration Authority may authorize or deny an application.

Using the technical means provided by ANF AC to the Recognized Registry Authority, the certificate request is registered online on ANF AC's Trust Servers. If the Recognized Registry Authorities do not intervene, the certificate subscriber assumes the responsibility of processing the documentation, authenticating it, and registering it before ANF AC, per the procedure specified in the corresponding Certification Policy.

ANF AC has a customer service. Anyone interested in requesting an electronic certificate can receive support through:

- Telephone call 902 901 172
- Email info@anf.es

4.1.3 Verification of the application

The Issuance Reports Managers are responsible for evaluating the sufficiency of the documentation provided by the subscribers and for ordering the necessary verifications to determine the veracity of the information that is requested to be included in the certificate.

In addition, it has the power to modify changes in the request for the certificate, at the request of the RA and/or subscriber, if this is done prior to issuance of the certificate, and the data has been previously verified by the RA, or by the same Issuance Reports Manager.

Likewise, they are entitled to correct the material errors that they detect in the application, which are derived from the verification of the documents provided.

The Issuer Reports Manager, based on the verification procedures performed, will issue a report of approval, denial, or request for further documents to the subscriber.

4.1.4 Time to process certificate applications

A maximum period of 15 days is established for the processing of the certificate requests. ANF AC does not assume any liability for any delays that may arise, but in case of exceeding the maximum term established, it must inform the subscriber of the causes that caused the delay, and the subscriber becoming released to cancel the request and ANF AC reimbursing any fees that may have had perceived.

4.2 Certificate issuance

The issuance of a certificate means the complete and final approval of an application by the Issuance Reports Manager. Depending on the type of certificate, the issuance may be made on a cryptographic device or software support.

4.2.1 Proceedings during certificate issuance

The Issuer Reports Manager issues a certificate of compliance in which the certificate of petition sent by the subscriber is incorporated, as well as the identification minute issued by the Registration Authority that intervened in the identification process, or authentication performed by a public notary. Notifies the subscriber via signed email of the conformity of their request.

These documents are processed automatically by ANF AC's certificate issuing service. This service proceeds in performing the security integrity verification of the documents received, verifying their consistency and their correspondence with the Certification Policy to which the requested certificate will be submitted. In case of conformity, the certificates are issued.

Once the certificate is issued, ANF AC informs the subscriber via email, proceeds to activate the necessary computer mechanisms so that the certificate is registered in the corresponding repository and is available for download. The subscriber, using the same electronic signature cryptographic device that he used to generate the key pair and request certificate, can download, and install it.

In case of technical certificates (SSL, Electronic Seal, Public Administration, Application, or Code Signature), ANF AC will deliver the certificate, through a secure mean (for example, signed e-mail, in person delivery, etc.) to the certificate responsible.

ANF AC signs the public keys of the certificates it issues with its private key.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed, considering that the certificate once issued is loaded in the centralized signature device in which the public key pair was generated. At that time, the subscriber receives an e-mail informing that the certificate has been issued and is available for use in the centralized electronic signature system.

4.2.2 Notification to subscriber of the certificate issuance

The electronic signature cryptographic devices of ANF AC incorporate a procedure that automatically proceeds to the connection with the trusted server, establishing a secure communication, which allows the downloading of the certificate once it has been issued.

In addition, an e-mail is sent to the subscriber, informing of the issuance and publication of the issued certificate, including the case of electronic certificates of centralized signature.

4.3 Certificate acceptance

4.3.1 Manner in which the certificate is accepted

Each Certification Policy determines the method of acceptance. Generally, it is established that:

- The certificate acceptance is formalized by the subscriber by signing the Subscription Agreement, as stated in section 4.1 of this document. Furthermore, ANF AC will be able to request the perfection of the certificate acceptance by requesting the subscriber to sign a Certificate Reception and Acceptance Minute. This requirement must be attended by the subscriber within 15 days. After that time, if the subscriber has not attended it, ANF AC will be able to revoke the Certificate.

- In the corresponding CP, it will be possible to detail or to extend the form in which the certificate is accepted.

- ANF AC guarantees the correct operation of the instruments supplied, which operate per the characteristics that are required. The subscriber has 7 calendar days to verify the certificate, software, and cryptographic device.

- In the event of technical defects (among others: certificate storage malfunction, program compatibility problems, technical error in the certificate, etc.) or errors in the data contained in the certificate, ANF AC will revoke the certificate issued and proceed to issue a new one within a maximum period of 72 hours.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

4.3.2 Publication of the certificate

ANF AC, once the certificate is issued, proceeds to publish it in the corresponding repositories.

4.3.3 Notification of certificate issuance to third parties

No notification is sent to third parties.

4.4 Rejection

In addition to the result of refusal that may be issued by the Issuance Reports Manager, ANF AC reserves the right to freely refuse the issuance or renewal of certificates and when it deems appropriate.

A PKI system is developed within a framework of mutual trust and in a bona fide relationship. Those persons who maintain or have directly maintained any type of conflict of interest with this entity providing certification services, or with the members of its Governing Board, cannot process any request for the issuance of certificates, nor urge third parties to do so. Neither can they process certificate applications to persons belonging to or dependent on entities that are a competition to ANF AC.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

4.5 Pair of keys and use of the certificate

4.5.1 Private key and certificate usage by the owner

The responsibilities and limitations of use of the key pair and the certificate, including in the scope of electronic certificates of centralized signature, are established in the corresponding CP.

In general, the subscriber of the certificate, in any case, must:

- Upon receipt of the electronic certificate issued by the CA, shall not use it until he/she verifies the correspondence of the data included in the certificate with the information provided by himself/herself, as well as the adequacy of the certificate to the request that it made. The use of the electronic certificate by the subscriber presupposes its full acceptance and conformity.
- Shall ensure the proper use and conservation of the storage of the certificates.
- Shall properly use the certificate and comply with the limitations of use.
- Shall be diligent in the custody of their private key, and will maintain the privacy of signature activation data to avoid unauthorized use.
- Shall notify ANF and any person the subscriber believes may rely on the certificate, without unreasonable delays:
    - The loss, theft or any risk that compromises the private key.

- Loss of control of signature activation data.
- The inaccuracies or changes related to the information contained in the certificate, requesting the revocation of the certificate when said modification constitutes cause of revocation.

- Shall no longer use the private key after the validity period of the certificate expires, or when a certificate has been revoked.
- Shall transfer to the holders of keys their specific obligations.
- Shall not monitor, manipulate, or reverse engineer the technical implementation of certification services without the prior written permission of ANF AC.
- Shall not intentionally compromise the security of certification services.
- Shall not use the private keys corresponding to the public keys contained in the certificates, for signing any certificate, as if they were a Certification Entity.
- The qualified certificate subscriber who generates digital signatures using the private key corresponding to the public key listed in the certificate must recognize in the legal instrument that such electronic signatures are equivalent to handwritten signatures, whenever a cryptographic device is used, In accordance with the provisions of article 3.4 of the Spanish Law 59/2003, of December 19th, on Electronic Signature, and eIDAS.

4.5.2. Public key and certificate use by relying parties

Relying Parties may only place their trust in the certificates for what the corresponding CP establishes and in accordance with the "Key Usage" and "Extended Key Usage" field of the certificate.

Relying Parties must perform public key operations satisfactorily to trust the certificate, as well as assume responsibility for verifying the status of the certificate using the means set forth in this CPS and the corresponding CP.

In any case, they must:

- Verify that the certificate is appropriate for the intended use, and if they do not have sufficient knowledge to fully understand it, it is their responsibility to be advised independently.
- Know the conditions of use of the certificates per the provisions of the Certification Practices Statement and Certification Policies to which the issuance and use of each type of certificate is submitted.
- Verify the validity or revocation of the certificates, for which it will use information on the status of the certificates in accordance with the ANF AC's Validation Policy.

- Verify the integrity and authenticity of electronic certificates in accordance with the ANF AC's Validation Policy.
- Verify all certificates in the certificate hierarchy, before relying on the electronic signature or any of the certificates in the hierarchy in accordance with ANF AC's Validation Policy.
- Be aware of any limitations on the use of the certificate, regardless of whether it is on the certificate itself or in the verifier agreement.
- Keep in mind any precautions established in an agreement or other instrument, regardless of their legal nature.
- Notify any fact or anomalous situation related to the certificate and that can be considered a cause of revocation of the same.
- Not monitoring, manipulating, or reverse engineering the technical implementation of certification services without the prior written permission of ANF.
- Not intentionally compromising the security of certification services.
- Recognize that electronic signatures are equivalent to handwritten signatures, in accordance with eIDAS.

4.6 Certificate renewal without key change

With sufficient time, the certificate user shall be informed by electronic mail to the address indicated on the electronic certificate, that the certificate is close to its expiry date. The same e-mail will indicate the steps to follow for the renewal of the electronic certificate.

When requesting the renewal of a certificate without renewing the pair of keys, ANC AC, prior to issuance, will determine if this pair of keys is still cryptographically reliable and that there is no indication that the subject's private key has been compromised.

If it is so considered, it will be verified that the registration data remains valid and, if any data has changed, it must be verified, stored and the subscriber must agree with it, as specified in the corresponding section of this policy.

If the legal conditions of provision of the service have varied since the issuance of the certificate, ANF AC shall inform this to the subscriber.

The applicable procedure for the renewal, without re-keying, requires the safe recovery of the cryptographic devices where the keys reside, before, if necessary, proceeding to the safe deletion of the device and the generation of the new certificate.

The procedure applicable to the renewal, without re-keying of these certificates, may be based on the previous existence of a valid certificate, if the key pair of this certificate is cryptographically reliable for the new term of validity of the new certificate, and that there is no suspicion of the compromise of the private key of the subscriber or of the person in charge of the certificate.

In any case, the renewal of a certificate is subject to:

- That it be requested in due time and in accordance with the instructions and regulations established in ANF AC's CPS.
- That ANF AC or the RA that intervened in the request processing has not had certain knowledge of the concurrence of any cause of revocation of the certificate.
- That the request for renewal for the provision of services refers to the same type of certificate issued initially.
- That the certificate to be renewed is valid at the time of the request.

If a period of more than 5 years has elapsed since the identification was made in-situ by the subscriber, it is necessary to formalize the request by handwritten signature of the subscriber, a process performed in-situ by the interested party and using sufficient original documentation before a RRA, A Collaborating RA or a Trustworthy Entity.

Once the process for renewal of the certificate is finished, the user will receive a warning in his Cryptographic Device that will indicate that ANF AC has already issued the renewed certificate and that by entering the activation PIN it can be downloaded to the device. The end user can now use the renewed certificate.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

In case the Terms and Conditions for the Certificates and Services Usage have been modified, the new version shall be provided to the subscriber.

4.7 Certificate renewal with re-keying

4.7.1 Circumstances for certificate renewal with re-keying

If the reason for the renewal application is:

- Keys compromised or loss of reliability of the same.

The renewal will always be done with re-keying.

When a renewal of a certificate with re-keying is requested, it will be verified that the registration data continues to be valid and if any data has changed, it must be verified, stored and the subscriber must agree with it, as specified in the corresponding section of this policy.

If the legal conditions for the provision of the service have varied since the issuance of the certificate, ANF AC or the Recognized Registry Authority shall inform the subscriber of this fact.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

In case the Terms and Conditions for the Certificates and Services Usage have been modified, the new version shall be provided to the subscriber.

4.7.2. Processing of certificate renewal requests with key change

The applicable procedure for the renewal of the certificate shall be the same as for the issuance of a completely new certificate. Verifications of omission or error in the application shall be verified by ANF AC.

In any case, the renewal of a certificate is subject to:

- That it be requested in due time and in accordance with the instructions and regulations established in ANF AC's CPS.
- That ANF AC or the RA that intervened in the request processing has not had certain knowledge of the concurrence of any cause of revocation of the certificate.
- That the request for renewal for the provision of services refers to the same type of certificate issued initially.
- That the certificate to be renewed is valid at the time of the request.

If a period of more than 5 years has elapsed since the identification was made in-situ by the subscriber, it is necessary to formalize the request by handwritten signature of the subscriber, a process performed in-situ by the interested party and using sufficient original documentation before a RRA, A Collaborating RA or a Trustworthy Entity.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

4.8 Certificate modification

This is not authorized.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The revocation causes the loss of validity of a certificate before its expiration. The effect of the revocation is final. Revocation, including in the scope of electronic certificates of centralized signature, is performed due to the following:

1. Circumstances affecting the information contained in the certificate:
    - Modification of any of the data contained in the certificate.
    - Discovery that some of the information provided in the certificate request is incorrect, as well as the alteration or modification of the circumstances verified for the issuance of the certificate.
    - Discovery that some of the data contained in the certificate is incorrect.

2. Circumstances affecting the security of the key or certificate:
    - Compromise of the private key or the infrastructure or systems of the Certification Entity that issued the certificate, as long as it affects the reliability of the certificates issued from this incident.
    - Infringement, by the Certification Entity, of the requirements provided in the certificate management procedures, established in ANF AC's DPC.
    - Compromise or suspicion of compromise of the key security or the certificate of the subscriber or subject.
    - Unauthorized access or use by a third party of the private key of the subscriber or subject
    - Irregular use of the certificate by the subscriber or subject, or lack of diligence in the custody of the private key.

3. Circumstances affecting the security of the cryptographic device:
    - Compromise or suspicion of compromise of security device.
    - Loss or disablement due to damage of the cryptographic device.
    - Unauthorized access by a third party to the activation data of the subscriber or certificate manager.

4. Circumstances that affect the subscriber or the certificate responsible
    - Termination of the relationship between the subscriber and the subject.
    - Modification or termination of the underlying legal relationship or cause that produced the issuance of the certificate to the subscriber or certificate responsible.
    - Infringement by the subscriber of the certificate of the pre-established requirements for the latter's request.

- Infringement by the subscriber or certificate responsible of their obligations, responsibilities and guarantees, established in the corresponding legal instrument or in the CPS of the Certification Authority that issued the certificate.
- Supervening disability of the subscriber or certificate responsible.
- Extinction of the legal entity represented or subject of the certificate, as well as the termination of the powers of attorney of subscriber, cessation of the authorization of the subscriber to the certificate responsible or the termination of the relationship between the subscriber and the certificate responsible.
- Request of the subscriber for revocation of the certificate, in accordance with what is established in section 3.4 of this policy.

5. Other circumstances:
    - The termination of the service of this electronic certification service provider, in accordance with the provisions of section 4.16 of this policy.

The legal instrument that links the Certification Entity with the subscriber establishes that the subscriber must request the revocation of the certificate in the event of being aware of any of the circumstances indicated above.

4.9.2 Entity that can request revocation

ANF AC, or the Registration Authority that processed the petition, may request ex officio the revocation of the certificate if they had knowledge or suspicion of compromise of the holder's private key or any other determining factor that recommends taking such action.

In addition, the subscriber, and, if applicable, the certificate responsible, may request the revocation.

4.9.3 Procedure for revocation request

The entity that needs to revoke a certificate, including in the scope of electronic certificates of centralized signature, must request it to ANF AC or, as the case may be, the Registration Authority with which it processed the certificate request.

The revocation request must contain at least the following information:

- Date of request for revocation.
- Identity of the subscriber or, as the case may be, the certificate responsible
- Detailed reason for the request for revocation.
- Name and title of the person requesting the revocation.

- Contact information of the person requesting the revocation.

The request for revocation will be processed upon receipt. It must be authenticated in accordance with the requirements set forth in the corresponding section of this policy. Once the request is authenticated, ANF AC may directly revoke the certificate.

When a certificate is revoked, all instances are revoked. The subscriber and, as the case may be, the certificate responsible, through the e-mail address on the revoked certificate, is informed of the change of status of the revoked certificate. ANF AC shall not reactivate the certificate once revoked.

Likewise, in the Critical Access Cryptographic Device it will be possible to consult that the certificate has been revoked.

All revoked certificates will be included in all CRL publications, at least up to three months after their expiration date.

The Certificate Revocation Application Forms published on ANF AC's website: www.anf.es/en

4.9.4 Revocation request grace period

Requests for revocation will be processed reasonably immediately upon becoming aware of the cause of revocation, and having authenticated the subscriber and verified their ability to act. Therefore, there is no grace period associated with this process during which the revocation request can be annulled.

4.9.5 Maximum processing time of the revocation request

The correct request for revocation shall be processed, always following the procedure of verification and authentication of the submitted application, whose responsibility lies in the Issuance Reports Manager. The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties, shall be at most 24 hours.

4.9.6 Obligation to consult the certificate revocation information

Relying parties must verify the status of those certificates that they wish to trust.

ANF AC makes available to relying parties a status information service for certificates based on the OCSP protocol, and access and download of Certificate Revocation Lists (CRLs).

4.9.7 Frequency of issuance of Certificate Revocation Lists (CRL and ARL)

Each certificate will specify the address of the corresponding CRL, using the CRLDistributionPoints extension.

ANF AC issues a weekly CRL, even when there are no changes or updates, to ensure the validity of the published information (in accordance with Section 2.7 "Scheme of identification and electronic signature of Public Administrations. Block III: Proposals for additional general conditions of the AGE").

The CRL specifies the time programmed as the limit for issuing a new CRL. In its elaboration, it follows what is established in the RFC 5280 (updated by RFC 6818).

ANF AC issues an ARL every six months, even when there are no changes or updates.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

4.9.8 Maximum publication period for CRLs and ARLs

The change of status of the validity of a certificate must be indicated in the CRL or, where applicable, in the ARL, less than five minutes after the change occurred (in accordance with Section 2.7 "Scheme of identification and electronic signature of Public Administrations. Block III: Proposals for additional general conditions of the AGE"). Based on this, ANF will publish a new CRL or ARL in its repository at the time of any revocation.

All CRLs and ARLs published by ANF AC will be available in a history available on the web.

In any case, ANF will issue a new CRL in its repository at intervals not exceeding 7 days, and ARL at intervals not exceeding one year.

4.9.9 Certificate status verification services availability

Relying parties will be able to consult the certificates published in ANF AC's Repository by means of a certificate status information service based on the OCSP protocol, or by consulting the CRL and ARL Revocation Lists.

Both services are available 24 hours a day, 7 days a week, accessible by secure protocol.

4.9.10 Obligation to consult the certificate status verification services

Relying parties must verify the status of those certificates they wish to trust, including in the scope of electronic certificates of centralized signature.

One way to verify the status of certificates is by consulting the most recent CRL and ARL issued by the Certificate Authority that issued the certificate they wish to trust.

ANF AC will provide support to relying parties on how and where to find OCSP-based certificate status verification services or the corresponding CRL and ARL (in accordance with Section 2.7 "Scheme of identification and electronic signature of Public Administrations. Block III: Proposals for additional general conditions of the AGE").

If for any circumstance, it is not feasible to obtain information on the status of a certificate, the system that must use it must disregard its use or, depending on the risk, the degree of responsibility and the consequences that might occur, use it without guaranteeing its authenticity in the terms and standards set forth in this policy.

4.9.11 Other forms of certificate revocation information

In addition to the on-line consultation service through Online Certificate Status Protocol (OCSP) and the Revocation List (CRL)/(ARL) consultation, ANF AC makes available to the public:

4.9.11.1 Personalized service

In case of urgent need, the Customer Service Center can be contacted by phone 24x7x365 at 902 902 172 (calls from Spain), International (+34) 933 935 946, or in-situ at the offices of ANF AC, during work hours from 9 am to 6 pm, from Monday to Friday.

4.9.11.2 SOAP service

Enables the computer incremental update of the certificate revocation list. This service has been developed following the requirements of the Spanish State Tax Administration. Its access is restricted to authorized entities.

4.9.11.3 Web service

It allows the verification of the validity status through consultation on the website of ANF AC:

https://www.anf.es/en

4.9.12 Special requirements in case of private key compromise

In case of compromise of the private key of the certificate, the subscriber, or the certificate responsible for the use of the certificate shall notify the circumstance to ANF AC for the revocation of the certificate.

In case of compromise of the private key of the CA, the key compromise will be notified to all participants of that Hierarchy, especially to:

- the Governing Board of the PKI;
- all the RRAs;
- all holders of certificates issued by that CA
- Known relying parties.

In addition, it will be published on ANF AC's website, and will be immediately revoked.

The Root CA will publish the certificate revoked in the ARL (Authority Revocation List).

After resolving the factors that led to the revocation, ANF AC may:

- Generate a new certificate for the issuing CA.
- Ensure that all new certificates and CRLs issued by the CA are signed using the new key.
    - The issuing CA may issue certificates to all affected subscribers who so require

On the other hand, in the scope of electronic certificates of centralized signature, ANF AC as custodian of the certificate, must notify this to the subscriber of the certificate and be responsible for its revocation. It shall also:

- Notify the PKI's Governing Board and the members of the Security Committee, a detailed report of the incident, and
- Issue a new free certificate to the subscriber who requires it.

4.9.13 Circumstances for certificates suspension

ANF AC does not authorize temporary suspension of certificates.

4.9.14 Legitimization to request suspension

Not authorized.

4.9.15 Procedure for suspension request

Not authorized.

4.9.16 Maximum period of certificate suspension

Not authorized.

4.10 Certificate recovery

The CA puts at the disposal of subscribers a service to recover their certificates. This service complies with the requirements established in terms of Personal Data Protection, and only provides a copy of these certificates to duly authorized third parties.

The recovery process is as follows:

- The certificate recovery subscriber is identified and verified to be authorized to request the recovery of the certificate.
- It is verified that the certificate to be recovered is neither expired nor revoked.
- It is verified that the data contained in the certificate is correct.
- The recovery subscriber is notified that the certificate must be revoked and replaced by the new certificate.
- An email is sent to the e-mail account that appears in the electronic certificate, which indicates the steps to follow to recover the certificate.
- After the new certificate is generated and a PIN activation is assigned, the validation and issuance process is exactly the same as a new certificate.

The procedure applicable to the recovery of the certificate shall be the same as for the issuance of a completely new certificate. Verifications of omission or error in the application shall be verified by ANF AC. The recovery of a certificate implies a renewal of the certificate with re-keying.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

4.11 Key custody and recovery

4.11.1 Key custody and recovery procedures and policies

In the case of electronic certificates stored on personal devices, cryptographic software token or HSM token, ANF AC does not generate the keys of its subscribers. In the scope of electronic certificates of centralized signature, ANF AC will back up the signature creation data provided that the security of the duplicate data is the same as that of the original data and that the number of data duplicates does not

exceed the minimum necessary to guarantee the continuity of the service. Signature creation data will not be duplicated for any other purpose.

4.12 Security audit procedures

Log files are used to reconstruct significant events that have been performed by ANF AC's software, Recognized Registry Authorities, the subscriber, or the event that originated them. Logs are evidence that can be used as a means of arbitration in potential disputes.

4.12.1 Audits and incidents

ANF AC maintains the following criteria in relation to the information available for audits and analysis of incidents that may exist with the certificates issued and the treatment thereof. Certificate users can communicate to ANF AC complaints or suggestions through the following means:

- Telephone: 902 902 172 (from Spain) International (+34) 933 935 946
- Via e-mail: soporte@anf.es
- In-situ: Headquarters address on the web https://www.anf.es/en/show/section/offices_725
- By completing the form available on the web https://www.anf.es/en
- Completing the forms of complaints or claims available at the registration authorities.

There is an internal record of incidents that have occurred with the certificates issued (security incidents managed by ANF AC's Security Committee). These incidents are logged, analyzed, and solved per ANF AC's ISMS procedures.

In accordance with the corresponding ISMS policy, it will be updated in a timely and coordinated manner to respond to incidents as soon as possible and limit their impact. Reliable personnel will be assigned to monitor critical events and incidents.

In the annual audit planning, the issuance operation of the certificates is audited with a minimum sample of 2% of the certificates issued.

The CPS defines the period of conservation of documentation.

4.12.2 Types of events recorded

Events related to the PKI's security is recorded:

- Starting and stopping of the systems.

- Start and termination of the certificate issuance application.
- Attempts to create, delete, change passwords or user permissions within the system.
- Generation and changes in the keys of the certification service provider.
- Changes in certificate issuance policies.
- Attempts to enter and exit the system.
- Unauthorized attempts to enter the network of the certification service provider.
- Unauthorized attempts to access system files.
- Failed read attempts on a certificate, and read and write attempts on the certificate repository.
- Events related to the certificate lifecycle, such as requesting, issuing, revoking, and renewing a certificate.
- Events related to the cryptographic module life cycle, such as reception, use and uninstallation of the module.
- Request for renewal of the certificate and the resulting action.

Whether manually or electronically, ANF AC records the following information:

- The key generation ceremony and key management databases.
- Physical access records.
- Maintenance and system configuration changes.
- Changes in staff.
- Incidents.
- Records of the destruction of material containing key information, activation data or personal information.
- Possession of activation data, for operations with the CA private key.
- Agreements with the subscriber and any specific choices made in accordance with the subscriber. They are held by the Registration Authorities, available to the CA.
- For all events identified in this section, the audit record shall contain at least:
- The type of event recorded.
- The date and time it was produced.

- For messages from the Registration Authorities requesting actions from the Certification Authority, the identification of the origin of the message, the recipient, and the content.
- For requests for issuance or revocation of certificates, an indicator of the grant or denial of the request.

4.12.3 Types of events recorded in the key management life cycle

The following events related to the management of the life cycle of the keys are recorded:

- How the keys were generated.
- The installation of manual cryptographic keys and their results (with the identity of the operator).
- The key backup of the CA.
- The storage of CA keys.
- The recovery of CA keys. Key CA activities of custody (if applicable).
- The use of CA keys.
- CA key files.
- Removal of key material from the service.
- Destruction of the CA key.
- The identity of those responsible for manipulating any material associated with the keys (such as key components, portable devices that store keys, or means of transmission).
- Custody of keys, devices or means of use of keys and possible compromise of a private key.

4.12.4 Types of events recorded related to the cryptographic device

The following events related to the cryptographic device are logged:

- Reception and installation of the device.
- Connecting or disconnecting a storage device.
- Activation of the device and use.
- The installation process.
- The designation of a device for service and repair.

- The end of the device's life cycle.

4.12.5 Types of events recorded in the use of the subscription

The following events related to the use of the subscription are recorded:

- How the keys were generated.
- Distribution of keys.
- Security copies of keys.
- Storage of keys.
- Destruction of keys.

4.12.6 Types of information to be recorded by the RA during certificate applications

The following information is registered and required to the Recognized RAs by ANF AC:

- The method of identification applied.
- Registration of unique identification data (e.g. National/Foreign Citizens ID card or other identification documents, if applicable).
- Digitized and signed copy of the documents submitted by the subscriber.
- Identity of the AR operator who processes the request.
- Place of storage of copies of applications and identification documents.
- The identity of the operator accepting the request.
- Method used to validate identification documents.
- Name and identifier of the RA that performs the processing.
- The acceptance of the subscriber of the Subscription Agreement, the consent of the subscriber to allow the CA to maintain in its repositories the records containing personal data, the possible authorization for third party access to these records, and the publication of the certificate.
- Place of storage of copies of applications and identification documents.

4.12.7 Types of information on keys life cycle management

The following information is recorded:

- Receipt of certificate requests.
- Requests for initial certificates, requests for renewal and regeneration of request keys.
- Public key requests for certification.
- Generation of certificate.
- Distribution of the public key.
- Certificate revocation requests.
- Generation and publication of certificate revocation lists.

This CA does not record information about reactivation of certificates, since the temporary suspension is not authorized, and the revocation is permanent.

4.12.8 Types of recorded security events

The following events are recorded:

- Safety profile changes.
- Use of authentication and authentication mechanisms, both authorized and denied (including multiple authentication attempts denied).
- System failures, hardware failures, and other anomalies.
- Measures taken by individuals in trusted roles, computer operators, system administrators, and system security officers.

4.12.9 Frequency of processing of audit records

The auditor periodically reviews audit records.

The processing of audit records consists of a review of the records (verifying that they have not been manipulated), a random inspection of all the registry entries and a deeper investigation of any alert or irregularity in the records.

The incidents detected are documented, detailing the measures taken and the personnel involved in the decision-making process.

There is an access control to the audit tools, thus avoiding the use or abuse of these. The use or access to these tools is only performed by the responsible persons with special authorization.

4.12.10 Period of retention of audit logs

Audit records are retained on the premises, after being processed, for a minimum of three months. They are then filed in accordance with section 4.13.2 of this policy.

4.12.11 Audit logs protection

Log files, both manual and electronic, are protected from readings, modifications, deletions, or any other type of unauthorized manipulation, applying logical and physical access controls. The private keys used for the audit log are only intended for this purpose.

These protection measures preclude the elimination of audit records prior to the expiration of their storage period.

4.12.12 Audit log back-up procedures

Backups of the audit logs are done per the measures established for the backups of the Databases.

4.12.13 Audit information collection system (internal vs. external)

Log files are stored on internal systems by a combination of automatic and manual processes executed by PKI applications.

List of risks covered:

- Insertion or fraudulent alteration of a session record.
- Fraudulent suppression of intermediate sessions.
- Insertion, alteration, or fraudulent suppression of a historical record.
- Insertion, alteration, or fraudulent deletion of the record of a table of queries.

4.12.14 Notification to the subject that caused the event

Automatic notification of the action of the audit log files to the cause of the event is not provided.

4.12.15 Vulnerability analysis

A periodic vulnerability analysis is carried out on all ANF AC internal systems.

4.13 Information and log storage

All information regarding certificates is kept for an appropriate period of time, as set forth in section 5.5.2 of this document.

It should be noted that in relation to confidential documentation, ANF AC does not use paper documents in its work activity. All documents are dematerialized, coded per their security level, and stored in secure repositories created for such purpose.

The paper support is stored in closed warehouses, only accessible to expressly authorized personnel, and they have permanent security 24/7/365, with monitoring system and alarms.

4.13.1 Type of recorded events and information stored

ANF AC saves all events that occur during the life cycle of a certificate, including renewal.

The certification service provider must keep a record of at least the following information:

- Data related to the registration procedure and the request for certificates.
- The audit records specified in this document.
- Incidents detected.

4.13.2 Retention period for the file

ANF AC saves all logs specified in the previous section of this policy for a period of at least 15 years.

4.13.3 Protection of file

The measures of protection of the archive are adopted, so that its contents cannot be manipulated or destroyed.

4.13.4 File backup procedures

ANF AC makes daily incremental backup copies of all its electronic documents, complete weekly backups, and monthly historical copies are safeguarded.

There is a backup policy that defines the criteria and strategies for action against an incident.

4.13.5 Requirements for time-stamping of records

The information systems used by ANF AC guarantee the registration of the time in which they are made. The instant of time of the systems comes from a reliable source that verifies the date and time.

The clock signal is synchronized with the Royal Institute and Observatory of the Navy - San Fernando (Cadiz), "ROA", which is responsible for maintaining the basic unit of Time, declared for legal purposes as the Spanish National Patron of such unit, as well as the maintenance and official dissemination of the "Coordinated Universal Time" (UTC (ROA)) scale, considered for all purposes as the basis of the legal time in the entire Spanish national territory (Spanish Royal Decree 23 October 1992, number. 1308/1992).

This lab maintains several servers that distribute the time through the NTP protocol. This system of high stability and precision uses a set of cesium atomic patterns, which allow to know the UTC time with a precision superior to the microsecond, and with a stability of 32 s/year.

At least once a day all systems are synchronized with this source.

4.13.6 Audit information storage system (internal or external)

The information collection system is internal and belongs to ANF AC.

4.13.7 Procedures to obtain and verify stored information

Access to this information is restricted to authorized personnel for this purpose, protecting against physical and logical access.

4.14 Renewal of certificates or keys of a CA

The validity of the CA certificate is superior than the period of validity of the certificates it issues, so that certificates cannot be issued whose validity period exceeds the validity of the CA certificate issuing them.

Prior to the expiry date of a CA certificate, ANF AC may proceed to renew the certificate with or without re-key. Said process will always start at least 36 months before expiration and end 24 months before.

4.14.1 Renewal of certificates without key change

The renewal of the certificate without re-key is based on the creation of a new certificate of CA with a new period of validity, but retaining the same cryptographic keys. This renewal strategy allows the hierarchy (current and renewed) to be used interchangeably to validate all certificates that have been issued by these certification hierarchies.

Both certificates are valid until their expiration date. Both certificates use the same private key, the same public key, the same CA name, and share the same CRL. This certification model with shared keys is called "Cross Certification*[1]".

Thus, issued certificates can be validated with either hierarchy, but in case of a CRL query, each hierarchy publishes its specific CRL and ARL.

4.14.2 Renewal of certificates with re-key

The rekeying will take place before the CA certificate expires. Changes in the content of the certificate may be made to best comply with current legislation, the PKI of ANF AC and the reality of the market. This procedure generates a new CA with a new private key.

The old CA and its private key will only be used for CRL and ARL signing as long as there are active certificates issued by this CA.

4.15 Recovery in case of key compromise or disaster

There is a Business Continuity and Disaster Recovery Plan, OID 1.3.6.1.4.1.18332.13.1.1, which defines the actions to be performed, resources and personnel to be used in the event of an intentional or accidental event that would render useless or degrade the resources and certification services of ANF AC. The main objectives of the Business Continuity and Disaster Recovery Plan are:

- Maximize the effectiveness of recovery operations by establishing three phases:
    - Notification/Evaluation/Activation Phase to detect, evaluate damages and activate the plan.
    - Recovery Phase to restore services temporarily and partially until the recovery of damages caused in the original system is done.
    - Reconstitution Phase to restore the system and processes to their normal operation.

- Identify the activities, resources, and procedures necessary for the partial provision of certification services.
- Assign responsibilities to the personnel designated by the Safety Committee and provide a guide for the recovery of normal operations.
- Ensure coordination of all operators involved in the planned contingency strategy.

The damage assessment and action plan are described in the Business Continuity and Disaster Recovery Plan.

It will be informed to the subscribers and other entities with which ANF AC has agreements or relationship in case of compromise.

In the event of weakness of the cryptographic system: the algorithm, the combination of the key sizes used or any other technical circumstance that significantly weakens the technical security of the system, will be applied as defined in the Business Continuity Plan and Disaster Recovery.

4.15.1 Alteration of hardware, software or data resources

When an event of corruption of resources, applications or data takes place, a procedure will be activated that would allow to initiate the necessary steps, per the Business Continuity and Disaster Recovery Plan that includes the strategy of action in this type of situations.

4.15.2 Entity public key revocation

In case of revocation of one of ANF AC's Hierarchies, the following will be carried out:

- Notify this fact, when it occurs, to the General State Administration.
- Report the event by publishing an ARL.
- Make every effort to report the revocation to all subscribers to whom the certification service provider issued certificates, as well as third parties wishing to rely on those certificates.
- Perform a re-key and carry out an electronic transmission of it, in the event that the revocation was not due to the termination of the service by the certification service provider, as established in this CPS.

The causes of revocation contemplated in this section can be by compromise of key, technical reasons, organizational reasons, or disaster.

4.15.3 CA private key compromise

ANF AC's Business Continuity Plan contemplates compromise or suspicion of compromise of a CA's private key as a disaster.

In case of an intermediate or subordinate CA compromise, the following actions must be performed:

- Verify the compromise and, in case of confirmation, inform all subscribers.
- Indicate that certificates and revocation status information that have been delivered using the CA key are no longer valid.
- Proceed in accordance with section 4.9.11

If the compromised key is the root CA, the certificate will be removed from all applications and a new one will be distributed.

ANF AC's Business Continuity Plan establishes that, in case of compromise of the CA key, the associated certificate shall be immediately revoked, and all certificates issued with that certificate will also be revoked, offering to the final entities the possibility of having a new certificate issued by a new CA, free of charge and for a period of time equal to the remainder of life.

In addition, a free reissuing service will be offered for signed documents with revoked certificates.

4.15.4 Security Installation after a natural disaster or other type of disaster

ANF AC's Business Continuity and Disaster Recovery Plan develops, maintains and contemplates the possibility of testing and, if necessary, executing an emergency plan in the event of a disaster, whether due to natural or human causes, on the facilities, which indicates how to restore information systems services.

The systems and facilities defined in the Business Continuity Plan and Disaster Recovery have the physical protection required.

ANF AC's Business Continuity and Disaster Recovery Plan establishes the capacity to restore the normal operation of revocation services and, if necessary, suspension, within 24 hours after the disaster, and at least the following actions may be executed:

- Suspension of certificates.
- Revocation of certificates (if applicable).
- Publication of revocation information.

The disaster recovery database used by the certification service provider must be synchronized with the production database within the time limits specified in the provider's security plan.

The disaster recovery systems of the certification service provider have the physical security measures specified in the security plan.

4.16 Certification Services Provider Termination

In accordance with article. 24.2.a (i) of Regulation (EU) 910/2014, ANF AC follows the recommendations expressed in the reference standards.

To minimize the effects to the Recognized Registry Authorities, to the subscribers and to third parties because of the cessation in the provision of services. ANF AC undertakes to carry out, as a minimum, the following procedures:

- Notify at least ninety days in advance to the holders of electronic signature certificates and regulatory control bodies on the termination of its activities.
- Inform all subscribers and relying parties of the certificates they have issued. To do so, during a period of ninety days, there shall be a publication, in this sense, on the main page of the corporate website.
- Remove any authorization to subcontractors acting on behalf of the certification service provider in the process of issuing certificates.
- Execute the necessary tasks to transfer the maintenance obligations of the registration information and the event log files, during the respective periods of time indicated to the subscriber and to relying parties.
- Destroy the private keys of all CAs.
- Revoke all issued CA certificates.
- Transfer of the obligations of the certification service provider to another certifying entity, for which it must have the express authorization from the certificate holder.

If the activity is not transferred to another certification entity or the holder does not authorize this process:

- The certificate will be revoked in advance.
- The lists of revoked certificates will be kept online for a period of not less than five years.
- An escrow in a notary public will be made of the certificate revocation lists and of the necessary means to verify the validity of the certificates and electronic signatures made with them.
- Termination of the Recognized Registry Authority, pursuant to the provisions of section "4.17 Termination of the Registration Authority".

4.17 Termination of the Registration Authority

The framework of collaboration of ANF AC with its Recognized Registry Authorities [RRAs] is formalized through the corresponding agreement that states their "Obligations and Responsibilities". The ARR, formally undertakes among other issues to:

- Notify at least thirty days in advance to ANF about the termination of its activity.
- To cease its activity as RRA at the same moment in which it communicates its intention to cease its activity, or at the moment in which ANF AC notifies the revocation of its accreditation as RRA.

Immediately, it will communicate the corresponding order of cessation of the activity to all its RA Operators.

- Within thirty days from the notification of cessation of activity, the RRA will proceed to deliver to ANF AC all material related to the activity developed as ARR, removing from its physical and computer files any information and content related to its work as ARR.
- Provide maximum collaboration and transparency in case it is required to carry out an internal security audit to ensure that all obligations such as RRA have been adequately addressed.

4.18 Termination of the RA Operator

The framework of collaboration of ANF AC with the RA Operators, is formalized by means of the corresponding agreement that states their "Obligations and Responsibilities". The RA Operator, formally undertakes among other issues to:

- Notify at least fifteen days in advance to the RRA Office to which it is attached, on the termination of its activity as an RA Operator.
- To cease its activity as an R Operator at the same moment in which it communicates its intention to cease its activity, at the moment in which the RRA Office so orders, or when ANF AC communicates the revocation of its accreditation as an RA Operator.
- Within fifteen days from the notification of cessation of activity, the AR Operator will proceed to deliver to the AR Office to which all the material related to the activity developed as AR Operator is attached.

Provide maximum collaboration and transparency in case it is required to perform an internal security audit to ensure that all obligations as an RA Operator have been adequately addressed.

4.19 Subscription Termination

The certificate when its term expires or when it has been revoked, ceases to be valid for its use.

Each Certification Policy specifies the expiration of the different certificates.

5 Physical security, facilities, management, and operational controls

5.1 Physical controls

Controls are maintained in all places in which ANF AC provides services.

5.1.1 Location and construction

The buildings where the ANF AC's infrastructure is located have access control security measures, so that entry is not allowed unless the persons have been duly authorized.

Facilities in which information is processed meet the following physical requirements:

a) The building containing the information processing units is physically solid, the outer walls of the site are solidly constructed and only access to duly authorized persons is allowed.

b) All doors and windows are closed and protected against unauthorized access.

c) The generation of the keys and the issuance of CA certificates is done in a Data Processing Center with adequate protection measures per the requirements established in the ANF AC's ISMS policies. This property has a physical structure that fully guarantees that the place is free of electromagnetic radiation, has 24x7x365 security service and multiple barriers that prevent access to unauthorized persons.

d) The computer equipment that serves the public (main and mirrors) are installed in a Data Processing Center belonging to a national communications company, with adequate facilities for such purpose, and that has adequate infrastructure to guarantee a stable, secure, and continued service.

e) The building where the central infrastructure of ANF AC is installed, it's a physically secure enclosure, equipped with up to six security levels to be able to access critical machines and applications.

   The systems are physically separated from other existing ones in the place, so that only authorized personnel of ANF AC can access them, thus guaranteeing the independence of other equipment and third-party systems housed in the place.

f) Among the protection measures that these facilities have, it should be noted that:

   - The facilities have an independent surveillance service to ANF AC of 24 hours and control by permanent closed circuit television. Cameras are not able to view the operations

performed on ANF AC's servers to avoid any risk of displaying the activation PINs when they are entered or other confidential data.

- Their location is far from basements, to prevent possible flooding.
- The building is a modern building, built for the purpose and for the exclusive use of the operator. Located in a business area of recognized prestige, of an easy and quick access, if necessary, for the services of Public Order and Firefighters.
- The building is in an area of low seismic activity and without a history of natural disasters.
- The building is in an area of low levels of delinquency.
- Neither the building nor the area where it is located are considered terrorist targets.
- The facilities do not have windows to the exterior.
- The premises are constantly protected by personnel belonging to a security company authorized by the Ministry of Interior.

  This staff has a detailed and up-to-date list of the people that ANF AC authorizes to access the central core (where ANF AC computers are located), and make a record of the date and time of entry and exit, identity and signature of the person that access and of each one of the people that accompany him/her, delivering card of personal access. In no case, it allows the extraction of computers without express authorization.
- Access to the central core is performed by overcoming different controls. The personnel that access is at all times accompanied by personnel responsible for the administration of the data center and any work that is done on the computer equipment of ANF AC is carried out in the constant presence of a technician belonging to the personnel responsible for the administration of the center of data.
- All facilities have redundant power and air conditioning systems that meet industry standards to create a proper operating environment.
- All facilities have prevention mechanisms to reduce the effect of contact with water.
- All facilities have fire prevention and protection mechanisms. These mechanisms comply with industry standards.
- All wiring is protected against damage or electromagnetic interception or interception of both data and telephony transmission.
- The screens that protect the central areas of the core are transparent and have permanent illumination, to allow observation from surveillance cameras or from corridors

or even administrative offices, thus preventing illegal activities inside the Center Data Processing (Datacenter).

5.1.2 Physical access

- Physical security perimeter:

  In addition to the measures outlined above, customized access control systems have been implemented, which record the passage of people through each zone. Likewise, it has been established that the visiting staff must be permanently supervised by a person in charge of the data center.

- Physical access controls:

  There is an exhaustive physical control system for people at the entrance and exit that forms several safety rings, and is regularly checked.

  Various safety systems, human and technical, are combined in the realization of the physical access controls:

  - Access to the entrance identified with their the National/Foreign Citizens ID card by the security service, monitoring and registering the person, time of arrival, departure, authorization, and a personal identification number.
  - Use of their personal number for identification before the security devices, verifying authorization and registering access.
  - Entry is not allowed unless the persons have been duly authorized by a member of the PKI Board, the Security Manager, the Technical Director, or the Legal Officer.

- Introduction or removal of equipment:

  Authorization of the Security Manager is required for carrying out these operations, taking an inventory of the existing material and the inputs and outputs that have occurred.

- ANF AC implements controls to prevent losses, damages or compromise of assets, and disruption of activity, in accordance with the Business Continuity and Disaster Recovery Plan.

5.1.3 Power and air conditioning

The rooms, where the equipment that makes up the ANF AC's certification systems are located, have sufficient electricity and air conditioning to create a reliable operating environment. The installation is protected against power failure or any power anomaly by means of an auxiliary line independent of the main electrical source.

Mechanisms have been installed that keep the heat and humidity controlled at levels corresponding with the equipment installed on site.

Those systems that require it, have uninterruptible power and generator sets.

The facilities where the certification servers are located, and where the process of issuing certificates of final entity and CA is performed, have the following features:

- Servers providing certification services have a system to protect against power failure and other electrical anomalies, and the entire wiring system is protected against interception and damage.
- The equipment for issuing certificates is permanently disconnected from the power supply, and for its activation only autonomous power supplies are used, free of any possible anomalies.

5.1.4 Water exposures

Suitable measures have been taken to prevent water exposure to all equipment and cabling.

5.1.5 Fire prevention and protection

The rooms have the appropriate means - detectors - for the protection of their content against fires. The wiring is in false floor or ceiling and the appropriate means are available - detectors in floor and ceiling - for the protection of the same against fires.

5.1.6 Media storage

ANF AC has established the necessary procedures to have backup copies of all the information of its productive infrastructure.

Plans have been established for the backup of all sensitive information and of that considered as necessary for the persistence of its activity.

ANF AC stores and holds all the certificates it has issued for a period never less than 15 years after the loss of validity thereof.

5.1.7 Waste disposal

ANF AC has developed a policy that guarantees the destruction of any material that might contain information, as well as a policy for the management of portable media.

Media containing confidential information is destroyed in such a manner that the information is irrecoverable after its disposal.

5.1.8 Off-site backup

The storage of the backups outside the premises, is done in bank bunker.

Each storage device has a unique identifier, description, model, and brand.

5.1.9 Safety security box

ANF AC has contracted, in a Spanish bank, a safety security box in which copies of the devices that allow the regeneration of the system in case of loss are deposited.

Access to the Security Box is restricted to authorized personnel of ANF AC, who have in their possession one of the keys that allows the opening of the safety security box.

Among the protection measures that these banking facilities have, the following are stated:

- The facilities have a 24-hour surveillance service and is controlled by permanent internal TV circuit.
- The architecture and armor of the building correspond to the design commonly used in establishments called "banking bunker".
- The premises are constantly protected by personnel belonging to a security company authorized by the corresponding department of the Ministry of Interior.
- The personnel to which the bank entrusts with the administration of the accesses makes a record of the day and time of entry and exit, identity and signature of the person who accesses.
- Access to the central core is performed by overcoming different controls. The personnel that access is at all times accompanied by the staff responsible for the administration of the bank bunker and the operation of opening the bank is done by double key: one held by the staff of ANF AC and another by the staff of the bank.
- All facilities have energy and air conditioning systems, which comply with the applicable regulations.
- All facilities have fire prevention and protection mechanisms. These mechanisms comply with industry standards.
- Access to the safety security box requires the presence of at least two authorized operators and the use of the master key of the bunker supervisor.

5.1.10 Security against intruders

The facilities where the certification servers are located, and where the process of issuing certificates of final entity and CA is performed, have fire doors, intrusion detection systems are installed and are regularly tested to cover all exterior doors of the building.

The facilities that host the servers are permanently operational, 24 hours 365 days a year.

Likewise, the installations where the processes of generation of keys of the CA, and emission of certificates are performed, have security measures and alarms to avoid any type of raid.

For the identification of terminals and, in particular, portable equipment, a model has been established per the location of the terminal, and in accordance with the sensitivity of the services to which it is intended:

Local access: The identification is made by authentication based on electronic signature technology, accessing by internal IP and prior authorization control of the MAC of the terminal.

Remote access: Only equipment configured for this purpose can be accessed, and depending on the sensitivity of the service, access to certain previously authorized IPs is restricted.

5.1.11 Terminal security

For the identification of terminals and portable equipment, a model has been established per the location of the terminal, and in accordance with the sensitivity of the services to which it is intended:

- Local access: The identification is made by authentication based on electronic signature technology, accessing by internal IP and prior authorization control of the MAC of the terminal.
- Remote access: Only equipment configured for this purpose can be accessed, and depending on the sensitivity of the service, access to certain previously authorized IPs is restricted.

5.2 Procedural controls

ANF AC manages access to information processing systems, to duly authorized operators, administrators, and auditors of the system. These controls include the management of user accounts, modification, or timely removal of access.

5.2.1 TSP

ANF AC has a policy to control access to information. The functions of the application system are restricted by its Information Security Management System (ISMS).

- The ISMS define sufficient security controls and establishes separation of roles, identifies responsibilities, performs a separation between security management and operations functions. It establishes rules that restrict and control the use of system utility programs.
- All staff of ANF AC is identified and authenticated before using critical applications related to the service.
- System operators are responsible for their activities, for example, retention of event logs. ANF AC has a personnel policy that includes disciplinary measures and procedures.
- The Safety Committee contemplates and supervises the adoption of appropriate measures in the treatment of risks, considering from commercial to technical personnel, ensuring that the level of information security is proportional to the level of risk.

5.2.2 PKI control and management roles

The following persons are responsible for the control and management of the system:

a) Responsible for issuing certificates.

b) Area Directors.

c) Systems administrators.

d) Operators of the Certification Authority.

e) Responsible for selection and training.

f) Security Manager

g) Auditors.

h) Responsible for the elaboration of issuance reports and revocation of certificates.

i) Documentation responsible.

5.2.2.1 Certificate issuance managers

There is a minimum of four operators that have the capability to access and activate ANF AC's certificate issuing devices.

To activate the keys, the presence of at least two persons is required per the dual control requirement.

5.2.2.2 Area managers

They are the people who assume the management of each section of ANF AC. Under their control and supervision, the personnel assigned to them are located. It's their responsibility:

- Receive and follow up on complaints for infractions that may affect their staff, proposing appropriate disciplinary measures.
- Conduct a permanent control of the adequacy of material and human resources that the Department has, to meet the service needs it has been entrusted with.
- Managers must have experience or training in relation to the trust service provided.

5.2.2.3 Systems administrators

It is staff assigned to the area of Computer Technology and Telecommunications. None of them are involved in internal audit tasks. It's their responsibility:

- Installation and configuration of operating systems, software products and maintenance and updating of installed products and programs. They can install, configure, and maintain reliable TSP systems, but without access to data.
- Activate CRL, OCSP and Timestamping services through specific certificates.
- Establish and document the procedures for monitoring the systems and the services they provide, as well as the control of the tasks performed by the Certification Authority Operators.
- The design of the programming architectures, the control and supervision of the developments entrusted and the correct documentation of the applications.
- To supervise the correct execution of the Copy Policy to maintain sufficient information to be able to restore any of the systems in the shortest possible time, to ensure that local backups are carried out and per the provisions of the Security Plan.
- Maintain the inventory of servers and other components of ANF AC certification systems.
- Management of router services and of firewall rules, management and maintenance of intrusion detection systems, and other related tasks.
- The installation or removal of cryptographic hardware from the CA.
- Maintenance or repair of CA's cryptographic equipment (including installation of new hardware, firmware or software), and removal of disposables.

- PKI operators involved in day-to-day management of systems, are authorized to perform backups and recoveries for the proper functioning of the CA infrastructure.

5.2.2.4 Certification Authority operators

- They work in the administrative area.
- They perform administrative tasks which require no physical access to Certification Servers.
- They carry out traditional administrative tasks: filling, data entry, reception and sending of mail, receiving visitors and telephone calls, etc.
- Essentially, they collaborate in all those functions that are required by the area managers, under whose criteria their work is organized and delegation of responsibilities.
- They must have undergone specific training in data protection and computer security, passing the corresponding tests. A minimum of one year's experience in administrative duties is required.

5.2.2.5 Training and selection manager

- Assigned to the legal area.
- Keeps up-to-date the training plans of the personnel that provides their services in ANF AC.
- Supervises the performance of the training and degree of confidence of the personnel and carries out the tests necessary to be able to evaluate the appropriate level of assimilated knowledge.
- Manages the selection of new personnel, controlling the obtaining of references and compliance with established levels.
- Minimum experience of one year is required in this type of duties.

5.2.2.6 Security manager

As defined in the ISMS Policy:

- General responsibility for managing the implementation of security practices.
- Controls the formalization of agreements between staff and ANF AC.
- Communicates agreed disciplinary measures, monitoring their compliance.
- Must enforce ANF AC's security policies, and must take care of any aspect of the PKI's security, from physical security to application security, to network security.

- He/she is responsible of managing the perimeter protection systems and of verifying the correct management of the rules of the firewalls.
- He/she is responsible for verifying the correct installation, configuration, and management of intrusion detection systems (IDS) and associated tools.
- He/she is responsible for solving or having resolved security incidents, eliminating detected vulnerabilities, and other related tasks.
- He/she is responsible for the management and control of physical security systems, and material movements outside the premises of the CA.
- Must make the selection and determine the contracting of third party specialists who can collaborate in improving the safety of ANF AC.
- Minimum experience of one year is required in these functions.
- Should be familiar with security procedures, information security and risk assessment.

5.2.2.7 Auditors

- Assigned to the legal area and to the area of Computer Technology and Telecommunications.
- Perform internal audit functions.
- Assume the responsibility of performing the internal audit in accordance with the Standards and Audit Criteria of the Certification Services (ANF AC).
- They can access the (records and files) of the system.
- A minimum of being assigned one year to the legal area and/or to the Computer Technology and Telecommunications area is required.

5.2.2.8 Issuance reports and certificates revocation manager

He/she is responsible for validating the petitions, and for ruling on the issuance of a certificate. A minimum of being assigned to the legal area is required.

5.2.2.9 Documentation manager

- Assigned to the administrative area.

- Controls that the ANF AC's electronic documentation repository and paper documentation files are up to date.
- Supervises document updating when necessary.
- It is the only one allowed to store, delete, or modify documents in ANF AC's documentation repository.
- A minimum of being assigned to the administrative area is required.

5.3 Personnel controls

5.3.1 History, qualifications, experience, and authentication requirements

In accordance with the provisions of the Administrative Security Plan.

The Administrative Security Policy and the CPS establish the personnel configuration necessary to adequately carry out CA operations. It always follows the principle of certain necessity to grant an access authorization in a transactional CA. The area managers are the people in charge of establishing in each moment the number of operators, the qualification that they must possess per the work to realize, and to select the identity of the same ones.

In particularly sensitive operations, redundant personnel will always be available. These are personnel who have received the training necessary to deal with this type of operations, and whose number is always higher than what is necessary to deal with any incidence.

ANF AC has a Personnel Policy that supervises that the operators of the PKI, are free of conflicts and personal interests, that can damage the impartiality in the functions that are entrusted to them.

5.3.2 Background verification procedures

In accordance with the provisions of the Administrative Security Plan, it should be noted that contractors performing functions of trust are subject to the same plan.

Staff will not have access to trusted functions, until the controls defined in the Personnel Policy are completed.

5.3.3 TSP personnel shall be formally appointed to the trust functions by senior management responsible for security

ANF AC has a Roles Policy that determines the minimum privileges that an area manager must have to grant and configure access privileges.

5.3.4 Training requirements

ANF AC regularly develops, at least every twelve months, training exercises aimed at personnel involved in CA systems. This training may include a combination of training, credentials, or experience in the development of the functions entrusted to it. Maximum attention is given to training on the following aspects:

- Access control.
- Storage management.
- Record of incidents.
- User Registration.
- Identification and authentication.
- Backup and recovery.
- Analysis of files, data, and computer systems.
- Security system access to computer terminals.
- Administrative Security. Security plan.

The following aspects are included in the training:

- Delivery of a copy of the Certification Practice Statement.
- Awareness of physical, logical, and technical security.
- Software and hardware operation for each specific role.
- Security procedures for each specific role.
- Operating and administration procedures for each specific role.
- Procedures for recovery of PKI operation in case of disasters.
- Security and protection of personal data.

5.3.5 Requirements and frequency of training update

Per ANF AC's Annual Training Plan.

5.3.6 Job rotation frequency and sequence

Not stipulated.

5.3.7 Sanctions for unauthorized actions

The personnel are subject to a process of disciplinary regime previously noticed and known by all the operatives of the organization. The operation of the procedure followed is documented in the Sanctions Policy (OID: 1.3.6.1.4.1.18332.39.14.2).

The performance of unauthorized operations, breach of policies or procedures is subject to disciplinary measures. The sanction can lead to dismissal, regardless of what is established in the legislative framework that can lead to a claim before Judicial Authority.

5.3.8 Third parties contracting requirements

All personnel with access to ANF AC certification services sign a confidentiality agreement as part of the terms and conditions of their incorporation.

This agreement provides information on the work of control and inspection that ANF AC's security officers permanently carry out on personnel, software, and hardware.

The purpose of this activity is to guarantee the highest degree of security of the services that this CA provides, and of the assets that it has the obligation to protect.

5.3.9 Documentation provided to the personnel

Access to the mandatory security regulations will be facilitated, which the employee will sign, together with this CPS and the regulations contained in the CPs that are applicable.

5.3.10 Unauthorized activities

Unless expressly authorized, he/she is not allowed to install, use or request information on instruments that can be used to evaluate or compromise the safety of ANF AC certification systems. The installation or use, without express authorization, of instruments that have as an end any attempt to evaluate the services used or received by ANF AC is not allowed.

This prohibition extends to any attempt to verify or attempt to compromise ANF AC's safety measures, even if no instrument is used. In the same way, it extends to the unauthorized evaluation of the services provided or received from ANF AC, whether or not devices are used to that effect.

It is also expressly prohibited the use of software or hardware that is not expressly authorized by the company, as well as the installation, storage, or distribution by any means.

It is forbidden to communicate to another person the user ID and password. If the user suspects that another person knows his/her identification and access data, he/she must activate the mechanisms of change of password.

The user is obliged to use the data, corporate network and/or intranet of the entity and/or third parties without incurring in activities that may be considered illegal or illegal, that infringe the rights of the company and/or third parties or which may violate the morality or etiquette rules of computer networks.

Also, it is not allowed:

- Share or facilitate the user ID and password provided by the Entity to another natural or legal person. In case of non-compliance with this prohibition, the user will be solely responsible for the acts performed by the natural or legal person that uses their user identification in an unauthorized way.
- Try to decrypt the encryption key, systems or algorithms and any other security element that intervenes in the Entity's computer processes.
- Attempting to read, delete, copy, or modify e-mail messages or other users' files.
- Attempt to distort or falsify system log records.
- Use the system to try to access restricted areas of the Entity's computer systems and/or third parties.
- Attempt to increase the level of privileges of a user in the system.
- Destroying, altering, rendering useless or otherwise damaging the data, programs, or electronic documents of the Entity or third parties.
- The user must not store personal data on the computer's hard disk, but use the assigned corporate network folders for this purpose.
- Voluntary obstruct the access of other users to the network through the massive consumption of the computer resources of the organization, as well as actions that damage, interrupt or generate errors in these systems.
- E-mail massively for commercial or advertising purposes without the consent of the recipient.

- Voluntarily introduce programs, viruses, macros, applets, ActiveX components or any other logical device or sequence of characters that causes or is likely to cause any type of alteration in the company's computer systems or third parties. In this regard, it should be remembered that the system itself automatically runs anti-virus programs and their updates to prevent entry into the system of any element intended to destroy or corrupt computer data.
- Introduce, download from the Internet, reproduce, use, or distribute computer programs not expressly authorized by the company. This prohibition includes any other type of work or material whose intellectual or industrial property rights belong to third parties, when authorization is not available.
- Install illegal copies of any program, including those that are standardized.
- Delete any legally installed programs.
- Send or forward messages in chain or pyramid type.
- Use the company's computer resources, including the Internet, for activities that are not directly related to the user's workstation.
- Introduce obscene, immoral, or offensive content and, in general, not useful for the objectives of the company.
- Encrypt information without being expressly authorized to do so.
- Physical or logical access to ANF AC's facilities outside of their working hours.

5.3.11 Periodic compliance controls

In accordance with the provisions of the Administrative Security Plan.

5.3.12 Expiration of contracts

In accordance with the provisions of the Administrative Security Plan.

6 Technical security controls

ANF AC uses reliable systems and products, which are protected against any alteration and that guarantee the technical and cryptographic security of the certification processes that they support.

For the development of its activity as a Certification Services Provider, ANF AC has a R&D Department, and a cryptographic section that determines the security status of all cryptographic elements used in its PKI.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The root and subordinate CA cryptographic keys must be generated in a cryptographic hardware module (HSM) that complies with FIPS 140-2 level 3 (or higher) and Common Criteria EAL 4+ on the corresponding protection profile.

The cryptographic keys of the VA must be generated in a cryptographic hardware module (HSM) that complies with FIPS 140-2 level 3 (or higher) and Common Criteria EAL 4+ on the corresponding protection profile.

The cryptographic keys of the TSA must be generated in a cryptographic hardware module (HSM) that complies with FIPS 140-2 level 3 (or higher) and Common Criteria EAL 4+ on the corresponding protection profile.

ANF AC guarantees that the cryptographic hardware module used, in accordance with the previous sections, has not been manipulated during the sending, reception, or storage. On the other hand, the installation, activation, backup, and recovery of the keys in the cryptographic hardware module requires the simultaneous control of two trusted employees of ANF AC. Also, ANF AC guarantees that the CA signature keys stored in the cryptographic hardware are destroyed when the device is removed; This destruction does not affect all copies of the private key, only the key stored in the cryptographic hardware in question.

Cryptographic keys of CA, VA, TSA, and end users must be generated following the minimum algorithm and key length recommendations defined in ETSI TS 119 312.

ANF AC provides its end users with two types of devices:

- Token cryptographic software.
- HSM token incorporating a cryptographic hardware module that complies with FIPS 140-2 level 3 (or higher) and Common Criteria EAL 4+ on the corresponding protection profile.

ANF AC delivers to its users the cryptographic devices necessary to generate in private and without third party intervention, its key pair and activation data of the same.

In Public Key Infrastructure (PKI) systems, all the robustness of the system weighs on the protection of the private key, ensuring that it is only in the hands of the subscriber, unlike the public key, which as its name indicates, can be distributed without fear and by means of which the third parties will be able to verify the signatures of the subscriber, and to encrypt messages that only the subscriber will be able to read. The private key performs the reverse functions, allows one to sign documents and decrypt data, which is why one must protect its security.

ANF AC does not generate user's private keys and always recommends that this process be performed in a secure environment. ANF AC provides the necessary instructions so that this task can be carried out and tries by all means that its clients do not ask for help to their Recognized Registry Entities as this could imply security breaches.

On the other hand, in the socpe of electronic certificates of centralized signature, ANF AC for the generation of the keys, their storage and later use in the scope of centralized signature, exclusively uses devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS Regulation, and therefore included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

Https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

In addition, ANF provides subscribers with secure communication channels and specific management and administrative security procedures.

6.1.2 Private key delivery to end-entity

In cases where ANF AC generates the cryptographic keys of its users, the procedure of delivery of the private key varies per the type of certificate and device.

Each Certification Policy specifies the method used.

6.1.3 Public key delivery to certificate issuer

The public key is generated by the subscriber and is delivered to ANF AC by sending a certificate request in CSR (Certificate Signing Request) format, which follows the PKCS#10 specification.

6.1.4 CA public key delivery to relying parties

The public key of the Root CA and the Intermediate CA is available to relying parties, ensuring the key integrity and authenticating its source.

The public key of the Root CA is published in the Repository, in the form of a self-signed certificate in the case of Root CA and certificate issued by the Root CA in the case of the Intermediate CA, together with a statement that specifies that the key is authentic to ANF AC.

Additional measures are included to rely on the self-signed certificate, such as the fingerprint verification of the certificate that appears published in this CPS. Users can access the Repository to obtain the public keys of ANF AC through the web https://www.anf.es.

6.1.5 Key sizes

The algorithm used is the RSA with SHA256.

The size of the keys, depending on the cases, is:

- At least 2048 bits, in all cases, for end-user certificate keys, OCSP Responder and Time Stamping Unit.
- At least 4096 bits for CA Root keys and their current CA Intermediate.

End-user certificates are signed with RSA and using SHA-256.

ANF AC uses an algorithm considered qualified by the industry and suitable for qualified signature. The validity period of the certificate will also be considered in addition to the recommendations indicated by the CAB/Forum and the different ETSI standards.

ANF AC has a Business Continuity and Disaster Recovery Plan that will be applied in case the advances of the technique put at risk the technical safety of the algorithms, the size of the key used or any other technical circumstance. In case of possible risk, an impact analysis will be carried out. This analysis will study the criticality of the security problem, its scope, and the strategy of recovery from the incidence.

The minimum points to be included in the impact analysis report are:

- Detailed description of the contingency, temporal scope, etc.
- Criticality, scope.
- Proposed solutions.
- Deployment plan for the chosen solution, which will include at least:
    - Notification to users, both subscribers and relying parties.

- It will be informed on the website of the contingency produced
- Revocation of affected certificates
- Renewal strategy

6.1.6 Supported uses of keys

All certificates include the Key Usage extension and Extended Key Usage, indicating the enabled uses of the keys.

Root CA keys are used to sign the subordinate CAs certificates, and the ARLs. The subordinate or issuing CA keys are only used to sign end-user certificates and CRLs.

Supported key uses for final certificates are defined in the corresponding Certification Policies.

6.1.7 Certificates signature algorithms

The algorithm identifier (AlgorithmIdentifier) that ANF AC uses to sign the certificates is SHA-256 (hash algorithm) with RSA (signature algorithm) corresponding to the identifier for "Identifier for SHA-256 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc. " The padding scheme used is emsa-pkcs1-v2.1 (per RFC 3447 section 9.2) ".

SHA1 Sunset

ANF Certification Authority, as a member of CABForum, adheres to the policy of ceasing the use of cryptographic algorithms that the industry considers potentially breachable. That is why this schedule has been set for using the SHA1 digestion algorithm in favor of its evolution, SHA2 (SHA256 - SHA512).

Root Certificates

Although there is no international agreement to set a date for the end of the use of SHA1 in root certificates, due to the complexity of the change of the same, since they are integrated in multiple platforms both software and hardware, very difficult to update, **ANF AC decided in the year 2013**, for the issuance of the new **ANF Global Root CA**, to use the **SHA1 algorithm and resign to SHA256** with a key length of **4096 bits**. These certificates will be valid until **June 5, 2033**.

These certificates are the root of the hierarchy of certification under which all certificates approved in the European Union are issued.

It is established that, if at any time the algorithms or key lengths used by the root certificates are compromised, the PKI's Governing Board will order the resigning of all the certificates in that situation.

Intermediate Certificates

The CAB Forum established a ban on Cas, that follow the BaselineRequirements, from issuing intermediate authority certificates with SHA1 algorithm as of **January 1st, 2016.**

The **ANF Global Root CA hierarchy** has 4 Intermediate Authorities (CA IA), all with **SHA1**, **SHA256** algorithm, and **4096-bit** key length. The expiration of the four is **July 23, 2023**.

These intermediate authorities are:

- ANF Assured ID CA1
- ANF Global CA1
- ANF High Assurance AP CA1
- ANF High Assurance EV CA1 It is established that if the algorithms or key lengths used by intermediate certificates are compromised at any time, the Governing Board of the PKI will order the reissuing of all certificates in this situation.

End Entity Certificates

As with IA certificates, in the final certificates it was established not to issue certificates with SHA1 algorithm as of **January 1st, 2016**.

Furthermore, for these user certificates, from **January 16th, 2015** it shall not be issued certificates with SHA1 algorithm expiring after January 1, 2017, by virtue of this disuse policy.

This policy applies to all end-user certificates issued by ANF AC, which are outlined per their certification policy. To see the updated list one can visit:

https://www.anf.es/en/show/section/cps_597

Unused hierarchy

Following the BaselineRequirements and the last agreements defined in this text, certificates have not been issued under the hierarchy **ANF Global Root CA with SHA1 signature algorithm**.

Thus, this hierarchy was created and is owned by ANF Certification Authority, but has never been used beyond to issue internal tests, because at the same time as its generation and exploit was planned, the agreements that prevented its use were published.

6.1.8 CA public key generation parameters

- Keys generated on HSM support: FIPS 140-2 Level 3 recommendations are followed. Key generation on HSM devices requires approval of at least two persons.

- Cryptographic keys generated in cryptographic device: FIPS 140-2 Level 2 or equivalent recommendations are followed.

6.1.9 Parameters quality checking

The specifications of section 6.1.7 certificate signature algorithms apply.

6.1.10 Key generation in computer applications or in capital goods

The keys are generated, as the case may be, as follows:

- CA: on the HSM device itself.
- End Entity: in the devices or systems that support them.

6.1.11 Key pair usage purposes

The authorized uses of the key, for each type of end entity certificate issued by ANF AC, are defined by the corresponding Certification Policy.

All certificates contain the "Key Usage" extension, which is considered critical, defined by the X.509 v3 standard. Additionally, additional limitations are set on the Extended Key Usage extension, which is also classified as critical. This classification allows limiting the use of the certificate to the purpose for which it was issued.

6.2 Private Key Protection

6.2.1 CA cryptographic module standards

ANF AC requires that the HSM tokens be qualified signature creation devices (QSCD or SSCD), officialy recognized by the regulatory body.

The cryptographic security module (HSM token) is a certified device that generates and protects cryptographic keys. ANF AC maintains protocols to verify that the HSM module has not been tampered with during transport and storage.

The European reference standard for subscriber devices used is Commission Implementing Decision (EU) 2016/650 of 25 April 2016.

ANF AC maintains control over the preparation, storage, and distribution of end-user devices, but the generation of keys is done by the user himself.

6.2.2 Multi-person control of the private key

The use of the CA's private keys requires the intervention of at least two of the authorized operators.

6.2.3 Private key storage

There is a document of Key Generation Ceremony of the Root CA and Intermediate CAs, which describes the processes of generation of the private key and the use of the cryptographic hardware.

ANF AC, for CA key generation, complies with ETSI recommendations EN 319 411-1, and CABForum Baseline Requirement Guidelines. On the other hand, ANF AC guarantees that the keys used to generate certificates, and/or to issue information on revocation states, will not be used for any other purpose, and once they reach the end of their life cycle, all private keys of signature of the CA shall be destroyed or rendered useless.

Furthermore, the use of the private key of the CA will be limited to that which is compatible with the hash algorithm, signature algorithm and signature key length used in the generation of certificates, in accordance with ETSI TS 102 176 " Technical Specification Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures ".

The private key of the root CA and intermediate CA are deposited in a hardware cryptographic device certified with FIPS 140-2 level 3 and/or CC EAL4 + (or superior), ensuring that the private key is never outside the cryptographic device.

The private keys of the root CA will be maintained and physically isolated used from normal operations in such a way that only designated trusted personnel have access to the keys for use in the subordinate CA certificate signing.

End-user devices are under their custody, and the latter will be responsible for keeping it under its sole control.

On the other hand, in the socpe of electronic certificates of centralized signature, ANF AC for the generation of the keys, their storage and later use in the scope of centralized signature, exclusively uses devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS Regulation, and therefore included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

Https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

In addition, ANF provides subscribers with secure communication channels and specific management and administrative security procedures.

6.2.4 Private key backup

There is a key recovery procedure for the CA (root or intermediate) cryptographic modules that can be applied in case of contingency, and that is applied during the CA Certificate Issuing Ceremony.

There is a key recovery procedure for the cryptographic modules of the subscribers who have contracted ANF AC custody of keys, which can be applied in case of contingency.

6.2.5 Entering the private key in the cryptographic module

Only in the case of contingency, the procedure indicated in section 6.2.4 is used to enter the private key in the cryptographic modules.

6.2.6 Method of activating the private key

In all cases, the use of signature activation data (PIN) is required to use the private keys of the cryptographic devices. It is delivered by a system that allows to maintain the necessary confidentiality.

CA Root and subordinate CA keys are triggered by a process that requires the simultaneous use of at least two HSM cryptographic devices (SmartCards).

Access to the subscriber's private key depends on the device on which it is generated. Each user receives a user manual.

6.2.7 Method of deactivating the private key

The removal of the cryptographic device from the issuer’s equipment implies the completion of any ongoing operation action.

The root CA, and the subordinate Cas key are disabled when the session is idle for a certain time.

In end user devices, it depends on the device in which it is generated, but as a rule it is the subscriber's responsibility to disable access to the private key.

6.2.8 Method of destroying the private key

There is a CA key destruction procedure. Cryptographic devices containing private keys created by subscribers incorporate a key destruction procedure.

In the case of private keys on end user devices, it is the responsibility of the end user to destroy the device containing them.

On the other hand, in the scope of electronic certificates of centralized signature, ANF AC has a procedure of destruction of the private key of the subscribers that so request it. The subscriber who requires the destruction of his private key must personally identify himself before ANF AC, or one of its Registration Authorities, notary public or make the petition through an electronically signed document.

6.3 Other aspects of key pair management

6.3.1 Public key file

The certificates generated by the CA are stored during the period of time required by current legislation, and in any case for a minimum period of 15 years.

6.3.2 Public and private key usage periods

It is the period of validity of each of the certificates, and is specified in each one of them.

6.4 Activation data

6.4.1 Activation data generation

The activation data for the root CA and the subordinate CAs keys are generated during the Root CA and subordinate CA Creation Ceremony.

The generation and installation of the activation data of the subscriber's private key depends on the device:

- **Identity certificates issued in a cryptographic device:**

  In all cases,

  - It is given to the authorized operator to use the cryptographic device, a system that allows to maintain the confidentiality and free choice of the signature activation data (PIN).

- The authorized operator of the cryptographic device generates the PIN, during the process of creating the keys.
- The cryptographic device employs a security logic that only allows the choice of activation data (PIN) that meets basic security requirements.
- The cryptographic device incorporates a function that allows the authorized operator to change the PIN.
- The PIN is never stored, nor is it noted in any form.

- **End-user technical certificates**
  Issued in software: the installation and start-up of the private key associated with the certificates, requires the use of security systems that the user has defined. ANF AC does not control and cannot define the private key access mode in these cases.

On the other hand, in the scope of electronic certificates of centralized signature, ANF AC may require users to have a double authentication control, based on sending a session password sent to one of their secure mailboxes (SMS or eMail), plus their signature activation PIN.

6.4.2 Activation data protection

The activation data of the root CA and intermediate CA keys are distributed over multiple physical cards, with at least two persons being required to perform any operation. The keys of the cards are guarded in the safe of ANF AC.

The TSA and VA keys are generated and managed on an HSM device and the same rules apply as in the case of Root CA and Intermediate CA.

End users are required to keep their activation data secret.

6.4.3 Other activation data aspects

The lifetime of the activation data is not stipulated.

See Specific Policy for each type of certificate.

6.4.4 Specific technical requirements for computer security

There are several controls in the location of the different elements of ANF AC's certification service provision system (CA, Databases, Telecommunication Services, CA Operation, and Network Management):

- There is a Business Continuity and Disaster Recovery Plan.
- Operational controls:

- All operating procedures are duly documented in the corresponding operating manuals.
- Virus and malicious code protection tools are implemented.
- Continued maintenance of the equipment is carried out to ensure its continued availability and integrity.
- There is a procedure for saving, erasing and safe disposal of information media, removable media, and obsolete equipment.

- Data exchanges. The following exchanges of data are encrypted to ensure proper confidentiality:
  - Transmission of data between ANF AC Trust Servers and the Recognized Registry Authorities (RRA).
  - Data transmission between ANF AC's Trust Servers and ANF AC's subscribers.

- The revocation publishing service has the necessary functionality to guarantee operations 24x7x365.

- Access control:
  - Identity certificates will be used, so that users are related to the actions they perform and can be held responsible for their actions.
  - The allocation of rights is carried out in accordance with the principle of minimum privilege.
  - Immediate elimination of the access rights of users who change their job or leave the organization.
  - Periodic review of the level of access assigned to users.
  - The assignment of special privileges is done "on a case-by-case basis" and is deleted once the cause that led to its assignment is terminated.
  - Guidelines exist to ensure quality in passwords.

  ANF AC has a Security Policy and specific procedures to ensure security at different levels.

On the other hand, in the scope of electronic certificates of centralized signature, the same procedure detailed in this section shall be followed.

6.4.5 Assessment of the computer security level

The products used for the issuance of certificates have at least FIPS 140-2 Level 3 or Common Criteria EAL 4+ compliance certification for the corresponding protection profile.

6.4.6 System development controls

ANF AC performs analysis of safety requirements during the design and specification phases of any component used in the applications of this PKI, to ensure that the systems are safe.

Modification control procedures are used for new releases, upgrades, and emergency patches for these components. It controls the implementation of software in production systems.

To avoid possible incidents in the systems, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) in production.
- Before the software is put into operation, it is installed in a test environment, where the relevant tests are carried out.
- A log file is kept of all the updates of the libraries.
- Previous versions of the software are maintained.
- In processes that affect the security of the certification systems, no software is installed without the Engineering Department having its source code, and has performed the corresponding security verification in the presence of the Technical Manager.

6.4.7 Life cycle security controls

ANF AC performs controls to provide security to the device that performs the generation of the keys. To avoid possible incidents in the systems, the following controls are established:

- Key generation software/hardware is tested prior to production.
- Key generation occurs within cryptographic modules that meet the requirements of technology and business.
- Procedures for secure storage of cryptographic hardware and activation materials occur after the key generation ceremony.

The products used for issuing certificates have the international "Common Criteria" or ISO / IEC 15408:1999 standard, or equivalent. These products will be replaced in case of loss of certification.

Certificates generated in development processes or tests, since they have not been placed into production, can be discarded without the need for revocation, notification to third parties or activation of the Business Continuity and Disaster Recovery Plan.

6.4.8 Test environment controls

ANF AC performs analysis of business requirements during the design and specification phases of any component used in the applications of this PKI, to ensure that the systems are safe.

Modification control procedures are used in the test environment, and a procedure strictly controlled by the system manager in the test environment is followed.

Each user is identified when accessing the environment in the same way as in the production environment. New versions, updates and emergency patches of these components are always previously run in the test environment and are reviewed under the modification control procedure.

To avoid possible incidents in the systems, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) on test.
- The test environment is a replica of the production environment, both in hardware and software.
- There are the same access controls to the environment that exist in the real environment.
- The data in the test environment is test data, generated by the engineering department.
- Prior to the implementation of the software, it is validated in the test environment, where the relevant tests are performed.
- A log file is kept of all the updates of the libraries.
- The previous versions of the software are maintained, in case there is a need for system recovery.
- In processes that affect the security of the certification systems, software is not installed of which the Engineering Department does not have the source code, and has performed the corresponding security verification in the presence of the Technical Manager.

6.4.9 Modifications control procedure

Procedures are used to control modifications in the development of access to libraries that maintain application software (through version control). Each employee is identified by a unique ID and any modification, reading, downloading, or uploading of code is recorded in the library.

This keeps a control over access to the source code of the program. Also, to avoid possible incidents, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) on test.

- Before the software is placed into operation, it is installed in a test environment, where the relevant tests are carried out.

- Modification to files or independent developments that do not follow the ANF AC's business policies are discarded.

- The purchase or modification of the software is controlled, its procedure is authenticated and is versioned in the version control application.

- A log file is kept of all the updates of the libraries.

- Previous versions of the software are maintained.

- In processes that affect the security of the certification systems, software is not installed of which the Engineering Department does not have the source code, and has performed the corresponding security verification in the presence of the Technical Manager.

6.4.10 Security management controls

ANF maintains an inventory of all information assets and classifies them per their protection needs and consistent with the risk analysis carried out.

Capacity needs are monitored and procedures are planned to ensure availability.

ANF AC continuously monitors computer systems and communications to ensure they operate in accordance with ANF AC's Security Policy. All processes are logged and audited in accordance with current legislation and regulations.

6.5 Network security controls

Access to the different networks of ANF AC is limited to duly authorized personnel:

- Controls are implemented to protect the internal network of external domains accessible by third parties. Firewalls are configured to prevent access and protocols that are not required for service operations.

- Sensitive data is encrypted when exchanged over non-secure networks (including subscriber registration data).

- Ensures that local network components are in secure environments, as well as periodically auditing their configurations.

- VPN communication channels are used, and confidential information transmitted over non-secure networks is encrypted using SSL/TLS protocols.

6.6 Secure source of time

ANF AC obtains the time of its systems from a connection to the Spanish Royal Observatory of the Navy following the protocol NTP. The description of the NTP v.3. protocol can be found in the IETF RFC 1305 standard. Based on this service, ANF AC offers an electronic time stamp (TSA) service that can be used to create time stamps on documents, per IETF RFC 3161 updated by IETF RFC 5816 and ETSI EN 319 421. More information in ANF AC's Time-Stamping Authority Policy and Practice Statement

7 Certificate profiles, CRL lists, and OCSP

7.1 Certificate Profile, OCSP and CRL lists

All certificates issued by ANF AC are in accordance the following technical standards:

- In general, on all certificates:
  - Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280 (updated by RFC 6818)) April 2002
  - Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 5280) December 2005
  - Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) August 2006
  - ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework

- All certificates issued with the consideration of qualified:
  - ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
  - RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificate Profile

7.1.1 Version number(s)

Electronic certificates issued under this Certification Practice Statement use the X.509 version 3 standard.

7.1.2 Certificate extensions

Used extensions are:

1. Authority key Identifier
2. subjectKeyIdentifier
3. basicConstraints
4. keyUsage
5. certificatePolicies
2. subjectAltName
3. issuerAltName
4. extKeyUsage
5. cRLDistributionPoints
6. Subject Directory Attributes

7. Authority Information Access

7.1.2.1 Generic certificate profile

The profiles are defined in their respective Certification Policies.

7.1.2.2 Algorithm object identifiers (OID)

The algorithm identifier (AlgorithmIdentifier) that employs ANF AC to sign the certificates is SHA-256/RSA.

- SHA256withRSAEncryption (1.2.840.113549.1.1.11)

Public Key Object Identifier (OID):

- RSAEncryption (1.2.840.113549.1.1.1)

7.1.2.3 Proprietary fields

Univocal ObjectId identifiers have been assigned internationally. Specifically:

- Fields referenced with object identifier (OID) 1.3.6.1.4.1.18332.x.x are proprietary extensions of ANF AC.

- Fields with ISO/IANA of MPR 2.16.724.1.3.5.xx * 1, are proprietary extensions required and identified in the Electronic Signature and Identification Scheme v.1.7.6 published by the Superior Council of Electronic Administration.

- The fields with OID 1.3.6.1.4.1.18838.1.1 are proprietary extensions of the Spanish State Tax Administration Agency (AEAT).

Regarding the proprietary fields of ANF AC, all of them are referenced in the section "Proprietary fields of ANF AC", in this CPS.

7.1.3 Name formats

As specified in the section “Names” of this document.

7.1.4 Name restrictions

No name restrictions are used.

7.1.5 Certification Policy object identifier (OID)

As specified in the section "Identification" of this document.

7.1.6 Usage of "Policy Constraints" extension

No policy restrictions are stipulated.

7.1.7 Syntax and semantics of policy qualifiers

The Certificate Policies extension contains the following "PolicyQualifier":

- Policy Identifier: Identifies the type of certificate profile within a certification policy to which it is associated.
- Policy Qualifier ID: Identifies the applicable Certification Policy.
- CPS Pointer: contains a pointer to the Certification Practices Statement and Policies published by ANF AC.
- User Notice: A statement made by the issuing CA is expressed, which refers to certain legal rules.

7.1.8 Semantic treatment for the critical "Certificate Policy" extension

The Certificate Policy extension allows one to identify the policy to which the certificate is submitted and where the Certification Policy can be found.

7.1.9 Guidelines for the completion of certificate fields

As recommended in RFC 5280 (updated by RFC 6818), the fields will be encoded in UTF8. Based on this, international character sets are encoded, including characters from the Latin alphabet with diacritical marks ("Ñ", "ñ", "Ç", "ç", "Ü", "ü", etc.), for example, the character eñe (ñ), which is represented in Unicode as 0x00F1.

Furthermore, and to establish a common framework in all certificates issued in the scope of ANF AC's PKI, the following recommendations will be followed when issuing certificates:

- All literals are entered in uppercase, except for the domain name/subdomain and email, which will be in lowercase.
- Names will be coded as they appear in the supporting documentation.
- In relation to the surnames of natural persons, the FIRST AND SECOND SURNAME must be included, separated only by a blank space, per what is indicated in the National/Foreign Citizens ID card. In case the second surname does not exist, it will be left blank (without any character).
- Include the National/Foreign Citizens ID card number, together with the control letter, in accordance with the National/Foreign Citizens ID card.
- The literal "ID" can be optionally included before the National/Foreign Citizens ID card number.
- It can be included a literal that identifies the type of the certificate, for example (AUTHENTICATION), (SIGNATURE) or (ENCRYPTION). This identifier will always be at the end of the CN and in parentheses.
- 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 allowed, provided they do not imply difficulty in the interpretation of the information.
- The "User Notice" field will not be longer than 200 characters.
- Each Certification Policy may define specific rules and limitations.

7.1.10 Proprietary fields of ANF AC

The following are the proprietary extensions that ANF AC can enter in the issued certificates. Together with the assigned OID, it specifies what value it contains.

OID	Value contained
1.3.6.1.4.1.18332.10.1	Name of legal representative (subscriber)
1.3.6.1.4.1.18332.10.2	First Surname of legal representative (subscriber)

1.3.6.1.4.1.18332.10.3	Second surname of legal representative (subscriber)
1.3.6.1.4.1.18332.10.4	Tax identification number of legal representative (subscriber)
1.3.6.1.4.1.18332.10.5	Document accrediting the legal representative (subscriber)
1.3.6.1.4.1.18332.10.6	Joint powers (only in case of existing)
1.3.6.1.4.1.18332.10.7	E-mail address of legal representative (subscriber)
1.3.6.1.4.1.18332.10.8	Identity card type submitted by the subscriber
1.3.6.1.4.1.18332.10.9	Nationality (subscriber)
1.3.6.1.4.1.18332.10.10	Hash of the mandate document or powers of attorney, digitized from the original.
1.3.6.1.4.1.18332.10.10.1	Link for the download of the mandate document or powers of attorney, digitized from the original.
1.3.6.1.4.1.18332.11	Full name of a natural or legal person, who grants a representation to the subscriber
1.3.6.1.4.1.18332.12	First name of the individual granting representation to the subscriber
1.3.6.1.4.1.18332.13	Surnames of the individual granting representation to the subscriber
1.3.6.1.4.1.18332.14	VAT number / National/Foreign Citizens ID Card of the natural or legal person granting representation to the subscriber
1.3.6.1.4.1.18332.19	Locator of the application (sequential of process - RA Operator or IRM identifier that processed it)
1.3.6.1.4.1.18332.19.1	Identifier of the RA Operator who processed the request. NOTE: In case of Operator RA, IRM or PKI Operator certificates, this OID corresponds to the operator identifier of the certificate, outlined in the first part of the code)
1.3.6.1.4.1.18332.20.1	Corporate name(subscriber)
1.3.6.1.4.1.18332.20.2	VAT number (subscriber)
1.3.6.1.4.1.18332.20.3	Name (subscriber)
1.3.6.1.4.1.18332.20.4	First surname (subscriber)

1.3.6.1.4.1.18332.20.5	Second surname (subscriber)
1.3.6.1.4.1.18332.20.6	Tax identification number (subscriber)
1.3.6.1.4.1.18332.20.7	Address (subscriber)
1.3.6.1.4.1.18332.20.8	Identity card type submitted by the subscriber
1.3.6.1.4.1.18332.20.10	Numeric code that defines the treatment to be addressed to the subscriber
1.3.6.1.4.1.18332.20.11	Test certificate identifier, with three possible status values ("active", "revoked" or "expired")
1.3.6.1.4.1.18332.20.13	Nationality (subscriber)
1.3.6.1.4.1.18332.29.1	Name of certificate responsible
1.3.6.1.4.1.18332.29.2	First surname of certificate responsible
1.3.6.1.4.1.18332.29.3	Second surname of certificate responsible
1.3.6.1.4.1.18332.29.4	Tax identification number of certificate responsible
1.3.6.1.4.1.18332.29.5	E-mail of certificate responsible
1.3.6.1.4.1.18332.29.6	Position, title, role of certificate responsible
1.3.6.1.4.1.18332.29.7	Department to which the certificate responsible belongs to
1.3.6.1.4.1.18332.29.8	Identity card type submitted by certificate responsible
1.3.6.1.4.1.18332.29.9	Nationality of the certificate responsible
1.3.6.1.4.1.18332.29.10	Address where the certificate responsible resides
1.3.6.1.4.1.18332.29.11	Locality where the certificate responsible resides
1.3.6.1.4.1.18332.29.12	Province/state/area where the certificate responsible resides
1.3.6.1.4.1.18332.29.13	Postal Code where the certificate responsible resides
1.3.6.1.4.1.18332.29.14	Country where the certificate responsible resides
1.3.6.1.4.1.18332.29.15	Phone number of certificate responsible
1.3.6.1.4.1.18332.29.16	Mobile phone number of certificate responsible
1.3.6.1.4.1.18332.29.17	E-mail address of certificate responsible
1.3.6.1.4.1.18332.29.18	Mail of the certificate responsible

1.3.6.1.4.1.18332.30.1	Country to which the certificate issuance corresponds to
1.3.6.1.4.1.18332.40.1	Qualification with which the certificate was issued
1.3.6.1.4.1.18332.41.1	Limit of liability assumed by the CA
1.3.6.1.4.1.18332.41.2	Limitation of use of the certificate by concept
1.3.6.1.4.1.18332.41.3	Limitation of use of the certificate by amount
1.3.6.1.4.1.18332.41.4	Limitation of use of the certificate by currency type
1.3.6.1.4.1.18332.42.1	Identifier of the Recognized Registration Authority to which the operator belongs.
1.3.6.1.4.1.18332.42.2	Determines that it is a RA Operator Level 1 "Recognized Registration Authority Level 1"
1.3.6.1.4.1.18332.42.3	Determines that it is an Issuance Reports Manager "Issuance Reports Manager "
1.3.6.1.4.1.18332.42.4	Determines that it is a RA Operator Level 2 "Recognized Registration Authority Level 2"
1.3.6.1.4.1.18332.42.4.1	Determines if it is a RRA with the capacity to process short term certificates of validity "RA authorized to issue short term validity"
1.3.6.1.4.1.18332.42.8	PKI Operator security level
1.3.6.1.4.1.18332.42.9	Determines that it is a PKI Operator "PKI Authorized Operator"
1.3.6.1.4.1.18332.42.11	Name of the Holder of the RA Office to which the RA Operator is assigned
1.3.6.1.4.1.18332.42.13	Department in which the RA Operator works in the RA Office.
1.3.6.1.4.1.18332.43	Automation of limitations for automatic processes
1.3.6.1.4.1.18332.45.1	Tax identification of second representative (joint powers)
1.3.6.1.4.1.18332.45.2	Name of second representative (joint powers)
1.3.6.1.4.1.18332.45.3	First surname of second representative (joint powers)
1.3.6.1.4.1.18332.45.4	Second surname of second representative (joint powers)
1.3.6.1.4.1.18832.45.5	Accreditation document of the legal representation

1.3.6.1.4.1.18332.46	It determines that it is a certificate of short duration. Reference value 1.
1.3.6.1.4.1.18332.47	Determines the valid days of electronic certificates to personalize issuance
1.3.6.1.4.1.18332.47.1	UUID of the Electronic Signature Device that stores the certificate
1.3.6.1.4.1.18332.47.3	If active indicates that the signature generation data is contained in a cryptographic device
1.3.6.1.4.1.18332.56.2.1	Black list of persons and entities
1.3.6.1.4.1.18332.60.1	Micropayment system activated
1.3.6.1.4.1.18332.60.4	Electronic Payment System activated
1.3.6.1.4.1.18332.85.1	Incoming Hash of the chaining of a Digital Time Stamp
1.3.6.1.4.1.18332.85.2	Outgoing Hash of the chaining of a Digital Time Stamp
1.3.6.1.4.1.18332.90	Business descriptive aspects of the activity
1.3.6.1.4.1.18332.90.1	Other aspects related to the quality of service
1.3.6.1.4.1.18332.90.2	Other aspects related to the quality of service
1.3.6.1.4.1.18332.90.3	Other aspects related to the quality of service
1.3.6.1.4.1.18332.91	Company creation date
1.3.6.1.4.1.18332.91.1	Legal form of subscriber
1.3.6.1.4.1.18332.91.2	Year of origin of the activity
1.3.6.1.4.1.18332.92	Own trademarks
1.3.6.1.4.1.18332.92.1	Trademarks that distribute suffix 1
1.3.6.1.4.1.18332.92.2	Trademarks that distribute suffix 2
1.3.6.1.4.1.18332.92.3	Trademarks that distribute suffix 3
1.3.6.1.4.1.18332.93	Geographical area in which it operates
1.3.6.1.4.1.18332.94	Headquarters address, phone, fax, website location
1.3.6.1.4.1.18332.94.1	Delegations suffix 1
1.3.6.1.4.1.18332.94.2	Delegations suffix 2
1.3.6.1.4.1.18332.94.3	Delegations suffix 3

1.3.6.1.4.1.18332.95	Companies with which it maintains relations
1.3.6.1.4.1.18332.95.1	Companies with which it is related suffix 1
1.3.6.1.4.1.18332.95.2	Companies with which it is related suffix 2
1.3.6.1.4.1.18332.95.3	Companies with which it is related suffix 3
1.3.6.1.4.1.18332.96	Bank entities with which it maintains relations
1.3.6.1.4.1.18332.96.1	Bank accounts, SWIFT codes
1.3.6.1.4.1.18332.97	Financial information relating to its activity
1.3.6.1.4.1.18332.97.1	Financial information relating to its activity suffix 1
1.3.6.1.4.1.18332.97.2	Financial information relating to its activity suffix 2
1.3.6.1.4.1.18332.97.3	Financial information relating to its activity suffix 3
1.3.6.1.4.1.18332.98	Number of employees
1.3.6.1.4.1.18332.99	Number of distributors
1.3.6.1.4.1.18332.600	Contains the version of the AR Manager application used to process the certificate request.

I. Qualified certificates

The certificates issued with the consideration of qualified, additionally incorporate the object identifier (OID) defined by ETSI EN 319 412-5, of the European Telecommunications Standards Institute, on profiles of qualified certificates qcStatement – QcCompliance. Furthermore, the value "Qualified Certificate" is included in the proprietary extension of OID 1.3.6.1.4.1.18332.40.1.

Certificates that are issued with the consideration of qualified are identified in the extension OID 1.3.6.1.5.5.7.1.3, which indicates the existence of a list of "QCStatements", per the ETSI EN 319 412-5. Concretely:

- QcCompliance (OID 0.4.0.1862.1.1) establishes the consideration with which the "Qualified Certificate" issuance has been made.

- QcLimitValue (OID 0.4.0.1862.1.2) informs of the monetary limit assumed by the CA as a liability in the loss of imputable transactions. This OID contains the sequence of values: currency (coded per ISO 4217), quantity and exponent. E.g. EUROS 100x10 raised to 1, which presupposes monetary limit of 1000 EUROS.

  In addition, to facilitate the consultation of this information, the limit of liability is included in the proprietary extension of OID 1.3.6.1.4.1.18332.41.1, which summarizes in an absolute manner

directly. E.g. 1000 euros. In the event of doubt or discrepancy, preference should always be given to the reading value outlined in OID 1.3.6.1.4.1.18332.41.1

- QcEuRetentionPeriod (OID 0.4.0.1862.1.3) determines the period of conservation of all information relevant to the use of a certificate, after its expiration. In case of ANF AC, it is 15 years.

- QcSSCD (OID 0.4.0.1862.1.4) informs whether the certificate and the keys are contained in a cryptographic token device (in accordance with the description made in ANF AC CPS).

II. Subject Alternative Name

The IETF RFC 5280 specification (updated by RFC 6818) provides for use the following data types:

- Identity based on email.

- Identity based on distinguished name (DN), which is usually used to construct an alternative name based on proprietary attributes, which are not ambiguous in any case.

- Identity based on Internet domain name (DNS).

- Identity based on IP address.

- Identity based on Universal Resource Identifier (URI).

They can contain more than one instance (for example, various e-mail addresses).

The issuing authority verifies all names when they are included in the certificate.

The composition of the CN (Common Name) field for a Class 2 Legal Person certificate shall include:

- The corporate name of the subject and the acronym of the legal form of the subject, separated only by a space and in capital letters.
- The subject's VAT number (identifier), in uppercase and without separation.
- A "-" dash that separates the subject's name from the VAT number.

7.2 Certificate Revocation List (CRL) Profile

The CRLs issued by ANF AC are in conformity with the following standards:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) April 2002

- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006.

7.2.1 CRL version number

Version 2.

7.2.2 CRL and CRL elements extensions

The fields and extensions used are as follows:

Field	Values	Mandatory	Critical
Version	V2 (version of X.509 standard)	YES	NO
Authority key Identifier	Identifier of the issuer's key	YES	NO
CRL serial number	Unique code with respect to that particular hierarchy of the issuer	YES	NO
Signature algorithm	Sha1WithRSAEncryption	YES	NO
Hash algorithm	Sha1	YES	NO
Issuer	CN= of the issuing CA SERIALNUMBER = issuing CA's VAT number OU = Issuing CA organizational unit O= Issuing CA name C= Issuing CA country	YES	NO
Effective issuance date	CRL issuance date	YES	NO
Date of next update	Next CRL issuance date	YES	NO
Distribution point	URL Distribution point and type of certificates it contains	YES	NO
CRL entries	Certificate serial number	YES	NO

	Date of revocation	YES	NO
	Reason code	NO	NO

7.3 OCSP profile

Certificates issued by ANF AC for OCSP Responder are compliant with RFC 6960 "*Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP*".

7.3.1 Version number

Version 3.

7.3.2 OCSP extensions

Field	Mandatory	Critic
Version	YES	NO
Issuer Alternative Name	NO	NO
Authority / Subject key Identifier	NO	NO
CRL Distribution Point	NO	NO
Key usage	YES	YES
Enhanced Key usage	YES	YES

7.3.2.1. Certification Path Validation

The OCSP query verifies the entire Certification Path and determines the validity of each certificate in the chain, until it reaches the highest level of the Root Certificate.

The sequence of elements verified in the construction of the Certification Route contemplates as a minimum:

1. Name of the issuer of the verified certificate. It must be equal to the name of the Subject in the certificate of the issuer.
2. The Certificate format must be X.509v3 in the DER encoding.
3. The signature of the certificate must be verified with the public key of the certificate of the issuer.

4. The "AuthorityKeyIdentifier" field of the verified Key Identifier certificate must be the same as the "SubjectKeyIdentifier" in the certificate of the issuer. Each certificate must contain the "SubjectKeyIdentifier" field.

5. If the certificate contains "authorityCertIssuer" verified in "AuthorityKeyIdentifier", then the name must be equal to the name of the issuer in the certificate of the issuer.

6. If the certificate contains "authorityCertSerialNumber" verified in "AuthorityKeyIdentifier", "authorityCertSerialNumber" then it must be equal to "serialNumber" in the certificate of the issuer.

7. Determines whether the CA certificates "issuing entity" of the certification path, incorporate the field "basicConstraints", with value TRUE.

8. If "basicConstraints" is TRUE, the certificate can contain the "pathLengthConstraint" field that determines the maximum number of CA certificates that can be chained after the verified certificate. If the value is 0, it indicates that the CA can only issue end entity certificates.

   If the CA certificate does not contain the "pathLengthConstraint" field, it means that there is no restriction on the Certification Path unless it is restricted by the value reported in a top-level certificate. The parameter in an intermediate CA must be lower than that in a higher-level CA.

   Thus, the length of the Certification Path affects the number of CA certificates that will be used during certificate validation. The string begins with the end entity certificate that is validated and moves up.

9. The control time must be in the "notBefore, notAfter" interval. The certificate must not have expired at the control time.

10. The control time must be in the interval (not before, not after) (notBefore, notAfter) -None of the lower level certificates must have been issued at a time prior to the time of issue of the higher-level certificate.

11. It will be verified that the use of the "keyUsage" key is consistent with the type of certificate verified.

12. If the certificate has been issued with the consideration of qualified, it will be verified if the extension "QcStatements" is in conformity with the profile defined in its corresponding policy, which is identified by the OID included in the extension "PolicyIdentifier".

*[1] The signature of the petition is optional and depends on what the OCSP Validation Authority decides. ANF AC, in OCSP queries about WEB service, does not require signed requests, but it may, per the OCSP, respond consulted, require the subscriber to be an authorized user and be subscribed to the service. ANF

AC signs OCSP responses with an OCSP certificate issued by the same organization issuing the certificates of end entity.

*[2] In accordance with RFC 6960, NONCE cryptographically links a request and a response to prevent repetitive attacks. The nonce is included as one of the requestExtensions in the requests, whereas in the responses it would be included as one of the responseExtensions. In both the request and the response, the nonce will be identified by the id-pkix-ocsp-nonce object identifier, while the extnValue is the value of the nonce.

8 Compliance audit

Verification of compliance with safety requirements is defined in the document published by ANF AC "Standards and Audit Criteria for Certification Services" (OID 1.3.6.1.4.1.18332.11.1.1)

On-site verifications are carried out to determine whether operating personnel follow established procedures.

ANF AC performs a correct security management through the implementation of an Information Security Management System in accordance with the principles established by ISO / IEC 27001 which includes, among others, the following measures:

1. Regularly carry out security verifications, to check compliance with established standards.

2. Carry out a complete management of the security events, to guarantee their detection, resolution, and optimization.

3. Maintain appropriate contacts and relationships with groups of special interest in security matters, such as specialists, security forums and professional associations related to information security.

4. To adequately plan the maintenance and evolution of the systems, to guarantee at all times an adequate performance and a service that meets with all the guarantees the expectations of the users and clients.

8.1 Frequency of conformity controls for each entity

ANF AC submits its PKI annually to an audit process, in addition to the on-demand audits it may carry out in its sole discretion, because of a suspected breach of a security measure or a compromise of keys.

8.2 Identification of the personnel in charge of the audit

The PKI Governing Board determines for each control, and per the area under review, the personnel in charge of carrying out this operation, making sure that it has the necessary experience and that it is an expert in digital certification systems.

Audits based on ISO norms and standards, such as WebTrust, WebTrust EV and WebTrust BR, must be performed by auditors who have the necessary accreditation.

Conformity assessments: EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421. The auditor must be accredited in accordance with EN 319 403.

8.3 Relationship between the auditor and the audited entity

The Governing Board of the PKI may entrust control to internal or external auditors, but, in any case, functionally independent to the area under audit.

8.4 Topics covered by the audit

The elements to be audited are as follows:

- Public key certification processes.
- Information systems.
- Process center protection.
- Service documentation.
- Conformity of the CPS with published Policies.

8.5 Actions to be undertaken as a result of a lack of conformity

After receiving the report of the compliance audit carried out, ANF AC analyzes, together with the entity that carried out the audit, any deficiencies found, designing a corrective plan that solves these deficiencies and establishing their execution.

Once the deficiencies are corrected, a new audit is carried out to confirm their implementation and the effectiveness of the solutions taken.

8.6 Treatment of audit reports

The audit reports will be submitted to the PKI's Governing Board for analysis. The Board will adopt the appropriate measures per to the type of incidence detected.

9 General Provisions

9.1 Fees

ANF AC charges the subscribers of the certificates, and the persons or entities that contract its certification services regulated in this CPS, the fees that at any moment are valid.

9.1.1 Certificate issuance or renewal fees

Issuing and renewal fees for each certificate are published on the website

https://www.anf.es/en/show/section/official_fees_ce.

9.1.2 Certificate access fees

Free service.

9.1.3 Status information access fees

- Free of charge:

  Access to the information on the status of certificates (OCSP, revoked certificate publication service from a date and time) when they do not exceed 50 queries per day.

- Applicable rate:

  When a volume of more than 50 queries per day is expected, an agreement should be established specifying the estimated volume of queries, the resources that ANF AC will allocate to adequately address such workload, and the price applicable to the service.

9.1.4 Timestamp request fees

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.1.5 Re-issuing request fees

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.1.6 Signature verification certificate request fees

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.1.7 Signature device fees

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.1.8 Fees for other services and solutions of ANF AC

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.1.9 Refund policy

Fees found in the website https://www.anf.es/en/show/section/official_fees_ce.

9.2 Information confidentiality

ANF AC has a Privacy Policy. In general, it covers the following issues:

9.2.1 Types of confidential information

It is expressly declared as confidential information and may not be disclosed to third parties, except in cases where the law requires otherwise:

- The identity of the holders of certificates that have been issued under a pseudonym.
- Any information or data, which, having been submitted by the subscriber to the Certification Authority or the Registration Authority, does not appear on the electronic certificate.
- All information related to safety parameters.
- Information or documents that ANF AC has classified as confidential.
- Transaction records, including complete records and audit records of transactions.
- Internal and external audit records, created and/or maintained by ANF AC or the Registration Authorities and their auditors.

9.2.2 Non-confidential information

The following information is considered non-confidential and in this form, it is recognized by those affected in the binding agreements with ANF AC:

- Certificates issued or in the process of being issued.
- The linking of a subscriber to a certificate issued by ANF AC.
- The identity of the subscriber of the certificate, or of the subject, as well as any other circumstance or personal data of the same, if it is significant in function of the purpose of the certificate, and that it is recorded in the same.
- The uses and economic limits outlined in the certificate, as well as any other information contained therein.
- The different status or situations of the certificate and the starting date of each of them, namely: pending generation and/or delivery, valid, revoked, suspended, or expired and the reason that caused the change of status.
- Certificate Revocation Lists (CRLs), as well as any revocation status information.
- The information contained in the Publication Service of ANF AC classified as Public.

9.2.3 Disclosure of suspension and revocation information

ANF AC issues Certificate Revocation Lists (CRLs) that are publicly accessible and free.

ANF AC has other means of consultation of status, as outlined in section 2.5 "Publication of status of issued certificates"

9.2.4 Legal disclosure of information

As a rule, no document or registration belonging to ANF AC is sent to judicial or police authorities, except when:

- The agent of the law is properly identified.
- Provide a properly drafted court order.
- The Certification or Registration Authority is aware that the certificates issued, or any of the instruments belonging to this PKI, are being used for the commission of a crime.

ANF AC shall disclose the confidential information only in the cases legally provided for it.

Specifically, records that guarantee the reliability of the data contained in the certificate shall be disclosed should it be required to provide evidence of certification in the event of legal proceedings, even without the consent of the certificate subscriber.

9.2.5 Disclosure on request of the owner

The certificates will be published in accordance with what is established in article 18.c) of the Spanish Law 59/2003, of December 19, of electronic signature.

In addition, the owner of the information may require ANF AC to issue a report of the information of his property, which is stored or deposited with the Certification Authority or the Recognized Registry Authority. ANF AC will provide the budget for the fee for such service, and upon acceptance, will issue the aforementioned report.

On the exchange of registration data with the subscriber or subject or other parties involved in the PKI, security measures are taken to ensure the confidentiality and integrity of the information.

9.2.6 Other circumstances of information disclosure

Not applicable.

9.3 Intellectual property rights

Under the terms established in the Spanish Royal Decree-Legislative 1/1996, of April 12, approving the Revised Text of the Intellectual Property Law, ANF AC holds exclusive rights of all electronic certificates issued in the scope of its PKI in any of the types or modalities of certificates, including the CRL and ARL certificate revocation lists.

The object identifiers (OIDs) used are owned by ANF AC or its affiliates and have been registered on the Internet Assigned Number Authority (IANA) under the branch iso.org.dod.internet.private.enterprise 1.3.6.1.4.1-IANA -Registered Private Enterprises, having been assigned the following numbers:

- 1.3.6.1.4.1.18332
- 1.3.6.1.4.1.18333
- 1.3.6.1.4.1.18339
- 1.3.6.1.4.1.37442

Http://www.iana.org/assignments/enterprise-numbers

It is prohibited, outside the scope of the ANF AC PKI, the total or partial use of any of the OID assigned to ANF AC or its subsidiaries.

9.3.1 Property of certificates and information revocation

The issuance and delivery of the certificates issued by ANF AC does not presuppose any waiver of the intellectual property rights that they hold over them.

ANF AC, unless expressly authorized, prohibits the storage of the data of its certificates in repositories outside the PKI of ANF, and especially when it has as purpose the provision of information services on the validity or revocation.

Certificates and status information can only be used for the purposes of use specified in this document.

9.3.2 Property of PKI related documents

ANF AC owns all the documents that it publishes in the scope of its PKI.

9.3.3 Property of information relating to names

The subscriber retains any right, if any, relating to the trademark, product or trade name contained in the certificate.

The subscriber is the owner of the Distinguished Name of the certificate.

9.3.4 Property of keys

The certificate subscribers own key pairs. When a key is fractioned into parts, the subscriber owns all parts of the key.

9.4 Classification of documents drafted by ANF AC

The list of documents used by ANF AC is available at the following web address:

https://www.anf.es/en/show/section/documentary_structure

9.5 Obligations

9.5.1 Of the Trust Services Provider

ANF Certification Authority, as a Trusted Service Provider that issues certificates in accordance with this CPS, assumes the following obligations:

9.5.1.1 In the provision of the service

ANF AC provides its certification services in accordance with this CPS, being responsible for the fulfillment of all its obligations as Trust Service Provider. These obligations of the Certification Entity are as follows:

- Not storing or copying the signature creation data of the person to whom services have been rendered.

- Maintaining a system in which the issued certificates are indicated and if they are valid or if their validity has been suspended or extinguished.

- Keeping, for at least 15 years from the date of issuance of the certificate, all information and documentation related to the qualified certificates and valid CPS in every moment, and of the rest of the certificates for 5 years.

- Verify that the signer is in possession of the signature creation data corresponding to the verification data contained in the certificate.

9.5.1.2 Reliable operation

ANF AC guarantees:

- That the identity contained in the certificate corresponds uniquely to the public key contained in the certificate.

- The use of a fast and secure service to verify the validity of the certificates in accordance with the provisions of this CPS is permitted. This service is permanently available 24x7x365.

- Compliance with the technical and personnel requirements required by current legislation on electronic signature:

    1. Demonstrate the reliability necessary to provide certification services.

2. Ensure that the date and time of issuance of a certificate can be accurately determined, or when it was terminated or suspended.

3. To employ the personnel with the necessary qualifications, knowledge, and experience to provide the certification services offered and the appropriate security and management procedures in the electronic signature scope.

4. Use reliable systems and products that are protected against any alteration and that guarantee the technical and, as the case may be, cryptographic security of the certification processes they serve as support, in accordance with the Security Policy.

5. To take measures against the falsification of certificates, to guarantee the confidentiality in the process of generation according what is stated in section 6 and to provide it through a safe procedure to the signer.

6. Use reliable systems to store qualified certificates, that allow to verify their authentication and prevent unauthorized persons from altering the data, restricting their accessibility in the cases or persons that the signatory has indicated and that allow to detect any changes that affect these conditions of security.

- The correct management of its security, thanks to the implementation of an Information Security Management System in accordance with the principles established in ISO/IEC 27001 and which includes, among others, the following measures:

    1. Regularly carry out security verifications, to verify compliance with established standards.

    2. Carry out a complete management of the security events, to guarantee their detection, resolution, and optimization.

    3. Maintain appropriate contacts and relationships with groups of special interest in security matters, such as specialists, security forums and professional associations related to information security.

    4. To adequately plan the maintenance and evolution of the systems, to guarantee at all times an adequate performance and a service that meets with all the guarantees the expectations of the users and clients.

9.5.1.3 Of identification

ANF AC identifies the subscriber of the certificate, in accordance with articles 12 and 13 of the Spanish Law 59/2003 of December 19, electronic signature, and this CPS.

9.5.1.4 Of information to users

Prior to the issuance and delivery of the certificate to the subscriber, ANF AC or the Registration Authority on behalf of ANF AC, informs the users of the terms and conditions regarding the use of the certificate, its price, its limitations of use and provides them with documentation regarding the rights and obligations inherent in the use of ANF AC's certification services, in particular, the custody and privacy of electronic instruments and signature activation data. The terms and conditions can be downloaded by third parties by accessing ANF AC's website.

This requirement is fulfilled through the formalization of the corresponding subscription agreement.

ANF AC undertakes to notify the signatories of the termination of its activities of providing certification services two months in advance and inform, where appropriate, the characteristics of the provider to whom the transfer of the management of the certificates is proposed. Communications to the signatories are carried out in accordance with the provisions of this document.

ANF AC has a termination plan of its activity, which specifies the conditions under which it would be carried out.

All this public information regarding the certificates is available to the public in ANF AC's repositories indicated in this CPS.

9.5.1.5 Concerning verification programs

ANF AC offers mechanisms to verify the validity of electronic certificates and signatures, through the systems described in this document.

9.5.1.6 Concerning the legal regulation of the certification service

ANF AC assumes all obligations incorporated directly in the certificate or incorporated by reference. Incorporation by reference is achieved by including in the certificate an object identifier or another form of link to a document.

The legal instrument that links ANF AC and the subscriber or subject and relying party is in writing and understandable language, having the following minimum contents:

- Indication that enables the subscriber to know and enable the fulfillment of their obligations and rights.

- Indication of the applicable Certification Practice Statement, specifying, where appropriate, that the certificates are issued with the need to use a secure signature creation or decryption device approved by ANF AC.

- Clauses relating to the issue, revocation, and renewal of certificates.

- Manifestation that the information contained in the certificate is correct, except notification by the subscriber.

- Consent for the storage of the information used for the registration of the subscriber, for the provision of a cryptographic device and for the transfer of such information to third parties, in case of termination of ANF AC operations without revocation of current certificates.

- Limits of use of the certificate.

- Information on how to validate a certificate, including the requirement to verify the status of the certificate, and the conditions under which the certificate can reasonably be relied upon.

- Applicable liability limitations, including the uses for which ANF AC accepts or excludes its liability.

- Period of storage of certificate request information.

- Applicable dispute resolution procedures.

- Applicable law and jurisdiction.

- The manner in which the liability of ANF AC is guaranteed.

9.5.2 Responsibility of the Recognized Registration Authority

The Spanish Electronic Signature Law recognizes the possibility that the issuing entities may collaborate with third parties in the provision of their services, but nevertheless establishes that the sole responsibility of the certification services lies entirely with the Certification Services Provider. The Recognized Registry Authorities are responsible to ANF AC for damages caused in the exercise of their functions, in accordance with the obligations established in the corresponding agreement, and with the following:

- Transcribe accurately, in the request forms of the AR Manager device, the information collected from the original documents provided by the subscribers.

- Admit only original documentation in the identification process, obtaining a copy of the documentation provided by the subscribers. This documentation will be sent to the certification authority for custody.

- Not providing third parties with a copy of the documentation obtained from the subscribers, nor any information of the same or the subjects.

- Safeguarding the AR Manager device, not allowing its use or the revision of it by unauthorized third parties and, in case of loss, immediately inform ANF AC.

- Transmit to the Spanish Data Protection Agency the existence and activation of the AR Manager device, which contains personal data. It will use the form that automatically generates the system.

- Apply the official rates without increasing or applying any charges for any other concept than those stipulated by ANF AC.

- In the event of terminating its activity as a RRA, proceed in returning the AR Manager device, as well as any documentation or material in its possession derived from the activity performed as a Recognized Registry Authority.

- Report any judicial or extrajudicial claim that occurs in the scope of its activity as ARR.

- In relation to the information contained in the certificate or personal characteristics that qualified them at the time to obtain accreditation as a Recognized Registry Authority, they must report any changes that occur in their personal circumstances.

- Protect and personally guard the Private Keys of the RRA and the password of activation against the danger of usurpation or misuse. In the event of any suspicion of a breach of security, they must immediately notify it and proceed with its revocation.

- Be diligent in the attention of the subscribers, facilitating, if possible, information of the original documents that will be required and avoiding unnecessary waits.

- Not using copies that the subscriber accompanies with the original documentation. The Registration Authority shall directly obtain any hard or digitized copy.

- Communicate diligently to ANF AC the existence of requests for the issuance of Certificates, especially those that it has rejected.

- Not mediating in the generation of the signature creation data of the users, nor allowing to be informed of the activation PIN chosen by the subscriber.

- Storing, in a secure and permanent manner, a copy of the documentation provided by the user to make their request, as well as the documentation generated by the AR Manager, during the process of request, registration, or revocation.

- Collaborate with the audits directed by ANF AC to validate the renewal of their own keys.

- Respect the privacy of subscribers and certificate holders in accordance with the Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data and other applicable regulations.

9.5.3 Responsibility of subscribers and certificate responsible

The responsibilities of the holders of the certificates are established in the corresponding Certification Policies. In addition, in a general and complementary way it is established that:

- ANF AC certificate subscribers are responsible for complying with all obligations derived from this document, the Electronic Signature Policy, Certification Policies, Subscription Agreement and Terms and Conditions, limiting and adapting the use of the certificate and electronic signature systems contemplated in the scope of this PKI for licit purposes and in accordance with an honest and loyal action with the whole community: ANF AC, Recognized Registry Authorities, users and relying parties. The following list is merely illustrative and not limiting.

The subscriber agrees to:

- Ensure that all information contained in the Certificate is true.

- Ensure that the documentation provided in the processing of the certificate application is truthful and authentic.

- At the time of receiving their electronic certificate, urgently verify the correspondence of the same with the request made. To do this, they will use the certificate verification option that is included in the signature creation data generation device. In case the verification proves negative, it shall immediately be informed to ANF AC.

- Use the certificate respecting the restrictions that are imposed per its Certification Policy and the Electronic Signature Policy.

- If the certificate states "Declaration of the Issuer, Attributes, and Limitations of use", it must comply with what is stated therein.

- Carefully custody the container of the signature creation data and the activation secret key, as well as the user name and secret password for accessing the General Registry.

- Use only ANF AC devices, both for the storage of signature generation data and for the creation of electronic signatures, as well as their subsequent verification.

- Keep ANF AC cryptographic devices up to date, following ANF AC's instructions for their installation and maintenance, and ensure that the devices have not been omitted by the protection provided by ANF AC.

- Before creating an electronic signature using an ANF AC's Cryptographic device, verify the signature attributes that will be included in the electronic signature, and only activate the signature process if they are satisfied with all of them.

- Accept all electronic signatures linked to the certificate holder, provided they have been created using a valid certificate.

The essential activation of signature creation data, by the signatory through the use of his secret code, presupposes:

- Full consent to the creation of the electronic signature, and acceptance of the Electronic Signature Policy associated with that signature.

- The request for revocation of the Certificate when the security of the signature creation data or the activation secret key is compromised or when their personal data have undergone any modification.

- In case of revocation of the Certificate, the subscriber's obligation to cease its use.

Users guarantee that the nominations, corporate names, or domains described in the certificate application form and in the subscription agreement do not infringe the rights of third parties in any jurisdiction in relation to intellectual property rights and trademarks, that they will not use the domain and Distinguished Name for illicit purposes; among them, unfair competition, impersonation, usurpation and acts of confusion in general.

The subscribers and, in general, the users of certificates, shall indemnify ANF AC for the damages that it can cause in the execution of this activities. They also undertake to:

- Provide RRAs with original documentation and information they deem accurate and complete. As well as to notify any modification that it occurs.

- To pay the fees of the services rendered to them by the CA, or by the RRA.

- Not processing a certificate request in case of any conflict of interest with ANF AC or members of the Governing Board.

- Making the certificate request under the principle of good faith, and with the sole interest of making use of it for the purposes that are commonly accepted.

- In general, all those derived from the Spanish Law 59/2003, of Electronic Signature, especially those outlined in article 23 section 1.

9.5.4 Responsibility of relying parties

It has the consideration of a good faith relying party the receiver of an electronic file which has been electronically signed by a user of ANF AC's trust services, and that has deposit its trust in that electronic signature. This relying party has the following obligations:

- Verifying the signature using an ANF AC's electronic signature verification device.

- Verify the validity of the certificate using one of the means authorized by this CPS.

- Act diligently. It will be considered that the action has been negligent if it incurs in any of the cases contemplated in article 23 section 4 a) and b) of the Spanish Law 59/2003, of Electronic Signature.

- Evaluate the adequacy of the certificate associated to the electronic signature, according to: the type of certificate, the issuer's declaration, the limitations of use that are stated in it, and those declared in this CPS and the corresponding Certification Policy.

- Request advice from ANF AC's "Customer Service Office" in case of doubt.

The Spanish State Tax Administration Agency will manage the verification of the status of the certificates of the users of this Certification Authority, through the use of the corresponding web service that ANF AC has implemented for this purpose. This service uses the SOAP protocol per the technical specifications related to the O.M. HAC/1181/2003.

ANF AC puts at the disposal of relying parties the certificate revocation lists. Third parties may access this information with the sole use and personal purpose of verifying the validity of a certificate of their interest, and in no case, shall it be used for the provision of services to other third parties.

Recipients who do not meet the above requirements shall not be considered good faith parties.

9.5.5 Of the publication service

Not applicable because the Publishing Service is not an independent entity.

9.6 Civil Liability

9.6.1 Of the Trust Service Provider

ANF AC will respond of those damages that are derived, in general from:

- Failure to comply with the obligations contained in the Spanish Law 59/2003, of December 19, of Electronic Signature and development regulations, in this CPS and in the corresponding Certification Policies.

And specifically:

- As provided in article 22 of the Spanish Law 59/2003, of December 19, of Electronic Signature, ANF AC will respond for damages caused to any person by the lack or delay of the inclusion, in the consultation service, of the validity of the certificates or of the extinction or suspension of the validity of the certificates.

- ANF AC assumes all responsibility towards third parties for the actions of the persons in which it delegates the necessary functions for providing certification services.

In any case, the following situations are excluded, in general:

- ANF AC shall not be liable for any direct, indirect, special, incidental, consequential damages of any loss of profit, loss of data, punitive damages, whether or not foreseeable, arising in connection with the use, delivery, license, performance or otherwise of the certificates, electronic signatures, or any other transaction or service offered or contemplated in the Certification Practice Statement in case of misuse, or when used in transactions that carry a risk higher than the indemnity limit stated by ANF AC.

- In all the cases provided in article 23 of the Spanish Law 59/2003, of December 19, electronic signature.

- ANF AC assumes no other commitment or responsibility than those detailed in this CPS.

Specifically, with the subscribers and certificate responsible:

- When they fail to comply with the obligations contained in the Spanish Law 59/2003 of December 19, of Electronic Signature and development regulations, in this CPS and in the corresponding Certification Policies. Especially the obligations outlined in section 9.5.3 of this CPS.

And specifically, with relying parties:

- When they fail to comply with the obligations contained in the Spanish Law 59/2003, of December 19, of Electronic Signature and development regulations, in this CPS and in the corresponding Certification Policies. Especially the obligations outlined in section 9.5.4 of this CPS.

9.6.2 Of the Registration Authority

In the event that the Recognized Registry Authority (RRA) fails to comply with the obligations contained in the Spanish Law 59/2003, of December 19, of Electronic Signature and development regulations, in this CPS, in the Certification Policies corresponding to the certification procedures in which it intervenes, and in the terms established in the agreement that formalizes its activity as an RRA of ANF AC, shall be liable to ANF AC for damages caused in the exercise of the functions it assumes.

When the functions of identification are carried out by the Public Administrations subscribing to the certificates, the liability of the Public Administrations, shall be the one established in article 139 and subsequent of the Spanish Law of Legal Regime of Public Administrations and Common Administrative Procedure.

9.6.3 Of the subscriber

The subscriber is responsible for all authenticated electronic communications and documents, in which an electronic signature generated using his/her private key has been used, and the certificate has been validly confirmed through ANF AC's verification services.

Within the period of validity of the certificate, or as long as the revocation of the certificate is not recorded in ANF AC's records, liability that may arise from unauthorized and/or improper use of the Certificates, shall in any case correspond to the subscriber.

Upon acceptance of the Certificate, the subscriber undertakes to indemnify and hold ANF AC, Recognized Registry Authorities, and Relying Parties harmless of any act or omission that causes damages, losses, debts, procedural expenses or of any kind, including professional fees, in which they may be incurred. Especially when it comes to:

- breach of the terms foreseen in requesting certificates and contracting certification services that links them with ANF AC;

- the use of the Certificates in operations in which the limit of use has not been respected or that are prohibited, as expressed in this CPS and corresponding Certification Policies;

- The subscriber falsifies or intentionally errors;

- any omission done negligently or with the intention to deceive of a fundamental fact in the Certificates;

- breach of the duty to safeguard private keys, and to take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized use of private keys;

- breach of the duty to maintain the confidentiality of signature creation data and protect them from access or disclosure;

- breach of the duty to request the suspension or revocation of the certificate in case of doubt as to the maintenance of the confidentiality of their signature creation data;

- failure to comply with the duty to refrain from using signature creation data from the time the certificate validity period expires or the service provider notifies them of their loss of validity;

- breach of the obligation to communicate without delay any change in the circumstances reflected in the certificate;

9.6.4 Of relying third parties

The relying parties of a non-valid certificate or electronic signature that has not been verified with the devices that ANF AC has developed and approved for this purpose, assumes all risks related to it and cannot demand any liability to ANF AC, to the Registration Authorities, or to the subscribers for any concept derived from their trust in such certificates and signatures.

In this sense, ANF AC will not be responsible for damages caused to the subscriber or relying parties, if the recipient of the electronically signed documents fails to comply with any of the obligations established in the Spanish Law 59/2003 of December 19, of Electronic Signature and development regulations, in this CPS, in the corresponding Certification Policies, and especially for non-compliance with the responsibilities outlined in section 9.5.4 of this document.

9.6.5 Of the publication services

Not applicable because the publication service is not an independent entity.

9.7 Financial liability

9.7.1 Indemnity clauses

ANF AC, in this document, in the Certification Policies and in the agreements, that link it with the subscriber, the Registration Authorities, and the relying parties, includes indemnity clauses in case of breach of its obligations or of the applicable legislation.

9.7.2 Limits of damage compensation

ANF AC states that:

- Certificates issued without the consideration of qualified cannot be used for operations that carry financial risk, and therefore the compensation limit is zero euros.

- Certificates issued with the consideration of qualified the limit assumed by the CA is established in the certificate itself, specifically in the extension "QcStatements" in the field "QcLimitValue" OID 0.4.0.1862.1.2. and in the proprietary extension OID 1.3.6.4.1.18332.41.1.

  If no amount is fixed, it should be interpreted that the CA does not assume the use of that certificate for transactions that entail financial risk, and therefore the indemnity limit is zero.

9.7.3 Financial capacity

In accordance with the provisions of article 20.2 of the Spanish Law 59/2003, of December 19, of Electronic Signature, ANF AC, to undertake the risk of liability for damages caused by the use of the certificates issued, has signed the corresponding liability insurance, and per the guidelines of issuance and management of extended validation SSL certificates published by CA/Browser Forum, has increased the amount required by current legislation, up to the amount of FIVE MILLION EUROS (€ 5,000,000).

The data related to the policy are as follows:

- Underwriting Entity: CFC Underwriting Limited. Registered in England and Wales, No. 3302887. VAT number 135541330. Authorized and regulated by the Financial Services Authority. FRN: 312848.

- Policy number: ESE06177320.

The coverage of this insurance polity reaches the Registration Authorities Recognized by ANF AC.

9.7.4 Fiduciary relationships

ANF AC does not act as a fiduciary agent, nor is it representative of any users or relying parties in the certificates it issues.

9.7.5 Administrative processes

ANF and the Registry Authorities have sufficient resources to maintain their operations and perform their tasks. The Registration Authorities are reasonably capable of assuming the risk of liability to subscribers and relying parties.

9.7.6 Disclaimer with the subscriber

ANF AC does not assume any liability derived from denials of service, except in those cases in which the subscription agreement establishes a penalty in this regard.

ANF AC assumes no liability for the transactions made by its subscribers using its certificates.

ANF AC does not assume any liability when the holder makes use of the certificates using instruments that are not homologated by ANF AC.

ANF AC accepts other exemptions established in the Certification Policy corresponding to the type of certificate in question.

Except as provided in this document, ANF AC does not assume any other commitment or provide any other guarantee, nor does it assume any other liability before certificate holders, their legal representatives, and/or the certificate responsible.

9.7.7 Disclaimer with the relying party

ANF AC assumes no liability when the relying parties does not assume its obligation to verify the status of the certificate, using ANF AC's verification instruments.

ANF AC accepts other exemptions established in the Certification Policy corresponding to the type of certificate in question.

Except as set forth in this document, ANF AC does not assume any other commitment or provide any other guarantee, nor does it assume any other liability to relying parties.

9.8 Interpretation and enforcement

9.8.1 Applicable law

The legislation applicable to this document and to the underlying legal relationships is that of the Kingdom of Spain.

This CPS should be interpreted in accordance with valid legislation, its development regulations and the specific legislation affecting its services, especially in the area of personal data protection and consumer protection legislation.

9.8.2 Jurisdiction clause

All parties expressly submit to the Courts and Tribunals of the city of Madrid, waiving their own jurisdiction if it were another.

9.8.3 Dispute resolution procedures

9.8.3.1 Applicable procedure for extrajudicial resolution of conflicts

ANF AC voluntarily submits, for the resolution of any contentious issue that may arise from the exercise of its activity, to the institutional arbitration of the Business Distribution Council Arbitration Court (TACED), which undertakes the designation of the sole Arbitrator and the administration of the arbitration - that will be of equity - in accordance with its Regulation, becoming obliged from now, to the fulfillment of the arbitration decision.

If any of the counterparties to ANF AC do not accept this arbitration procedure, the following section shall apply.

9.8.3.2 Legal procedure

All parties expressly submit to the Courts and Tribunals of the city of Barcelona, waiving their own jurisdiction if it were another.

9.8.4 Notifications

Any notification, demand, request, or any other communication required under the practices described in this CPS shall be made by means of an electronic document or electronic message signed in accordance

with the latter or in writing by certified mail addressed to any of the addresses contained in section 1.5.1 Trust Service Provider.

Electronic communications will become effective once the recipient receives them.

9.9 CPS and Certification Policies administration

The evolution of the certification services of ANF AC implies that this CPS, and the Certification Policies are subject to modifications. A system of numbered versions is established for the correct differentiation of successive editions of these documents.

Any need for modification must be justified from a technical, environmental, legal, or commercial point of view. All technical and legal implications of the new version of specifications should be considered.

Modifications will be established to ensure, in any case, that the resulting specifications meet the requirements that were intended to comply and that led to the change.

9.9.1 Validity period

This Certification Practice Statement becomes valid on the date written in the "Issue date" field in section 1.2 of this document. It expires on the date that a new version of the CPS becomes valid.

The same validity period applies to ANF AC's Signature and Certification Policies.

9.9.2 Termination effect

The obligations, rights and restrictions established in this CPS, and in the corresponding Certification and Electronic Signature Policies, obtained during their validity period, shall endure after their termination.

9.9.3 Approval procedure

The Head of the Legal Department and the Head of the Technical Department will analyze that the changes proposed in the CPS and Policies are aligned with the latest versions of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" drafted by the CA/B Forum, and that they meet the requirements that gave rise to the proposed modification. They also undertake an annual control of updating the CPS, Certification Policies, and other associated documents, issuing the corresponding version maintenance report or modifications proposals.

All reports are subject to approval by the Governing Board of the PKI, which assumes the responsibility of verifying their conformity and, if applicable, issuing order of application of the same.

9.9.3.1 Modifications that do not require a new document or version change

ANF AC may carry out modifications of this document without the need to publish a new document and, therefore, apply a version change as long as they are not material changes, such as:

- Corrections for typographical errors in the document
- Modifications to URLs
- Modifications in contact information

9.9.3.2 Modifications that require a new document or version change

Any modification not contemplated in the previous section, entails the publication of a new document and its change of version.

9.9.4 Notification of the publication of a new CPS and Policies

The provisions of the section of this document "Publication and notification policy" are followed.

9.9.5 Severability and survival

If any of the sections of this document or of the Policies are considered null or legally unenforceable, it will be considered as not applicable, remaining the rest of obligations, rights and restrictions established in this document, applicable.

The invalid or incomplete clause may be replaced by another equivalent and valid by agreement of the parties.

The rules contained in the sections: Obligations, Liability, and Confidentiality, will remain in effect after the termination of this CPS.

9.9.6 Entire agreement and notification

None of the terms of this CPS that directly affect the rights and obligations of ANF AC and that does not affect the rest of the parts, can be corrected, renounced, supplemented, modified or eliminated if it is not through an authenticated written document of ANF AC, which in no case implies extinctive novation, but merely modification, and does not affect the other rights and obligations of the other parties.

Notifications should be addressed to:

ANF Certification Authority

Address: Paseo de la Castellana, 79

28046 Madrid (Spain)

Notifications can be made personally or through written notification, in any case, the identity of the person involved in the communication must be reliably guaranteed. In case of representing a third party, it shall also sufficiently attest its capacity of representation.

9.10 Customer service office

ANF AC is committed to having a fully functioning free service of attention of users and receivers.

9.10.1 Office purpose

This service will attend to all commercial, legal, and technical consultations related to:

- Current legislation on electronic signatures.
- This CPS, Certification Policies, and certificate request document.
- The installation and use of devices related to electronic signatures.
- Installation and use of the approved software.
- The generation and use of approved containers and, in general, everything related to the provision of certification services that this CA performs.
- General queries on the basic concepts of the Public Key Infrastructure, electronic certificates, electronic signature, and trust services.

It will also perform on behalf of the user or the person it represents, the different operations that this CPS, and Certification Policies entrust to him.

9.10.2 Consultation procedure

The consultations will be carried out by electronic mail addressed to: info@anf.es

In them, the identifier of the user who is consulting or, in case of being a receiver, the identifier of the received signature will be reviewed. The queries are answered through the same means to the email address of the sender.

A personal assistance service is also available by telephone at 902 902 172 (calls from Spain) International (+34) 933 935 946

9.10.3 Claim procedure

If a claim is to be filed, this certification service provider has a form found at:

https://www.anf.es/en/show/section/technical_assistance

Every notification, demand, request, or other communication required under the practices described in this CPS shall be made by document or electronic message electronically signed, in accordance with the CPS or by certified mail to any of the address contained on the Section 1.5.1 Trust Service Provider

It is also possible to visit the Customer Service Office in person.

ANF AC will answer the claim form in writing in a period of no more than 15 working days. If the answer is not satisfactory, that specified under the "Dispute Resolution Procedures" section will be followed.

9.10.4 Identification procedure

The people who appear before the Customer Service Office must be clearly identified by ID or original passport. Those persons acting on behalf of third parties must submit sufficient powers of attorney.

10 Personal data protection

10.1 Introduction

ANF AC, for the development of its activity as a Qualified Provider of Trust Services, needs to have personal data of the certificate subscribers. In addition, it is necessary, for the adequate provision of the service in a public PKI, to facilitate public access to the information contained in the certificates and determine their validity. To do this, it has the authorization of the owner of the data.

The personal data used in the ANF AC certification system are of basic security level, medium security level and high security level, per the classification regulated in the Spanish Royal Decree 1720/2007 by which the Regulation of development of the Spanish Organic Law 15/1999 is approved, and therefore ANF AC, as responsible for the file, must adopt adequate security measures to the data guarded.

ANF AC undertakes not to disclose or assign to third parties, without the express consent of the interested party, any data to which it has access due to the provision of its certification services. These data are processed exclusively to provide the services required.

ANF AC is committed to protect the data received by the certificate subscribers or the Registration Authorities, placing the appropriate security measures to the required Security Level per their corresponding characteristics, and in accordance with the current legislation.

The employees of ANF AC and/or any person who must intervene in the treatment of the information, are informed about the obligations of confidentiality included in this section, having to sign the corresponding confidentiality commitments before accessing them, and be informed of the security measures that they must adopt. ANF AC provides a copy of this CPS to each operator, and provides training and legal assistance to consult any question or doubt they may need.

This CPS and its addendum are obligatory for personnel with access to personal data and information processing systems. The objective is to provide effective controls to ensure that company data is not subject to unauthorized loss, dissemination, or modification.

To this end, appropriate technical and organizational measures have been defined against unauthorized or unlawful processing of personal data and against the accidental loss or destruction or damage of personal data.

Recognized Registry Authorities, and all ANF AC personnel responsible for collecting information from certificate subscribers, subjects, relying parties or any other natural person served on behalf of ANF AC, shall verify that the data owner provides their consent to the processing of their personal data, and is informed of the purpose to be given and their inclusion in the file declared for this purpose by ANF AC, as well as their right of access, rectification, cancellation and opposition, and the form of exercising them. In

addition, authentication of subscribers to an online service will only require identification data that are adequate, relevant, and not excessive to allow access to such online service.

In cases where the data has not been collected directly from the interested parties, ANF will expressly, precisely, and unequivocally inform them, within three months of the moment of registration of the information.

The owner of the data may exercise the rights of access, rectification, cancellation, and opposition, by going to the Customer Service Office listed in section 9.10

10.2 Legal framework

In accordance with the provisions of article 19.3 of the Spanish Law 59/2003, of December 19, of electronic signature, the CPS of Electronic Certification Service Providers is considered a security document for the purposes provided in the legislation on the protection of personal data.

This document and the protection of its files containing personal data follow the requirements of the Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD) and Spanish Royal Decree 1720 / 2007 by which the Regulation of development of the Spanish Organic Law 15/1999 is approved.

10.3 Creation of files and official registration in the Spanish Data Protection Agency

ANF AC must process its subscribers' information to fulfill its obligations as a Trust Service Provider. All files used are registered with the AEPD's (Spanish Data Protection Agency) General Data Protection Register.

ANF AC is the Data Controller and acts as the Security Manager the Chief Security Officer, formally assuming the role of coordinating, and controlling appropriate security measures.

In summary, below is a list of files subject to security measures established in this document, together with their corresponding security level:

File name	CLIENTS (basic security level)
Registration reference	2053010725
Description	Data on name, address, National/Foreign Citizens ID card number, method of payment for the provision of the electronic signature service.

Purpose	Commercial relationship management in all aspects and electronic signature services.

File name	USERS (basic security level)
Registration reference	2053010728
Description	Electronic certificate subscribers' personal details.
Purpose	Management and maintenance of persons who have requested electronic certificates.

File name	ELECTRONIC CERTIFICATES (basic security level)
Registration reference	2053010726
Description	Information on electronic certificates issued by the company.
Purpose	Management of issuing, administration and public consultations of certificates issued by the company.

File name	EXTERNAL COLLABORATORS (basic security level)
Registration reference	2053010729
Description	Personal data files of external collaborators of the company.
Purpose	Management and control of professional relationships with external collaborators of the company.

File name	SUPPLIERS (basic security level)
Registration reference	2053010733
Description	File containing company providers.
Purpose	Management and control of commercial relationships with providers of the company.

File name	HUMAN RESOURCES (medium security level)
Registration reference	2053010735

Description	Data file of company personnel.
Purpose	Company human resources management.

File name	CALLS RECORDING (medium security level)
Registration reference	2131300653
Description	Recording file of calls from customers and suppliers.
Purpose	Compliance with obligations in the provision of electronic signature certification and quality management services.

File name	BLACK LIST (medium security level)
Registration reference	2131300654
Description	List of natural and legal persons that are prevented from obtaining an electronic certificate.
Purpose	Compliance with obligations in the provision of electronic signature certification services.

File name	VIDEO SURVEILLANCE (high security level)
Registration reference	2131970653
Description	Installation of video surveillance systems in the organization for security reasons.
Purpose	Security control at the organization's premises

File name	FINGER PRINT (high security level)
Registration reference	2142900743
Description	Fingerprint of the electronic certificate subscriber or his/her legal representative as part of the identification process
Purpose	Provision of electronic signature certification services

The files reviewed contain personal data, so that, as determined in article 81 of the Spanish Royal Decree 1720/2007, the security measures corresponding to the level of security specified per the content in each of them are applicable.

The description of the structure and other requirements of the files is detailed in the document "Normative of registration and authorization of files" with OID 1.3.6.1.4.1.18332.39.8.1.

10.4 Scope of application

In accordance with the provisions of Spanish Law 59/2003, of December 19, Electronic Signature, this CPS is the Security Document for the purposes provided in the legislation regarding personal data protection.

In the development of this CPS, the Internet Engineering Task Force (IETF) specification RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (IETF) has been considered, having already measured multiple organizational and security aspects of ANF AC.

However, to meet all the requirements required by the Spanish Organic Law on Data Protection and the Spanish Royal Decree 1720/2007 approving the Regulation for the implementation of the Spanish Organic Law 15/1999, aspects that complement all those specified in previous section have been included in this CPS, to comply with the requirements of considering this CPS the Security Document in accordance to the Spanish Organic Law 15/1999.

This Security Document is obligatory for all personnel of the entity or external personnel who have access to the personal data that are the responsibility of the entity.

The documents listed in section 9.4 "Classification of documents drafted by ANF AC", classified as "non-public", which establish procedures and standards for data protection, have been brought to the attention of all personnel with access to personal data, and are included in the documentation to be delivered to the personnel at the time of hiring, to give due compliance with the current legislation.

The effective protection of personal data against unauthorized treatment or access, alteration or loss is done through the control of all the manners in which this information can be accessed.

Thus, the resources that serve as direct or indirect means to access the files with personal data of ANF AC, and thus, must be controlled by the regulations to the effect are:

- The facilities or treatment centers and premises where the files are located, and the storages and documents containing them.
- The servers, and the operating system and communications environment in which they are located and operated with the automated files.
- Non-automated documentation and information files.
- Systems, whether automated, manual, or mixed, established to access data.

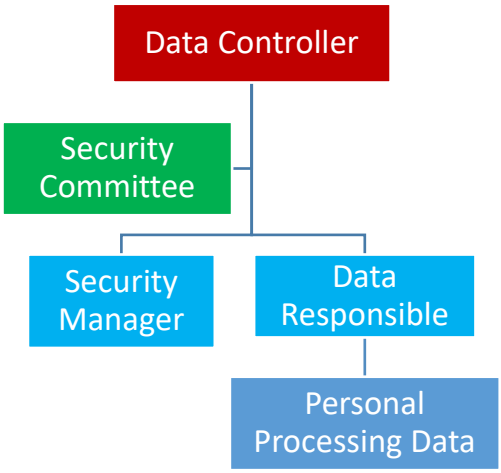
10.5 Security organization for the protection of personal data

This section describes the Security Organization established in ANF AC to guarantee the security of Personal Data.

The Organizational Security Model is represented, identifying, and showing the units involved and the hierarchical or functional dependency between them.

10.5.1 Security Organizational Model

The following chart shows the simplified graphic representation of the security structure to manage and control the security of the Personal Data in ANF AC. They represent the responsible units involved in the security organization and the hierarchical or functional relationships between them, namely, date controller, security committee, security manager, data responsible, and users.



10.5.2 Classification of units for the organization of security

This Certification Practice Statement is known by all ANF staff and is mandatory.

An organizational model has been created that establishes the functions assumed by each department involved in the treatment and security of the data, defining each of those responsible, namely:

Data Controller: it is **ANF AC**. It assumes the legal responsibility for the security of the data contained in the files and notifies in its behalf all creation of files before the Spanish General Registry of Data Protection.

Security Committee: Adopts and implements the necessary security measures so that the personnel involved in the processing of information are aware of and assume their responsibilities, and have the necessary capacity to carry out their work properly. Coordinates the different operational areas, both internal and external collaborations with third parties. The body in charge of keeping the CPS valid.

Security Manager: it is the Chief Security Officer, formally assumes the role of Security Manager. Coordinates and controls the security measures applicable in all its legal aspects, with the assistance of the Chief Legal and Human Resources Officer. Collaborates with the Data Controller and the Security Committee in the dissemination of the security document, cooperating in complying with it.

Technical Responsible of the Files (functional Responsible): it is the Chief Information Technology Officer. It is the person in charge of deciding on the operative aspects of the Information Systems, from the functional point of view of the services, as well as of the control and application of computer security measures. Collaborates with the Data Controller and the Security Committee in the dissemination of the security document, cooperating in complying with it.

Administrative Responsible of the Files (functional Responsible): it is the Chief Legal and Human Resources Officer. It is the person in charge of all the administrative processes that deal with the documentation that contains personal data, as well as the processes of loading of data, and of the attention to the requirements that the owners of the information solicit. Collaborates with the Data Controller and the Security Committee in the dissemination of the security document, cooperating in complying with it.

Personal processing data: depending on the Functional Technical or Administrative Responsible, per the area to which the file is associated, are the persons who, in the development of their functions, perform the processing of personal data.

All personnel previously mentioned are obliged to respect the rules and procedures contained in this CPS in its effects as a Security Document, as well as all the obligations established in the current legislation.

10.6 Safety Rules and Procedures

Personal data have precise measures, rules, and procedures to ensure their safety.

To this end, the Security Document pays special attention to the operating system environment, as well as to the premises and workstations in which computers containing the file that is object of protection by that document are located.

10.6.1 Rules

ANF AC has the necessary rules to guarantee the protection of the Personal Data that it treats in the exercise of its functions, and, thus, to comply with the applicable legislation to this type of data.

These standards apply to all ANF AC's services, information systems, to all Personal Data contained therein in any format (computer, paper, video ...) and to any person (internal or external) who makes use of these elements.

10.6.2 Procedures

On the other hand, ANF AC has the necessary procedures to guarantee the protection of Personal Data.

These procedures are applicable to all services, dependencies, and information systems of ANF AC, to all personal data contained therein in any format (computer, paper, video ...) and to any person (internal or external) who uses these elements.

The following sections describe the rules and procedures applied and followed by ANF AC in the area of personal data protection.

10.6.3 Information systems that storage the file

Within the structure of information systems that constitute ANF AC can be distinguished three subsystems in the treatment of the data. Specifically:

- Certificate management subsystem. It receives the minutes of identification, the certificates of request, and is responsible for issuing the certificates.
- Management subsystem. Assumes the internal management of the organization, suppliers, human resources, customers, and billing.
- Subsystem for analysis and verification of information. It is responsible for verifying subscriber identification, verifying the legal representation capacity of the legal representative, and verifying the veracity of the attributes that are requested to be included in the certificate. Emits decision of issuance or denial of service.
- Publishing subsystem. It is responsible for publishing certificate revocation lists (CRLs) and certificate repository lists.

More information in OID document 1.3.6.1.4.1.18332.37.5.1 "Description of Information Systems".

10.6.4 Backup and recovery copies

Backups are performed daily in incremental mode, and a complete data backup is performed monthly.

The data recoveries are made with the authorization of the person in charge of the file.

If the restoration is motivated by an incident caused by an attack to the system, the Technical Responsible of the files, prior to the restoration, must obtain an authorization from the owners of the data.

If the incident is a fortuitous type of computer system, the backup procedure established in the Technical Department will be followed.

More information in the document "Technical documentation of the procedures of backup and recovery of data" with OID 1.3.6.1.4.1.18332.37.3.1.

10.6.5 Access control

The Administrative Responsible of the Files and the Data Controller, together with the Security Manager, determine the persons who are authorized to make use of personal data processing equipment, always based on the principle of necessity for the adequate management of the services of ANF AC and depending on the position they occupy. The worker shall be established and informed of the duties to be performed, and the appropriate procedure to carry them out.

Solely, the Administrative Responsible of the Files is authorized to grant, alter, or cancel, alone, the authorized access to the data and the resources.

All equipment that has access to personal data is of restricted access.

All information hosted on the corporate network of ANF AC, statically or circulating in the form of emails, or any other type of physical support, is property of the company and is therefore confidential.

Security personnel are responsible for determining, implementing, managing, authorizing, inspecting or revalidating, as appropriate, the set of measures and security measures, as well as the rules and procedures that ensure the control of physical access to premises.

More information on the following documents:

- ISMS Security Policy Manual (OID 1.3.6.1.4.1.18332.101.45.2)
- Physical and Environmental Security Policy (OID 1.3.6.1.4.1.18332.101.45.14)
- Normative of Access for Non-Automated Files (OID: 1.3.6.1.4.1.18332.52.4.1)

10.6.6 Use of real data in tests

It is forbidden to use real personal data to perform tests, which is separated from the real environment.

10.6.7 Norms associated with the security document

ANF AC has rules that allow to guarantee in a sufficient way the protection of the Personal Data that it treats in the exercise of its functions, and thus to fulfill the obligations established in the current legislation.

These standards apply to all areas of work, personnel, external collaborators, and information systems, regardless of the support (computer, paper, video, etc.).

The list of documents published by ANF AC is detailed in section 9.4 "Classification of documents drafted by ANF AC" of this document. ANF AC undertakes to keep them updated at all times, and should be reviewed whenever relevant changes occur in the information system or in the organization of the entity. Likewise, it must be adapted at all times to the current provisions regarding the security of personal data.

The personnel affected by this Security Document know and must fulfill the part of the same that affects the development of their functions. Failure to comply with the obligations and security measures established in this document by the affected personnel shall be sanctioned per the disciplinary sanctions that contemplate the labor regulations at any time, without prejudice to the right of repetition for damages caused to the company, both for lost profits and for emerging damages.

The Administrative Responsible of the Files is in charge of keeping the Security Document up to date and will be in charge of communicating the modifications to the personnel that may be affected.

10.6.8 Identification and authentication

General principles:

1. ANF AC identifies and authenticates users who access its Information System.
2. The Security Manager supervises logging into and out of any system and application, and modifications to user access rights.
3. Given the importance of users' access to the Information System, the Security Manager must always have up-to-date knowledge of who is authorized to access the Information Systems.

ANF AC's employees have devices which have incorporated biometric identification and system authentication systems through electronic signatures. In some processes, authentication can come through the introduction of a username and password. This process follows an Access Key Policy

More information can be found in document OID 1.3.6.1.4.1.18332.45.3.1 "Access Keys Policy".

10.6.9 Modification of information system data

Modification of data means the change of any application data made directly or indirectly, by any software tool, other than the application itself for the processing of data by users of the same and using permissions or tools not common in daily operations.

These procedures are described in OID 1.3.6.1.4.1.18332.37.3.1 "Technical Documentation of Data Backup and Recovery Procedures".

10.6.10 Temporary files processing

The document OID 1.3.6.1.4.1.18332.39.6.1 "Regulations for the treatment of temporary files" describes the treatment that ANF AC performs for temporary files containing personal data.

10.6.11 Opposition, access, rectification, and cancellation of data

The OID document 1.3.6.1.4.1.18332.39.9.1 "Procedure for the exercise of the rights of owners of data" describes the procedures for exercising the rights of access, rectification, cancellation, and opposition to personal data.

10.6.12 Access to data through communication networks

The security measures required to access personal data through networks and communication ports, as well as firewalls, routers, antispam, guarantee a level of security equivalent to that of access in local mode.

10.6.13 Method of working outside of the premises in which the file is stored

The execution of processing of personal data outside the premises of the location where the file is stored must be expressly authorized by the person responsible for the file and, in any case, the level of security corresponding to the type of file processed must be guaranteed.

The Security Manager must create an operation that specifies point by point the procedures performed to ensure the security of the files outside the organization.

Processing time and date
User name
Processing operator
Duration of processing outside of the organization
Files
Date and time of departure
Authorization

10.6.14 Personnel functions and obligations

To comply with current legislation, ANF AC has established a series of obligations that must be known, accepted, complied with, and respected by the personnel.

To ensure that all persons are aware of the security rules that affect the performance of their duties, as well as the consequences of non-compliance, they will be informed with acknowledgment of receipt of the security documents that are delivered to them.

Likewise, ANF AC, through its Security Manager, will periodically inform the personnel of news about security in the treatment of personal data.

Document OID 1.3.6.1.4.1.18332.39.10.1 "Functions and Obligations of Personnel" describes the functions and obligations of the personnel related to the Spanish Organic Law for Data Protection and identifies the different responsible regarding the Spanish Organic Law for Data Protection.

10.6.15 File structure and systems which process them

To comply with current legislation, ANF declares the structure of its files and describes the Information Systems that treat them.

In the OID Document 1.3.6.1.4.1.18332.39.7.1 "Structure of the Data Files" the structure and description of the personal data included in the basic, medium, and high level files respectively are shown.

The description of the Information Systems that deal with these files appears in the document OID 1.3.6.1.4.1.18332.37.5.1 "Description of information systems".

10.6.16 Rules for notification, management, and response to incidents

To comply with the provisions of current legislation, ANF AC has the following rules for notification, management, and response of incidents, understanding "incidence" as any anomaly that affects or may affect the security or integrity of the data.

The details of the procedure can be found in document OID 1.3.6.1.4.1.18332.39.5.1 "Incident Management Procedure".

10.6.16.1 Notification

Any person who is part of ANF AC's personnel, or is temporarily providing services in ANF AC, must immediately notify the Security Manager of any anomaly that detects and that affects or may affect the

security of the data. The delay in notification of incidents constitutes a breach of contractual good faith, among other possible infractions, punishable per the applicable labor and/or corporate regulations.

10.6.16.2 Management

The Security Manager must register the incident in the corresponding application and address it to the Security Committee.

10.6.16.3 Response

The Security Committee must respond to the incident in the shortest time possible, ensuring at all times that the security and integrity of the data is not compromised. Once the incident has been corrected, the Data Controller will be informed.

10.6.16.4 Record

A record must be created stating the following:

- Type of incidence and moment in which it has occurred.
- Person who performs and who receives the notification.
- Effects arising from such notification.

It is the responsibility of the Data Controller to ensure the updated maintenance of the incident record.

10.6.17 Internal control and audit

1. Internal Control. Continuously and with a minimum frequency of once a year, the Security Manager will carry out a follow-up to verify compliance with the provisions of this Security Document.

2. Audit. Every two years there will be an audit (internal or external) of the information systems and data processing facilities to verify compliance with current legislation.

   The audit report will assess the adequacy of the measures and controls, identifying deficiencies, and proposing the necessary corrective or complementary measures.

   The audit reports will be analyzed by the Security Manager, who will forward the conclusions to the Data Controller, to take the necessary corrective measures, and will be available to the Spanish Data Protection Agency.

10.6.18 Procedure for notification, management, and response to incidents

For the execution of the recovery procedures, the written authorization of the person responsible for the file must be specified.

10.6.19 Additional high level measures

The measures described below will apply to the High Security Level files indicated in document OID 1.3.6.1.4.1.18332.39.7.1 "Structure of the Data Files", only in case the entity has files of this level.

10.6.19.1 Access control and digital information confidentiality

From each access, it will be stored the user identification, the date and time of access, the file accessed, the type of access and whether it has been authorized or denied.

If the access has been authorized, it is stored in the access register that allows to identify the accessed record. Access log data is stored for two years.

It is not allowed to deactivate access mechanisms, which is controlled by the Security Manager.

The Safety Manager will be in charge of monthly inspections of the registered control information, preparing a report of the revisions made and the problems detected.

10.6.19.2 Media management

The distribution of media containing high security level data is done by encrypting such data or by using any other mechanism to ensure that such information is neither intelligible nor manipulated during transport.

These supports will be identified by means of an understandable and meaningful labeling system, which will allow users with authorized access to the aforementioned media and documents to identify their content and make identification difficult for other people.

It will avoid the processing of personal data in portable devices that do not allow their encryption. If this is strictly necessary, it shall be reasonably stated in this Safety Document and measures shall be taken considering the risks of carrying out treatments in unprotected environments.

10.6.19.3 Physical access control

Only the personnel authorized in the security document may have access to the places where the physical equipment that supports the information systems is installed.

In the case of non-digital media, access to documentation is limited to authorized personnel only.

Mechanisms will be established to identify the accesses made in the case of documents that can be used by multiple users.

Access by unauthorized persons to high level data should be properly recorded in the Security Document.

10.6.19.4 Telecommunications

The transmission of high-level personal data and remote connections through telecommunications networks is done by encrypting such data or using any other mechanism to ensure that such information is not intelligible or manipulated by third parties.

10.6.19.5 High level personal data transmission record model

Data transmitted
Encryption method
Date and time of the transmission

10.6.19.6 Procedure to conduct backup and data recovery

A backup copy of the data recovery procedures is kept in a different place from the one in which the computer equipment that treats them is kept, in any case complying with the required security measures.

10.6.19.7 "Access log" monthly record model

Access to high level personal data, if verified, will be recorded in a monthly report which should include the following data:

File name
Date and time in which the access was made
File accessed
Type of access and if authorization was given
Record accessed
Management made on the file
Security Manager authorization