SSL and Electronic Headquarters

Certification Policy

SSL DV, OV, EV, QWAC and PSD2

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

902 902 172 (calls from Spain)

International +34 933 935 946

Website: www.anf.es

Security Level

Public document

Important Notice

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

902 902 172 (calls from Spain) International (+34) 933 935 946

Website: www.anf.es

INDEX

1. INTRODUCTION

1.1. Overview

This Certificate Policy (CP) defines the procedural and operational requirements that ANF AC follows for the issuance and management of Publicly-Trusted Certificates; certificates for Secure Server SSL in accordance to Certification Authority/Browser Forum (CA/B Forum) *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate* (herinafter, Baseline Requirements), certificates for Secure Server SSL with Extended Validation in accordance to CA/Browser Forum *Guidelines for Extended Validation Certificates* (hereinafter, EV Guidelines) and Qualified Web Authentication Certificates (QWAC) in accordance to Regulation (EU) 910/2014 (hereinafter, eIDAS Regulation).

Its purpose is to detail and complete what is generically defined in ANF AC's Certification Practice Statement (OID 1.3.6.1.4.1.18332.1.9.1.1) for this type of certificates and specify the policies ANF AC adopts to meet the current versions of the following policies, guidelines, and requirements:

- Article 45 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
- Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates,
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- Spanish Law 40/2015, of October 1, on the Legal Regime of the Public Sector. The profile of the electronic headquarters certificate is defined by the Ministry of Finance and Public Administrations (Ministerio de Hacienda y Administraciones Públicas).
- The CA/B Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* located at https://cabforum.org/baseline-requirements-documents ,
- the CA/B Forum *Guidelines for Extended Validation Certificates* located at https://cabforum.org/extended-validation ,
- the CA/B Forum *Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates*,
- Microsoft Trusted Root Program Requirements,
- Mozilla Root Store Policy, and
- Google's Certificate Transparency project.

With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this CP and the requirements and guidelines above, then the CA/B Forum requirements and guidelines above take precedence.

This CP is only one of several documents that govern ANF AC's PKI. Other important documents include Certification Practice Statements (CPS), registration authority agreement, subscriber agreements, relying party agreements, privacy policies, and ANF AC's addendum. These supplemental policies and statements are available to applicable users or relying parties.

In conformance with RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for certificate or time-stamping services within ANF AC's PKI.

Section and subsection headings already covered by ANF AC's CPS have the statement "defined in the CPS of ANF AC".

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

1.1.1. Description of certificates

ANF AC, in the framework of its electronic certification service, issues technical certificates of the type:

Secure Server SSL	Electronic Headquarters
Domain Validation (DV)	Medium and high level
Organization Validation (OV)	Extended Validation medium and high level
Extended Validation (EV) Qualified Website Authentication (QWAC)	
Extended Validatio (EV) QWAC for PSD2 (QWAC PSD2)	

Secure Server SSL certificates:

- **Domain Validated Secure Server SSL Certificate (DV)**
  This certificate will be used for the identification of the ownership of the domain hosting the website, providing reasonable assurance to the user of an Internet browser. It can be issued as wildcard. The DV Wildcard contains a "wild card" in the hostname (e.g.: *.frater.com). They are issued according to the CA/B Forum Baseline Requirements and ETSI EN 319 411-1. The validity of these certificates can be up to 397 days.

- **Organization Validated Secure Server SSL Certificate (OV)**
  This certificate will be used for identifying ownership of the domain and accreditation of the organization, providing reasonable assurance to the user of an Internet browser that the web site being accessed is owned by the organization identified in the certificate. The OV Wildcard contains a "wild card" in the hostname (e.g.: *.frater.com). They are issued according to the CA/B Forum Baseline Requirements and in compliance with ETSI EN 319 411-1. The validity of these certificates can be up to 397 days.

- **Qualified SSL Extended Validation (EV) - Qualified Website Authentication Certificate (QWAC)**
  Secure Server SSL certificate with Extended Validation, in compliance with eIDAS Regulation. This certificate, with consideration of qualified per eIDAS, will be used for identifying ownership of the domain and accreditation of the organization, providing a strong guarantee to the user of an Internet browser that the web site being accessed is owned by the organization identified in the certificate. In compliance with the requirements established in ETSI EN 319 412-4 and by CA/B Forum EV Guidelines. This type of certificate can only be issued to legal persons. The certificates issued with Extended Validation have a maximum validity period of 397 days.

  In addition to the utilities provided by the SSL certificate, Extended Validation (EV) aims to provide a better level of authentication for organizations to secure transactions on their websites. The purpose of EV SSL Certificates is their use in TLS/SSL protocols, to ensure the validity of the constitution of the organization identified in the certificate, and therefore avoiding phishing or other cases of online identity fraud.

- **Qualified Website Authentication Certificate for PSD2 (QWAC PSD2)**
  This certificate, with the consideration of qualified according to the eIDAS Regulation, is a QWAC *(ETSI EN 319 412-4 and CA/B Forum EV Guidelines)* issued in accordance with the ETSI TS 119 495 and complies with the Regulatory Technical Standards (RTS) of Delegated Regulation (EU) 2018/389 of the Commission, which complements the Directive (EU) 2015/2366, and Royal Decree-law 19/2018 of Spain, respecting the guidelines established by the Competent National Authority for payment services. ANF AC guarantees a procedure for identifying ownership of the domain and accreditation of the organization that owns it, equivalent to the procedure followed for the issuance of certificates with Extended Validation (EV). The certificates issued with Extended Validation have a maximum validity period of 397 days.

Electronic Headquarters certificate *(in accordance to Spanish Law 40/2015)***:**

- **Extended Validation (EV) Electronic Headquarters Qualified Certificate**
  Within the scope of the Spanish Law 40/2015, of October 1st, of the Public Sector's Legal Regime, ANF AC issues certificates of the electronic headquarters type. They are issued per the ETSI EN 319 411-4 standard, in conformance with CA/B Forum EV Guidelines, and the profile of the office certificate defined by the Ministry of Finance and Public Administrations. These are qualified web authentication certificates according to the eIDAS Regulation, in which the Public Administration, administrative body or entity owner of the office is identified. The purpose of this certificate is to establish data communications through TLS/SSL in services and computer applications, provide authentication for Public Administration, administrative body, or entity to secure transactions on their websites, avoiding phishing or any other online identity fraud cases.

  The maximum validity period of these certificates is 397 days.

  Certificates of the type Electronic Headquarters will follow the definitions established by the Directorate of Information and Communication Technologies (DTIC) of the Ministry of Finance and Public Administrations, in their document "Profiles of electronic certificates" of April 2016. Two levels of assurance are defined:
  a. Medium / substantial level:
     This level corresponds to a configuration of security mechanisms appropriate for most applications. The risk foreseen by this level is appropriate to access applications classified according to the ENS at the Integrity and Authenticity levels as low or medium risk.
  b. High level:
     This level corresponds to a configuration of appropriate security mechanisms for applications that require additional measures, in response to the risk analysis carried out. The risk foreseen by this level is appropriate to access applications classified according to the ENS at the Integrity and Authenticity levels as high risk.

1.2. Document name and identification

Document name	SSL and Electronic Headquarters Certificate Policy
Version	3.3.2.
Policy status	APPROVED
Document OID	1.3.6.1.4.1.18332.55.1.1
Publication date	31/03/2021
Related CPS	Certification Practice Statement (CPS) of ANF AC
Location	https://www.anf.es/en/

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

1.2.1. Revisions

Version	Changes	Approval	Publication
3.3.2.	Inclusion of DCV methods 3.2.2.4.13. and 3.2.2.4.14.	31/03/2021	31/03/2021
3.3.1.	Update band of accreditations, fix of typos and acronyms	08/01/2021	08/01/2021
3.3.	Corrections to align with Mozila's Root Store Policy	09/11/2020	09/11/2020
3.2.1	Update of breach/misuse reporting links.	30/10/2020	30/10/2020
3.2.	BR update 1.7.3. and EVG update 1.7.4. Changes in Reasons for Revoking a Subscriber Certificate and clarification in section 6.1.2.	10/10/2020	10/10/2020
3.1.	BR update 1.7.2. Minor change, the non-use of method 3.2.2.4.10 is specified	20/09/2020	20/09/2020
3.0	BR update 1.7.1. and EVG 1.7.3. Change of maximum validity to 397 days.	10/08/2020	10/08/2020
2.10	BR update 1.7.0. Without changes.	15/04/2020	15/04/2020
2.9	BR 1.6.8 & 1.6.9 and EVG 1.7.2 update review. Without changes. ANF AC does not issue .onion certificates	25/02/2020	25/02/2020
2.8	Improved RFC 3647 adaptation. BR update *1.6.6*. and removal of IV SSL certificate.	19/07/2019	19/07/2019
2.7	Update to clarify and comply with PSD2 policy requirements stated in ETSI TS 119 495	28/03/2019	28/03/2019
2.6	Inclusion of PSD2 certificates	30/01/2019	30/01/2019
2.5	Annual review	15/01/2019	15/01/2019
2.4	Annual review	22/02/2018	22/02/2018
2.3	Update to adapt to and comply with eIDAS requirements an EV Guidelines	27/02/2017	27/02/2017
2.2	Review and update for clarification	04/11/2016	04/11/2016
2.1	Updated for consistency with CA/Browser Forum Baseline Requirements	25/06/2016	25/06/2016
2.0	Document creation	10/07/2015	10/07/2015

1.2.2. OIDs

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

For technical certificates issued by the **ANF Global Root CA** hierarchy, with an expiration date **2036**:

Secure Server SSL	DV	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.1.22
	OV		1.3.6.1.4.1.18332.55.1.1.7.22
Qualified Secure Server SSL *(QWAC)*	PSD2	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.8.22
	Qualified EV *(QWAC)*		1.3.6.1.4.1.18332.55.1.1.2.22
Electronic Headquarters EV	Medium Level	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.5.22
	High Level	HSM Token	1.3.6.1.4.1.18332.55.1.1.6.22

For technical certificates issued by the hierarchy **ANF Secure Server Root CA**:

Secure Server SSL	DV	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.1.322
	OV		1.3.6.1.4.1.18332.55.1.1.7.322
Qualified Secure Server SSL *(QWAC)*	PSD2	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.8.322
	Qualified EV *(QWAC)*		1.3.6.1.4.1.18332.55.1.1.2.322
Electronic Headquarters EV	Medium Level	Cryptographic softw.	1.3.6.1.4.1.18332.55.1.1.5.322
	High Level	HSM Token	1.3.6.1.4.1.18332.55.1.1.6.322

In the CertificatePolicies extension (2.5.29.32), it may be included, as a means of affirming compliance of this Policy with the criteria adopted by CA/Browser Forum and ETSI, the following identifiers:

	CA/B Forum	ETSI
SSL DV	2.23.140.1.2.1	DVCP *(Domain Validation Certificate Policy)*: 0.4.0.2042.1.5
SSL OV	2.23.140.1.2.2	OVCP *(Organizational Validation Certificate Policy):* 0.4.0.2042.1.6
Qualified EV *(QWAC)*	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4
QWAC PSD2	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4 QCP-W-PSD2 certificate policy for EU qualified PSD2 website authentication certificates 0.4.0.19494.3
QWAC Natural Person	2.23.140.1.2.3	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4

In addition, as a means of affirming compliance with the requirements established in the scope of the General Administration of the State of Spain and its public bodies, in the CertificatePolicies extension (2.5.29.32), it will be included in PolicyInformation in the case of Electronic Headquarters certificates:

	CA/B Forum	ETSI	Spanish Administration
High Level Electronic Headquarters EV	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* 0.4.0.194112.1.4	2.16.724.1.3.5.5.1
Medium Level Electronic Headquarters EV	2.23.140.1.1	QCP-W *(certificate policy for EU-certified website authentication certificates):* OID 0.4.0.194112.1.4 QCP-W-PSD2 certificate policy for EU qualified PSD2 website authentication certificates 0.4.0.19494.3	2.16.724.1.3.5.5.2

1.3. PKI participants

PKI participants are defined in the CPS of ANF AC.

The following Applicant roles are required for the issuance of an EV Certificate.

1. **Certificate Requester:** natural person who submits the EV Certificate Request, and has sufficient powers of representation of the organization or entity.who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
2. **Certificate Approver:** natural person who approves the EV Certificate Request, who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
3. **Contract Signer:** natural person authorized to sign the Subscriber Agreement applicable to the requested EV Certificat, who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
4. **Applicant Representative:** In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Certificates issued under this Policy may be used for the following purposes:

- DNS Identification. The certificate issued under this policy allows to identify and link a determined DNS (Domain Name System) to the entity owning that domain, which is the certificate subscriber.

- Encryption of communications between the user and the website, facilitating the exchange of encryption keys necessary for encryption of information through Internet.

1.4.2. Prohibited certificate uses

No other uses than the ones stated in this Policy and the CPS of ANF AC are allowed.

1.5. Policy administration

ANF AC oversees and supervises that this CP is compatible and consistent with the other documents produced. This document is periodically reviewed, at least once a year and whenever there are legal or regulatory changes that cause changes in the procedures. This Certification Policy is freely available to users and relying parties at https://www.anf.es

1.5.1. Organization administering the document

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.

Department	PKI Governing Board
Email	juntapki@anf.es
Address	Paseo de la Castellana, 79
Locality	Madrid
Postal code	28046
Telephone number	902 902 172 (Calls from Spain) International (+34) 933 935 946

1.5.2. Contact person

Department	Legal Department
Email 1	soporte@anf.es
Email 2	mcmateo@anf.es
Address	Paseo de la Castellana, 79
Locality	Madrid
Postal code	28046
Telephone number	902 902 172 (Calls from Spain) International (+34) 933 935 946

1.5.2.1. Revocation Reporting Contact Person

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit Certificate Problem Reports informing ANF AC of reasonable cause to revoke a certificate:

- By means of the contact person in this section 1.5.2.
- Directly filing the form found at https://www.anf.es/en/report-breach-misuse/
- Any other method specified in section 4.9.3. of this CPS.

This includes reporting suspected Private Key Compromise, Certificate misuse, other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to ANF AC's Certificates or PKI.

1.5.3. Person determining CPS suitability for the policy

ANF AC determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from an independent auditor (Refer to section 8). ANF AC is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. CPS approval procedures

Refer to ANF AC's CPS.

1.6. Definitions and acronyms

Definitions and acronyms are defined in the CPS of ANF AC except as otherwise defined herein:

1.6.1. Definitions

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

CAA: From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue."

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Validation Certificate (DVC): certificate which has no validated organizational identity information for the subject, only identifying the subject by its domain name

EV Certificate: A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with CA/B Forum EV Guidelines.

Organizational Validation Certificate (OVC): certificate that includes validated organizational identity information for the subject

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Government Information Source: A database maintained by a Government Entity that meets the requirements of Section 11.11.6 of the EV Guidelines.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognised as a dependable source of such information.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Verified Accountant Letter: A document meeting the requirements specified in Section 11.11.2 of the EV Guidelines.

Verified Legal Opinion: A document meeting the requirements specified in Section 11.11.1 of the EV Guidelines.

Verified Professional Letter: A Verified Accountant Letter or Verified Legal Opinion.

1.6.2. Acronyms

CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
DBA	Doing Business As
DNS	Domain Name System
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CSO	Chief Security Officer
EV	Extended Validation
gTLD	Generic Top-Level Domain
IFAC	International Federation of Accountants
ISP	Internet Service Provider
QGIS	Qualified Government Information Service
UTC(k)	National realization of Coordinated Universal Time
DVC	Domain Validation Certificate
EVC	Extended Validation Certificate
OVC	Organization Validation Certificate
IRM	Issuance Reports Manager
RRA	Recognized Registration Authority
IVO	Identity Verification Office

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

Refer to ANF AC's CPS.

2.2. Publication of certification information

Refer to ANF AC's CPS.

Specific for QWAC PSD2 Certificates: The Competent National Authority may request information about certificates that contain an authorization number from a Payment Service Provider (PSP) assigned by that institution. ANF AC will report on the certificates issued in accordance with the provisions of each repository.

In the scope of the Google Certificate Transparency (CT) project, the certificates issued with the EV (Extended Validation) qualification will be published in different CT Log operators, in order to comply with the proposal RFC 6962 *Certificate Transparency.*

2.3. Time or frequency of publication

Refer to ANF AC's CPS.

2.4. Access controls on repositories

Refer to ANF AC's CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

Refer to ANF AC's CPS. ANF AC does not issue certificates to a Domain Name with .onion in the right-most label of the Domain Name.

3.1.2. Need for names to be meaningful

All the certificates of the type Secure Server SSL and EV Secure Server SSL contain a Distinguished Name (DN) that identifies the DNS domain and the natural person or organization holder of the same, per the ITU-T X.501 Recommendation, and contained in the Subject field.

3.1.3. Anonymity or pseudonymity of subscribers

Not permitted.

3.1.4. Rules for interpreting various name forms

Refer to ANF AC's CPS.

3.1.5. Uniqueness of names

The certificate will be issued with the full name of the service that will be provided with SSL features. This name must be unique in the network. Partial names will not be accepted.

3.1.6. Recognition, authentication, and role of trademarks

Generally, as defined in the CPS of ANF AC.

For EV SSL, ANF AC does not include, in an OU attribute, a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless this information has been verified in accordance with the EV Guidelines.

3.2. Initial identity validation

This section describes the procedures carried out in general for identity validation. Which verification and application validation processes apply for each type of certificate are specified in section *4.2.1 Performing identification and authentication functions* of this CP.

3.2.1. Method to prove possession of private key

Refer to ANF AC's CPS.

3.2.2. Authentication of Organization and Domain Identity

ANF AC inspects any document relied upon under this Section for alteration or falsification.

3.2.2.1. Identity of the Organization

In the event the certificate is to include the data of an organization, ANF AC will verify the identity and address of the organization and that the address is the Applicant's address of existence or operation, in accordance with section 3.2.2.1 of the Baseline Requirements. For EV certificates, the list of "Verification sources" is published in the legal repository of ANF AC website.

The following will be required:

- **Tax identification (VAT card) of the entity.**

Furthermore, per the legal form ANF AC will verify the identity and address of the Applicant using:

- Corporations or other legal persons which registration is mandatory in the Mercantile Register, shall prove their valid incorporation by providing:
  - A certificate from the Mercantile Register in relation to the incorporation data and current management of the entity.
- Associations, foundations and cooperatives shall prove their valid incorporation by providing original or certified copy of a certificate from a public registry in which they are inscribed in relation to their incorporation.
- Civil societies and other legal persons shall provide original or certified copy of the public document attesting their incorporation in a reliable way.
- Public Administrations and public sector entities:
  - Entities whose inscription is mandatory in a registry, shall prove their valid incorporation by providing original or certified copy of a certificate of in relation to the incorporation data and legal personality.
  - Entities created by law, shall provide reference to the norm by which they were created.

Consultation with a third party database periodically updated and considered a reliable data source. Such a source is understood to be a database used for verifying information about organisations identity, recognised among commercial companies and public administrations as a reliable source and created by a third party different than the applicant. A document or report issued by a reliable source is also valid, like for example einforma, DUN & BRADSTREET or Legal Entity Identifier (LEI).

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

3.2.2.2. DBA/Tradename

ANF AC does not allow the use of a DBA.

3.2.2.3. Verification of Country

If the subject:countryName field is to be present, ANF AC verifies the country associated with the Subject by the method identified in Section 3.2.2.1 or, alternatively, by the ccTLD of the requested Domain Name.

3.2.2.4. Validation of Domain Authorisation or Control

ANF AC confirms that, prior to issuance, has validated the Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the following methods listed in section 3.2.2.4 of the Baseline Requirements:

Email, Fax, SMS, or Postal Mail to Domain Contact *(3.2.2.4.2)*	Sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact in the "registrant", "technical", or "administrative" WHOIS records. Email addresses are limited to local-parts of "admin", "administrator", "webmaster", "hostmaster", and "postmaster". This Random Value is unique in each email, fax, SMS, or postal mail, and will remain valid for use in a confirming response for no more than 30 days from its creation.
Constructed Email to Domain Contact *(3.2.2.4.4)*	Sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster', followed by the atsign ("@"), followed by an Authorization Domain Name, including a Random Value in the email, and receiving a confirming response utilizing the Random

	Value, which will be unique for each email, and will remain valid for use in a confirming response for no more than 30 days from its creation.
Email to DNS CAA Contact *(3.2.2.4.13)*	Sending an email to a contact email included in DNS CAA tag "*contactemail*" (as indicated by BR *A.1.1. CAA contactemail Property*) including a random value (unique for each email, and with a validity period of 30 days from its creation), and receiving a confirming response utilizing said random value. The CAA resource record set is found using the search algorithm defined in RFC 8659, Section 3.
Email to DNS TXT Contact *(3.2.2.4.14)*	Sending an email to a contact email included on the DNS TXT "_validation-contactemail" subdomain of the domain being validated (as indicated by BR *A.2.1. DNS TXT Record Email Contact*), including a random value (unique for each email, and with a validity period of 30 days from its creation), and receiving a confirming response utilizing said random value.
Phone Contact with Domain Contact *(3.2.2.4.15)*	Calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

ANF AC does NOT use the retired Validation of Domain methods specified in Section 3.2.2.4.1, Section 3.2.2.4.3, Section 3.2.2.4.5, Section 3.2.2.4.6, Section 3.2.2.4.9, Section 3.2.2.4.10 and Section 3.2.2.4.11 of the CA/B Forum Baseline Requirements. ANF AC does NOT use the method described in Section 3.2.2.4.10 of the Baseline Requirements, as it contains major vulnerabilities.

ANF AC performs the domain validation tasks and does not delegate it to third parties.

ANF AC maintains a record of which domain validation method, including relevant BR version number, was used to validate every domain.

ANF AC does NOT issue certificates containing a new gTLD under consideration by ICANN, or an Internal Domain Name.

It is verified that the domain is not included as risky in Google's Safe Browsing List or in Miller Smiles phishing list.

Also, for domains associated to names that may create in relying third parties:

- Confusion of identity or activity.

The certificate issuance will not be authorized when the domain name may create confusion about the real activity of the subscriber, (e.g. www.bancoprogreso.com, when the subscriber's activity does not correspond to that of a financial institution).

- Especially relevant trademarks.

In case of a domain associated to an especially relevant trademark, the Patent and Trademark Register shall be verified. When the domain's name is associated to a trademark of special relevance and public awareness, it shall be verified if the owner of the trademark is related to the subscriber.

No certificate may be issued when the name is associated to a relevant trademark which is not owned by the subscriber of the domain, nor has permission from the owner of the trademark, since it may cause confusion to third parties (e.g. www.chanel.zn, www.cocacola.eu, etc.).

3.2.2.5. Wildcard Domain Validation

In case of DV SSL and OV SSL certificates the wildcard in subdomains or hostnames will be allowed, but not in top-level domains (TLD) or in the domain name.

The subscribing entity must be able to demonstrate their legitimate control on the entire domain, otherwise the application will be rejected. For example, *.co.uk, *.local or example.* cannot be issued but *.example.com may be issued to the company Example, LTD.

The determination of what is "*registry-controlled*" compared to the registrable part of a CountryCode Top-Level Domain Namespace is not standardized at the time of writing of the Baseline Requirements and is not a property of the DNS itself. The current best practice is to consult a "*public suffixes list*," such as http://publicsuffix.org/ (PSL), and retrieve a new copy regularly. If you use that list, ANF AC will consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. This list is regularly updated to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. ANF AC may issue a Wildcard to the Registrant of a complete gTLD, provided that control of the entire namespace is adequately demonstrated.

3.2.3. Authentication of individual identity

ANF AC will require the certificate requester, natural person, the following documentation:

- **ID card or passport** for national citizens or EU members. In case of non-EU foreign citizens: Passport; and residence permit of work permit, if applies. These documents shall containt a photograph allows verifying the identity of the person appearing. In case of low sharpness of the picture, another official document with picture may be requested (e.g. driver's license).

- **Sufficient Power of Attorney:** In addition to directors and legal representatives, voluntary representatives shall be accepted when they demonstrate sufficient powers of attorney to perform legal acts or celebration of contracts on behalf of the entity.

ANF AC will inspect the copy for any indication of alteration or falsification and verify the Applicant's address using a the same DNI, NIE or Passport.

ANF AC will verify the certificate request with the Applicant using a Reliable Method of Communication. For certificates with the consideration of "*qualified*" by eIDAS Regulation, the face-to-face verification of the identity of the applicant will be required, which can be avoided in case of notarization of the signature of the contract or in case of qualified signature in the contract and application.

3.2.4. Non-verified subscriber information

SSL DV Certificates do not include a verified organizational identity.

3.2.5. Validation of authority

ANF AC will take reasonable steps to establish that a Certificate request made on behalf of an Organization is legitimate and properly authorized. ANF AC will verify the sufficient powers of representation of the legal representative in accordance with section 3.2.3 of this CP.

In the case of SSL OV certificates, ANF AC will verify the authenticity of the representative through communication using a Reliable Method of Communication, as defined in the Baseline Requirements.

For EV Certificates, as specified in the EV Requirements.

In the application form, the subscriber must identify and expressly authorize the certificate responsible. This authorization must be perfected with a voluntary and express acceptance by the natural person who assumes the consideration as Certificate Responsible.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Refer to ANF AC's CPS.

3.3.2. Identification and authentication for re-key after revocation

Refer to ANF AC's CPS.

3.4. Identification and authentication for revocation request

Refer to ANF AC's CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

The certificate application must be carried out by a natural personal, of legal age, acting on its own behalf or as a legal representative of a third party.

In the case of EV Certificates and QWAC, ANF AC will only issue these type of certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified in section 8.5 of CA/B Forum EV Guidelines.

4.1.2. Enrollment process and responsibilities

4.1.2.1. Request process for DV and OV certificates

ANF AC obtains the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An signed Subscriber Agreement or Terms of Use, handsigned or electronically.

At the time ANF AC receives the request, the verification process will begin.

4.1.2.2. Request process for EV certificates

ANF AC obtains the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An signed Subscriber Agreement or Terms of Use.
3. *(Optional)* Authorization Letter, by which one or more persons are authorized to perform the functions described in the role of certificate approver. In that case, it must include the signature of the subscriber, in addition to that of the authorized persons, who, from that moment, may request/approve certificates.

Applicants are responsible for submitting sufficient information and documentation to ANF AC to perform the required verification of identity prior to issuing a Certificate. The subscriber will be able to submit it to ANF AC using any of the following means:

- **In person**: the subscriber may appear before a Recognised Registration Authority (RRA) or Identity Verification Office (IVO), in whose presence will proceed to sign the application form, which shall be dully fill out.
- **By mail:** certificate request form handwritten signed by the subscriber and his/her signature legitimized by public notary. Documentation sent by ordinary mail.
- **Electronically**: If the corresponding forms have been electronically signed by means of a qualified certificate for electronic signature.

The form contains a certification hat the subscriber assumes the responsibility of the accuracy of the information outlined.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The IRM shall verify the documentation provided by the subscriber, the Registration Authority (RRA) or the Identity Verification Office (IVO). ANF AC may reuse previous validations provided that ANF AC

obtained the data or document form a source specified under section 3.2 or completed the validation itself no more than 825 days prior to issuing the certificate.

RRA and IVO function, procedure and security measure applied in the procedures they carry out are in accordance with section 1.3.2 defined in the ANF AC's CPS.

The validation process will be supported by the Legal and Technical Department, which will review and technically validate the certificate request PKCS#10 / CRS. ANF AC is responsible for ensuring that the identity of each certificate applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a Certificate.

Prior to issuing a publicly-trusted SSL/TLS Server Certificate, ANF AC checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, according to the procedure in RFC 6844. ANF AC processes the "*issue*" and "*issuewild*" property tags. The issuer domain name recognized for ANF AC CAA Record is "anf.es". If the Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater. ANF AC will respect the critical flag and not issue a certificate if ANF AC encounters an unrecognised property with this flag set.

Moreover, to identify potential suspicious certificate requests, ANF AC verifies its internal database of all revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns.

Prior to using any data source as a Reliable Data Source, ANF AC evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. ANF AC takes into consideration the aspects highlighted in section 3.2.2.7 of the Baseline Requirements.

4.2.1.1. SSL DV Verification Requirements

In accordance with section 3.2.2.4 of this Certificate Policy.

4.2.1.2. SSL OV Verification Requirements

Verification of the applicant identity, address and country is performed in accordance with section 3.2.2.1, 3.2.2.2. and 3.2.2.3. of this CP. Domain name control verification is performed in accordance with section 3.2.2.4. of this CP.

4.2.1.3. SSL EV Verification Requirements

4.2.1.3.1. Verification of Applicant's Legal Existence and Identity

The verification procedures that will be defined in this section can be avoided if there is a **Verified Professional Letter** and if the following assumptions are met::

Verification Requirement	Completed if…
Applicant's Existence and Identity	The Verified Professional Letter includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act, and the CA confirms the Applicant's organization name specified in the Verified Professional Letter with a QIIS or QGIS.
Assumed name	The Verified Professional Letter indicates the assumed name under which the Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.
Physical Existence	The Verified Professional Letter indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

Operational Existence	The Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

Verification of Applicant's Legal Existence and Identity		
Private Organisation	**Aspects to be verified**	1. **Legal Existence.** *(Not designated on the records as "inactive", "invalid", "not current", or the equivalent).* 2. **Organisation Name.** 3. **Registration Number.** 4. **Registered Agent or Office.**
	Verification methods	One of the following options: 1. Online consultation with: ○ Mercantile Registry or other required registration records ○ National Chamber of Commerce, or ○ Legal entity identifier (LEI) 2. Certification issued by the Mercantile Registry or its equivalent, LEI or Chamber of Commerce, with a maximum of 30 days before the SSL EV certificate request.
Government Entity	**Aspects to be verified**	1. **Legal existence.** 2. **Entity Name**. 3. **Registration Number:** date of incorporation, registration or formation, or the identifier for the legislative act that created the Government Entity. If this information is not available, ANF AC will enter appropiate language to indicate that the Subject is a Government Entity.
	Verification methods	All items listed are directly verified with, or obtained directly from, one of the following: 1. Consultation with the official registry. 2. Official national or regional official bulletins for the publication of the creation of the governmental entity. 3. Consultation with the superior governmental entity that governs in the same political subdivision as the Applicant (for example, a Secretary of State can verify the legal existence of a specific State Department).
Business Entity	**Aspects to be verified**	1. **Legal Existence.** 2. **Organisation Name**. 3. **Registration Number.** 4. **Principal Individual[1] Identity.**
	Verification methods	One of the following options: 1. Online consultation with: ○ Mercantile Registry or other required registration records ○ National Chamber of Commerce, or ○ Legal entity identifier (LEI) 2. Certification issued by the Mercantile Registry or its equivalent, LEI or Chamber of Commerce, with a maximum of 30 days before the SSL EV certificate request. The Principal Individual associated with the business entity will be validated in person. ANF AC can be based on a face-to-face validation carried out by an authority that holds public faith, provided that ANF AC has evaluated the validation procedure and concluded that it meets the requirements of the

[1] *Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates*

EV Guidelines (section 11.11.3.) In other cases, ANF AC will perform the face-to-face verification of the Principal Individual.

Face-to-face verification: before an employee of ANF AC or Registration Authority of ANF AC. The main person(s) must submit the following documentation:

- A Personal Statement that includes the following information:
  1. Full name of names by which a person, is or has been, known (including all other names used);
  2. Residential Address at which he/she can be located;
  3. Date of birth; and,
  4. An affirmation that all of the information contained in the Certificate Request is true and correct.
- ID (DNI or equivalent) or Passport.
- At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.
  1. Acceptable **financial institution** documents include:
     a. A major credit card, provided that it contains an expiration date and has not expired.
     b. A debit card from a regulated financial institution, provided it contains an expiration date and has not expired.
     c. A mortgage statement from a recognisable lender that is less than six moths old.
     d. A bank statement from a regulated financial institution that is less than six months old.
  2. Acceptable **non-financial** documents include:
     a. Recent original utility bills ofr certificates from a utility company confirming the arrengement to pay for the services at a fixed address,
     b. A copy of a statment for payment of a lease, provided that the statement is dated within the past six months,
     c. A birth certificate,
     d. A local authority tax bill for the current year,

The presential validator must:

- Attest to the signing of the Personal Statement and the identity of the signer, and
- Identify the original Vetting Documents used to perform the identification. In addition, the validator must attest on a copy of the current signed goverrntment-issued identification document that it is a full, true, and accurate reproduction of the original.

Non-Commercial Entity *(International Org.)*	**Aspects to be verified**	1. **Legal existence.** 2. **Entity name**. 3. **Registration Number:** date of formation, or the identifier for the legislative act that created the International Organisation. In circumstances where this information is not available, ANF AC shall enter appropiate language to indicate that the Subject is an International Organisation Entity.
	Verification methods	All items listed are verified either: 1. Constitutive document under which the International Organization was formed; or 2. Directly on any current list of qualified entities that CA / Browser Forum maintains at www.cabforum.org. 3. In cases where the International Organization is an organ, an agency, or a non-governmental organization dependent on a verified International Organization, ANF AC will verify the Applicant directly with the parent International Organization.

Verification of Assumed Name
ANF AC does not allow the use of a DBA or d/b/a or "trading as".

Verification of Applicant's Physical Existence
To verify the physical existence and commercial presence of the Applicant, ANF AC verifies that the physical address provided by the Applicant is an address where the Applicant or a parent company/subsidiary conducts business operations (not, for example, a mailbox or a post office box). and is the address of the applicant's place of business. • If the place of business stated in the certificate request appears in the official source consulted for the verification of the identity of the organization, no additional checks are made. • If the registered address and the place of business are different, verify that appears listed in at least one official source other than the one used to verify the legal existence, ANF AC will confirm that the address of the Place of Business is a valid business address by reference to said official source; • In the event that the Place of Business outlined in the application can not be validated by the previous procedure, ANF AC will confirm the validity of the address provided by the applicant in the application through a visit to the business address made by a employee of ANF AC or an authorized third party. The following evidences must be obtained: a) The Applicant's business is at the exact address indicated in the Application, b) Identify the type of installation (for example, the office in a commercial building, private residence, showcase, etc.) and if it seems to be a permanent commercial location, c) Indicate if there is a permanent sign that identifies the applicant, d) Indicate if there is evidence that the Applicant is carrying out ongoing commercial activities on the site, and e) Include one or more photos of (i) the exterior of the site (with signs indicating the name of the Applicant, if present, and showing the street address if possible), and (ii) the reception area interior or the work area. • If the place of Business not in the Country of Incorporation of Registration: ANF AC shall rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

Verification of Methods of Communication

ANF AC verifies a telephone number, fax number, email address to help communicate with the Applicant and confirm that the Applicant knows and approves the issue. To verify a verified method of communication with the applicant, ANF AC:

(A) By:
- records provided by the corresponding telephone company;
- an official or independent qualified source; or
- a Verified Professional Letter; and

(B) Confirm the communication method obtaining an affirmative response from the same (for example: telephone call, email with acknowledgment of receipt).

In case of discrepancy between the documentation provided and the verification, it will be verified that the address that appears in the application corresponds to a location in which the Organization of the subject operates in a constant manner.
The email address and the SMS service associated with your mobile phone will be considered as authorized mailboxes so that ANF AC can deliver certified email, including double authentication in the case of a centralized electronic signature service, or any other that is consider necessary. The user assumes the obligation to inform ANF AC of any change of email address or mobile phone number.

Veriffication of Applicant's Operational Existence
ANF AC verifies the commercial capacity through the operative existence of the Applicant. (1) If it is a Government Entity, ANF AC is based on the verification carried out in "Verification of the Applicant's existence and identity" In other cases, through one of the following processes: (2) Verify that the Applicant has existed for at least three years, as indicated by the records of an Official Registry; (3) Verification that the applicant appears in a Source of Independently Qualified Information or in a registry of Hacienda (Tax Authority); or (4) Verification, through authenticated documentation, that the Applicant has an operating bank account in a Regulated Financial Institution;

4.2.1.3.2. Verification of Domain Name

For each Fully-Qualified Domain Name listed in a Certificate, ANF AC will verify the domain control using a procedure specified in Section 3.2.2.4 of this CP.

ANF AC will visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. Then ANF AC will perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

4.2.1.3.3. Verification of the Applicant's authorisation for the EV Certificate

Verification of Name, Title, and Authority of Contract Signer and Certificate Approver	
Name and Title	• ID card or Passport • Power of Attorney and/or Official Register ANF AC will verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business ils identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's

	jurisdiction prohibit doing business. In that case, ANF AC will not issue any EV Certificate to the Applicant.
Signing Authority of the Contract Signer	In case the Signer does not match the applicant of the certificate, it will include: • An affidavit, where it is acknowledged that the Signer is authorized to act on behalf of the applicant to request an SSL EV Certificate from ANF AC, and to use and secure the issued certificate. In this way, the faculty of the signer of the subscriber's contract is verified; or • Clause added in the subscription contract with the content established in Appendix E of the EV Guidelines.
EV Authority of the Certificate Approver	In the event that the figure of the certificate approver does not match the certificate applicant, there must be an authorization letter, outlined in section 4.1.2.2. of this CP. The letter must include the signatures of each of the authorized persons, in addition to the signature of the signatory of the contract.

Verification of Signature on Subscriber Agreement and EV Certificate Request
Both the Subscriber Agreement and each EV Certificate Request must be signed. The method to authenticate the signature of the Certificate Applicant or the Contract Signer is one of the following: 1. Physical presence of the subscriber before an ANF AC Operator, employee or authorized third party, who also signs accrediting the verification. 2. Notarization of the signature (s) inserted in the contract.

Verification of Approval of EV Certificate Request
In the event the Certificate Approver is different from the Applicant, to verify the approval of the Certificate Approver of an EV Certificate Request, ANF AC will contact the Certificate Approver using a verified communication method for the Applicant. and obtain oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request.

ANF AC verifies whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business is identified on any government denied list, list of prohibited persons OID 1.3.6.1.4.1.18332.56.3.1, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business (document with OID 1.3.6.1.4.1.18332.56.2.1). ANF AC shall not issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

ANF AC regularly updates its database with all the people that appear in the search and seizure, and links this blacklist to the certificate request control.

4.2.1.4. QWAC Verification Requirements

All verification requirements defined in section 4.2.1.4. of this Certificate Policy apply for the Qualified Website Authentication Certificate issued to legal persons. For QWAC issued to natural persons, procedures stablished in CA/B Forum Baseline Requirements shall be followed.

Additionaly, in PSD2 SSL EV Certificates, ANF AC shall verify, using authentic information of the Competent National Authority, the specific attributes of PSD2,

- authorization number,

- roles, and
- name of the Competent National Authority provided by the subject.

If the Competent National Authority provides standards for the validation of these attributes, ANF AC will apply those standards.

4.2.1.5. Electronic Headquarters Certificates Verification Requirements

Verification of the applicant identity is performed in accordance with section 3.2.2.1. and 3.2.2.2. of this CP. If the subject:countryName field is present, the country is verified in accordance with section 3.2.2.3. of this CP. Domain name control verification is performed in accordance with section 3.2.2.4. of this CP.

For the designation of electronic headquarters within an organization, clear and unambiguous criteria of the headquarters will be followed. No specific number or criterion is prescribed to determine the number of existing headquarters in a public body or ministerial department. Examples of designation of electronic headquarters would be ("Descriptive name of the electronic headquarter"):

- "Technology Transfer Center of Public Administrations"
- "General Access Point
- "Official Portal of the Ministry of the Presidency"

Verification that the landline number (not mobile) belongs to the Subject entity in:

- Telephone operators' pages, Data Protection Agencies.
- Via direct call

Verification of operational existence. Private entities must certify that they perform banking transactions with a regulated financial institution.

ANF AC performs a dual verification, intervening the Technical and Legal Departments. Also in the same cases, all validations are reviewed by the Head of the Technical Department.

If the certificate has "Extended Validation" character, verification procedures specified in section 4.2.1.4 shall be followed.

4.2.1.6. High risk Status

High Risk Certificate Request are requests that ANF AC flags for additional scrutiny by reference to internal criteria and databases maintained by ANF AC, which may include:

- Names at higher risk for phishing or other fraudulent usage,
- Names contained in previously rejected certificate requests or revoked Certificates,
- Names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or
- Names that ANF AC identifies using its own risk-mitigation criteria.

ANF AC maintains documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified.

4.2.2. Approval or rejection of certificate applications

The Issuance Reports Manager (IRM) assumes the final responsibility of verifying the information contained in the Application Form, to assess the adequacy of the documents provided and of the application, in accordance with the provisions of section 4.2.1. of this Certificate Policy.

ANF AC shall reject any certificate application that cannot be verified.

Moreover, IRM will determine:

- That the subscriber has had access to the terms and conditions relating to the use of the certificate, as well as to the issuance fees.
- That the subscriber has had access and has permanent access to all documents relating to the duties and responsibilities of the CA, the subscriber, the subject, those responsible for the certificate and relying parties, especially the CPS and Certification Policies.

Besides, he/she shall monitor compliance with any requirement imposed by the legislation on data protection, as established in the security document included in the CPS.

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

The IRM may require additional information or documentation from the subscriber (E.g. Bill of utilities, bank statement, credit card statement, tax document issued by a public administration), which will have 15 days to deliver it. After this period, without having completed the requirement, the IRM will issue a report denying the issuance. Should the subscriber meet the requirement, the IRM will have 7 days to issue the final report.

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

ANF AC verified, by itself or through its Registration Authorities or Identity Verification Offices, the request, the identity, the address, and any other circumstances of the subscribers and subjets of the certificates. The existing legal instrument between the parties shall include the necessity of compliance with the requirements stated in ETSI and CA/B Forum.

4.2.3. Time to process certificate applications

Refer to ANF AC's CPS.

4.3. Certificate issuance

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

4.3.1. CA actions during certificate issuance

Refer to ANF AC's CPS.

Prior to issuing the certificate, the issuing system proceeds to validate the certificate format using linting tools: Zlint, x509lint and certlint. Certificate issuance is held up for manual review if a linting error or warning is found. The error is flagged and brought to the attention of management to complete further internal verification and final decision on the certificate issuance.

4.3.2. Notification to subscriber by the CA of issuance of certificate

Refer to ANF AC's CPS.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Refer to ANF AC's CPS.

4.4.2. Publication of the certificate by the CA

Refer to ANF AC's CPS.

4.4.3. Notification of certificate issuance by the CA to other entities

Only in case of PSD2 certificates, if ANF AC has been notified about the e-mail address of the National Competent Authority (NCA) identified in the new certificate issuance, ANF AC will send to this e-mail address the information of the certificate content as well as contact information and instructions for revocation requests.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

Refer to section 9.6.3, provisions 2. And 4.

4.5.2. Relying party public key and certificate usage

Refer to ANF AC's CPS.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

Refer to ANF AC's CPS.

4.6.2. Who may request renewal

Refer to ANF AC's CPS.

4.6.3. Processing certificate renewal requests

The process for renewal is the same as the one for issuing a new certificate. The documentation that must be provided by the subscriber and the validation steps, issuance and delivery of certificates are the same as the issuance of a new certificate.

Two ways for renewal are considered:

- Certificate renewal with re-keying
- Certificate renewal without re-keying

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

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

4.6.4. Notification of new certificate issuance to subscriber

Refer to ANF AC's CPS.

4.6.5. Conduct constituting acceptance of a renewal certificate

Refer to ANF AC's CPS.

4.6.6. Publication of the renewal certificate by the CA

Refer to ANF AC's CPS.

4.6.7. Notification of certificate issuance by the CA to other entities

No notification is made to third parties.

4.7. Certificate re-key

Refer to ANF AC's CPS.

4.8. Certificate modification

Not applicable.

4.9. Certificate revocation and suspension

Generally, as defined in the CPS of ANF AC.

4.9.1. Circumstances for revocation

ANF AC shall revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that ANF AC revoke the Certificate;
2. The Subscriber notifies ANF AC that the original certificate request was not authorized and does not retroactively grant authorization;
3. ANF AC obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. ANF AC is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. ANF AC obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

ANF AC shall revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum Baseline Requirements;
2. ANF AC obtains evidence that the Certificate was misused;
3. ANF AC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. ANF AC is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. ANF AC is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. ANF AC is made aware of a material change in the information contained in the Certificate;
7. ANF AC is made aware that the Certificate was not issued in accordance with CA/B Forum Baseline Requirements or this Certificate Policy or ANF AC's Certification Practice Statement;
8. ANF AC determines or is made aware that any of the information appearing in the Certificate is inaccurate;

9. ANF AC 's right to issue Certificates under CA/B Forum Baseline Requirements expires or is revoked or terminated, unless ANF AC has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by ANF AC 's Certificate Policy and/or Certification Practice Statement; or
11. ANF AC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

ANF AC shall revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies ANF AC that the original certificate request was not authorized and does not retroactively grant authorization;
3. ANF AC obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B Forum Baseline Requirements;
4. ANF AC obtains evidence that the Certificate was misused;
5. ANF AC is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or ANF AC's Certification Practice Statement;
6. ANF AC determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. ANF AC or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. ANF AC's or Subordinate CA's right to issue Certificates under CA/B Forum Requirements expires or is revoked or terminated, unless the ANF AC has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by ANF AC's Certificate Policy and/or Certification Practice Statement.

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

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

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

4.9.2. Who can request revocation

Refer to ANF AC's CPS. Additionally, Subscribers, Relying Parties, Application Software Suppliers, National Competent Authorities, and other third parties may submit Certificate Problem Reports informing ANF AC of reasonable cause to revoke the certificate.

4.9.3. Procedure for revocation request

Refer to ANF AC's CPS.

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

You may file directly your suspicion or complaint at: https://www.anf.es/en/report-breach-misuse/

ANF AC has a 24x7 service to answer revocations, complaints or incidents related to the certificates. Any person that needs technical instructions or legal support in this area, can make their consultations for free by any of the following procedures.

- During office hours, on the telephone 902 902 172 (calls from Spain), International +34 933 935 946, or by means of an appointment at their premises.
- Outside office hours, by calling +34 930 502 397
- Online. The interested must fill the form published in the website: https://www.anf.es/en
- Online service: https://www.anf.es/ac/revocar-certificado-web
- Sending an e-mail to: soporte@anf.es

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

- ANF AC shall investigate incidents of which they become away within twenty-four hours of their receipt. The Security Manager, based on inquiries and verifications, shall issue a report to the Issuance Reports Manager, whom shall determine, if appropriate, the corresponding revocation substantiated in a Minute, which shall include:
  - Nature of the incident.
  - Received information.
  - Legal rules and regulation on which the revocation order is based on.

  Anyone interested may open an incident using one of the following procedures:

  - Via telephone call during office hours:
    902 902 172 (calls from Spain) (Monday to Friday from 9 hrs. to 18 hrs.) (+34) 933 935 946 (International)
  - Online. The interested must open an incident in the Webservice:
    https://www.anf.es/ac/abrir-incidencia

4.9.4. Revocation request grace period

Refer to ANF AC's CPS.

4.9.5. Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, ANF AC will investigate the facts and circumstances related to the revocation request and provide a preliminary report on its findings to both the Subscriber requesting the revocation or the entity who contacted ANF AC reporting a certificate problem.

Regarding a communication of a certificate problem, ANF AC, after reviewing the facts and circumstances, will work with the Subscriber and any entity reporting the Certificate Problem or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which ANF AC will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation shall not exceed the time frame set forth in Section 4.9.1.1

ANF AC has an Incident Registry in which it is registered every incident that has occurred with the certificates issued and the evidences obtained. These incidents are registered, analyzed and resolved per the procedures of ANF AC's Information Security Management System.

The Security Manager determines the severity of the incident and names a responsible and, in case of significant security incidents, reports to the PKI Governing Board. In cases of fraud or phishing, the information is reported to the Anti-Phishing Working Group site,

https://apwg.org/

4.9.6. Revocation checking requirement for relying parties

Refer to ANF AC's CPS.

4.9.7. CRL issuance frequency

Refer to ANF AC's CPS.

4.9.8. Maximum latency for CRLs

Refer to ANF AC's CPS.

4.9.9. On-line revocation/status checking availability

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

4.9.10. On-line revocation checking requirements

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

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

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

Access to this system is free.

4.9.11. Other forms of revocation advertisements available

No stipulation.

4.9.12. Special requirements re key compromise

Refer to section 4.9.1.

4.9.13. Circumstances for suspension

Not applicable. Suspension is not allowed.

4.10. Certificate status services

Refer to ANF AC's CPS.

4.11. End of subscription

Refer to ANF AC's CPS.

4.12. Key escrow and recovery

Refer to ANF AC's CPS.

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

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

Refer to ANF AC's CPS.

5.2. Procedural controls

Refer to ANF AC's CPS.

5.3. Personnel controls

Refer to ANF AC's CPS.

5.4. Audit logging procedures

Refer to ANF AC's CPS.

5.5. Records archival

Refer to ANF AC's CPS.

5.6. Key changeover

Refer to ANF AC's CPS.

5.7. Compromise and disaster recovery

Refer to ANF AC's CPS.

5.8. CA or RA termination

Refer to ANF AC's CPS.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

Refer to ANF AC's CPS.

6.1.2. Private Key Delivery to Subscriber

As established in the CPS of ANF AC, ANF AC provides its users with the necessary cryptographic devices/software to generate, in private and without third party intervention, their key pair and their activation data. This ensures compliance with the parameters established in BR sections 6.1.5 and 6.1.6. It is the subscriber himself who is generated and is in possession of the private key.

ANF AC does NOT generate the key pairs for end-entity certificates that have an EKU extension containing the KeyPurposeIds id-kp-serverAuth or anyExtendedKeyUsage.

If ANF AC or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, ANF AC shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Refer to ANF AC's CPS.

6.3. Other aspects of key pair management

Refer to ANF AC's CPS.

6.4. Activation data

Refer to ANF AC's CPS.

6.5. Computer security controls

Refer to ANF AC's CPS.

6.6. Life cycle technical controls

Refer to ANF AC's CPS.

6.7. Network security controls

Refer to ANF AC's CPS.

6.8. Time-stamping

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

7. CERTIFICATE, CRL, AND OCSP PROFILES

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

7.1. Certificate profile

7.1.1. Version number(s)

x.509 v3.

7.1.2. Certificate Content and Extensions; Application of RFC 5280

ANF AC uses certificate extensions in accordance with applicable industry standards, including RFC 3280/5280.

Technically Constrained Subordinate CA Certificates shall include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId shall not appear in the EKU extension of publicly trusted certificates.

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

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

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

Extension	Critical	Value
basicConstraints	-	Optional. cA field is not set true
keyUsage	-	Optional. Bit positions for keyCertSign and cRLSign are NOT set.
certificatePolicies	NO	certificatePolicies:policyIdentifier A Policy identifier, defined by ANF AC that indicates a Certificate Policy asserting ANF AC's adherence to and compliance with the applicable requirements.
extendedKeyUsage	NO	id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values are NOT present.
cRLDistributionPoints	NO	HTTP URL of ANF AC's CRL service
authorityInformationAccess	NO	HTTP URL of the issuing CA's OCPS responder (accessMethod=1.3.6.1.5.5.7.48.1)
authorityKeyIdentifier	NO	keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.

ANF AC will NOT issue a certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified above unless is aware of a reason for including the data in the Certificate.

Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network) will not be included, unless:

i. such value falls within an OID arc for which the Applicant demonstrates ownership, or ii.
ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or

Semantics that, if included, will mislead a Relying Party about the certificate information verified by ANF AC will not be included (such as including extendedKeyUsage value for a smart card, where ANF AC is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.1. Propriertary Fields

Internationally unambiguous identifiers have been assigned. Specifically:

- Fields referenced with OID 1.3.6.1.4.1.18332.x.x are proprietary extensions of ANF AC. The complete list of OID codes and the information associated to the same may be consulted in the section "Proprietary fields of ANF AC" of the Certification Practice Statement of ANF AC.
- Fields with ISO/IANA of MPR 2.16.724.1.3.5.x.x, are proprietary extensions required and identified in the Identification and Electronic Signature Scheme v.1.7.6 published by the High Council of Electronic Administration.
- Fields with OID 1.3.6.1.4.1.18838.1.1 are proprietary of the Spanish State Tax Administration Agency (Agencia Estatal de Administración Tributaria “AEAT”).

7.1.2.2. QcStatements

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

- **QcCompliance**, refers to a declaration of the issuer in which it states the qualification with which the certificate is issued, and the legal framework to which it is submitted. Specifically, the certificates submitted to this policy, issued as qualified, outline:
  “This certificate is issued with the qualification of qualified in accordance with Annex I of Regulation (EU) 910/2014 of the European Parliament "

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

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

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

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

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

- **QcPDS**, The URL that allows access to all the ANF AC PKI policies is provided (PDS Policy Disclosure Statements)

- **PSD2QcType**

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

  a) The function of the Payment Service Provider (PSP), which may be one or more of the following:
     i. account service (PSP_AS);
     ii. initiation of payment (PSP_PI);
     iii. account information (PSP_AI);
     iv. issuance of card-based payment instruments (PSP_IC).
  b) Name of the Competent National Authority where the PSP is registered. This information is provided in two forms: the full name string (NCAName) in English and an abbreviated unique identifier (NCAId).

7.1.3. Algorithm object identifiers

Refer to ANF AC's CPS.

7.1.4. Name forms

Subject attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. Common Name certificate field is not included.

Subject information on subscriber certificates follows requirements specified in section 7.1.4.2 of the Baseline Requirements.

EV Certificates will include the information about the Subject organization in the fields listed in section 9.2 of EV Guidelines.

7.1.4.1. Subject Alternative Name Extension

This extension contains at least one entry of a dNSName containing the Fully-Qualified Domain Name. Wildcard FQDNs are permitted.

Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280. Underscore characters in dNSNAme entries are not accepted.

7.1.5. Name constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate MUST include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId MUST NOT appear within this extension.

7.1.6. Certificate policy object identifier

When ANF AC issues a Certificate containing one of the policy identifiers set forth in Section 1.2, it asserts that the Certificate is managed in accordance with the policy that is identified herein.

7.1.7. Usage of Policy Constraints extension

Refer to ANF AC's CPS.

7.1.8. Policy qualifiers syntax and semantics

Refer to ANF AC's CPS.

7.1.9. Processing semantics for the critical Certificate Policies extension

Refer to ANF AC's CPS.

7.2. CRL profile

Refer to ANF AC's CPS.

7.3. OCSP profile

Refer to ANF AC's CPS.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

Refer to ANF AC's CPS.

8.2. Identity/qualifications of assessor

Refer to ANF AC's CPS.

8.3. Assessor's relationship to assessed entity

Refer to ANF AC's CPS.

8.4. Topics covered by assessment

Refer to ANF AC's CPS.

8.5. Actions taken as a result of deficiency

Refer to ANF AC's CPS.

8.6. Communication of results

Refer to ANF AC's CPS.

8.7. Self-Audits

Refer to ANF AC's CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Refer to ANF AC's CPS.

9.2. Financial responsibility

Refer to ANF AC's CPS.

9.3. Confidentiality of business information

Refer to ANF AC's CPS.

9.4. Privacy of personal information

Refer to ANF AC's CPS.

9.5. Intellectual property rights

Refer to ANF AC's CPS.

9.6. Representations and warranties

When ANF AC issues an EV Certificate, ANF AC represent and warrant to the Certificate Beneficiaries listed in Section 9.6.1, during the period when the EV Certificate is Valid, that ANF AC has followed the requirements of CA/B Forum EV Guidelines, ANF AC's CPS and this CP, in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate. The EV Certificate Warranties include the ones specified in section 7.1. of the EV Guidelines.

EV Certificate Applicants make the commitments and warranties set forth in Section 9.6.3 of ANF AC's CPS for the benefit of the CA and Certificate Beneficiaries.

9.7. Disclaimers of warranties

Refer to ANF AC's CPS.

9.8. Limitations of liability

Refer to ANF AC's CPS.

9.9. Indemnities

Refer to ANF AC's CPS.

9.10. Term and termination

Refer to ANF AC's CPS.

9.11. Individual notices and communications with participants

Refer to ANF AC's CPS.

9.12. Amendments

Refer to ANF AC's CPS.

9.13. Dispute resolution provisions

Refer to ANF AC's CPS.

9.14. Governing law

Refer to ANF AC's CPS.

9.15. Compliance with applicable law

Refer to ANF AC's CPS.

9.16. Miscellaneous provisions

Refer to ANF AC's CPS.

9.17. Other provisions

No stipulation.