Certificate Policy for Secure Server SSL, Extended Validation Secure Server SSL (EV SSL), Electronic Headquarters and Extended Validation Electronic Headquarters Certificates

B2 Industry Street, Qormi, QRM 3000 Malta
Telephone: (+356) 2299 3100
Fax:(+356) 2299 3101
Web: www.anfacmalta.com

Security Level

Public Document

Important Notice

Address: B2, Industry Street, Qormi, QRM 3000 (Malta)

Telephone: (+356) 2299 3100

Fax: (+356) 2299 3101. Web: www.anfacmalta.com

Index

1 Introduction

ANF AC Malta, Ltd. (hereinafter, ANF AC) is a corporate entity, duly registered with the Maltese Registry of Companies, with registration number C75870 and VAT number MT 23399415.

The Public Key Infrastructure (PKI) of ANF AC has been designed and is managed in accordance with the legal framework of the European Parliament [UE] 910/2014 Regulation, and with the Maltese Chapter 426 Electronic Commerce Act. The PKI of ANF AC complies with the ETSI EN 319 411-1 (Part 1: General Requirements), ETSI EN 319 411-2 (Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates), ETSI EN 319 411-3 (Part 3: Policy Requirements for Certification Authorities issuing public key certificates), ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI) and RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificate Profile) standards.

ANF AC uses OIDs in accordance with the ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs) standards. ANF AC has been assigned the SMI Network Management Private Enterprise Code 18339 by the international organization IANA - Internet Assigned Numbers Authority - under the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).

This document is the Certification Policy (CP) corresponding to the certificates issued by ANF AC, of the type "Secure Server SSL ", "Extended Validation Secure Server SSL (EV SSL)" "Medium and High Level Electronic Headquarters" and "Medium and High Level Extended Validation Electronic Headquarters". These certificates are issued with the consideration of qualified in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

To develop its content the IETF RFC 3647 PKIX structure has been followed, including those sections that are specific to this type of certificate.

This document defines the operational and procedural requirements to which the usage of these certificates is subjected, and defines the guidelines that ANF AC uses for its issuance, management, revocation, renewal and any other process that affects the life cycle. The roles, responsibilities and relationships between the end user, ANF AC and trusted third parties are described, as well as the application, renewal and revocation rules that must be met.

The legal and regulatory framework in which the issuance of these certificates is based is:

- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates

- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-4 (Certificate profile for web site certificates) Electronic Headquarters certificate profile defined by the Ministry of Finance and Public Administrations
- 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 (hereinafter eIDAS).

In the scope of the Google Certificate Transparency project (CT), the certificates issued with the EV (Extended Validation) qualification will be published in different CT Log operators, to comply with the policy defined by Google.

This document is only one of the several documents governing the PKI of ANF AC, it details and complements what is defined in the Certification Practice Statement and its addendum. ANF AC oversees and supervises that this CP is compatible and consistent with the other documents produced. All documentation is freely available to users and relying parties at https://www.anfacmalta.com.

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

1.1 Description of certificates

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

- **Secure Server SSL**

The purpose of this certificate is to establish data communications through TLS / SSL protocols in services and applications, especially for:

- The identification of the organization holding the domain (DNS), providing a reasonable assurance to the user of a web browser that the website being accessed is owned by the organization identified in the certificate through its name and address.

- Encryption of communications between the user and the website, facilitating the exchange of encryption keys necessary for encryption of information through Internet.
  The maximum validity of these certificates is 5 years.

This type of certificates can be issued in the following modes:

- **DV and DV Wildcard**

This certificate, with the consideration of unqualified per eIDAS, 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. The DV Wildcard contains a "wild card" in the hostname (e.g.: *.frater.com). They are issued in accordance with ETSI EN 319 411-1.
The validity of these certificates can be up to 3 years.

- **OV and OV Wildcard**

This certificate, with the consideration of unqualified per eIDAS 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 per the policy OVCP of ETSI EN 319 411-1. The validity of these certificates can be up to 3 years.

- **Extended Validation Secure Server SSL (EV SSL)**

This certificate, with consideration of unqualified 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. They are issued per the policy EV of ETSI EN 319 411-1. The validity of these certificates can be up to 2 years.

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. Furthermore, this type of certificates need to be stored in SSCD devices (HSM).

ANF AC complies with what is stated in the CA/Browser Forum guidelines published in their website https://www.cabforum.org, including the acceptance of the audit programs specified therein.

- **Electronic Headquarters**

ANF AC issues certificates of the electronic headquarters type, per the ETSI EN 319 411-2 standard and the profile of the office certificate defined by the Ministry of Finance and Public Administrations. This is a certificate, with the consideration of qualified per eIDAS, in which the Public Administration, administrative body or entity owner of the office is identified.

The validity of these certificates is 2 years.

The purpose of this certificate is to establish data communications through TLS/SSL in services and applications.

- **Extended Validation Electronic Headquarters**

In addition to the utilities provided by the Electronic Headquarters certificate, the Extended Validation (EV) aims to provide a higher level of authentication for Public Administration, administrative body, or entity to secure transactions on their websites, avoiding phishing or any other online identity fraud cases. Furthermore, this type of certificates need to be stored in SSCD devices (HSM).

ANF AC complies with what is stated in the CA/Browser Forum guidelines published in their website https://www.cabforum.org, including the acceptance of the audit programs specified therein.

The validity of these certificates is 2 years.

1.2 Identification

Document name	Certification Policy for Secure Server SSL, Extended Validation Secure Server SSL (EV SSL), Electronic Headquarters and Extended Validation Electronic Headquarters Certificates
Version	1.0
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.55.1.1
Publication date	November 15th, 2016
Expiration date	Not applicable
Related CPS	Certification Practice Statement (CPS) of ANF AC
Location	https://www.anfacmalta.com

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

Certificate	OID
Secure Server SSL DV With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.1.22
Secure Server SSL OV With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.7.22

Secure Server SSL EV With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.2.22
Medium Level Electronic Headquarters With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.3.22
Medium Level EV Electronic Headquarters With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.5.22
High Level Electronic Headquarters With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.4.22
High Level EV Electronic Headquarters With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.55.1.1.6.22

When the certificate is of the type "Secure Server SSL", in the extension CertificatePolicies (2.5.29.32), it will include at least one of the following PolicyInformation:

- If only domain validation is performed (Compliant with Baseline Requirements – No entity identity asserted) [CA/B FORUM - SSL DV]:
    - 2.23.140.1.2.1

- If the subscriber is a legal person, organization or institution (Compliant with Baseline Requirements – Organization identity asserted) [CA/B FORUM - SSL OV]:
    - 2.23.140.1.2.2

- If the subscriber is a natural person (Compliant with Baseline Requirements – Individual identity asserted):
    - 2.23.140.1.2.3

In the case of certificates of "High Level Electronic Headquarters", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.5.1

In the case of "Medium Level Electronic Headquarters", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.5.2

All certificates meet the ETSI TS 102 042 and ETSI 101 456 standard requirements, in relation to the identified certificate policies:

0.4.0.2042.1.1	Advanced Certificate Policy (Individual or Professional) [1]
0.4.0.2042.1.2	Advanced Certificate Policy (Individual or Professional) issued on cryptographic device [2]
0.4.0.2042.1.7	TLS/SSL Certificate Policy with Organization validation [3]
0.4.0.2042.1.6	TLS/SSL Certificate Policy with Domain validation [4]
0.4.0.1456.1.1	Qualified Certificate Policy [5]

[1] *Normalized Certification Policy (NCP) in accordance with ETSI TS 102 042 standard*

[2] *Extended Normalized Certification Policy (NCP+) in accordance with ETSI TS 102 042 standard*

[3] *Organization validation certificates policy (OVCP) in accordance with ETSI TS 102 042 standard*

[4] *Domain validation certificates policy (DVCP) in accordance with ETSI 102 042 standard*

[5] *Referred to QCP+SSCD (Qualified Certificate Policy + Secure Signature Creation Device) in accordance with standard ETSI TS 101 456*

Moreover, in the case of including the extension "Extended Validation", the extension CertificatePolicies (2.5.29.32) will include the OID of EV SSL [ETSI TS 102 042 - EVCP]:

- 0.4.0.2042.1.4

Moreover, per [CA/B FORUM – EV SSL] will include the OID of EV SSL

- 2.23.140.1.1

And, when the certificate is issued with the consideration of website qualified per eIDAS, complies the requirements of the QCPW policy of ETSI EN 319 411-2, and the eIDAS annex IV. In the extension CertificatePolicies (2.5.29.32), it will include at least one of the following PolicyInformation:

- qcp-web (0.4.0.194112.1.4)

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

1.3 Storage types

These certificates can be issued in two storage types:

- Cryptographic software token.

- Cryptographic token (HSM). Devices exclusively certified specifically in accordance with the applicable requirements established in Article 30.3 of the eIDAS Regulation and, therefore, included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

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

This policy, regarding Electronic Headquarters certificates, follows the definitions of the present policy, regarding Public Employee certificates follows the definitions established by the Information and Communications Technologies Directorate.

Two different levels of assurance are defined:

a. Medium level:

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

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

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

Minimum acceptable security mechanisms include X.509 software certificates. In the case of certificates issued to natural persons, they correspond to a "qualified certificate" as defined in Regulation (EU) 910/2014 for qualified electronic signature without a qualified signature creation device. In the case of certificates issued to legal persons, it corresponds to a "qualified seal certificate", as defined in the Regulation (EU) 910/2014 for qualified electronic seal without a qualified seal creation device. The use of signature hardware devices (HSM or qualified signature creation device) is also permitted.

The maximum validity of these certificates is 5 years, except for certificates issued with Extended Validation, which maximum validity period is 27 months.

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

**1 The IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens) program. Decision 2004/387/EC of the European Parliament and of the Council of*

21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004].

b. High level:

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

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

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

Acceptable security mechanisms include X.509 certificates in hardware. In the case of certificates issued to natural persons, they correspond to a "qualified certificate", for "qualified electronic signature", as defined in the Regulation (EU) 910/2014. In the case of certificates issued to legal persons, it corresponds with the "qualified seal", as defined in the Regulation (EU) 910/2014. Furthermore, this type of certificates need to be stored in SSCD devices (HSM).

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

The maximum validity of these certificates is 5 years, except for certificates issued with Extended Validation, which maximum validity period is 27 months.

1.4 Parties of the PKI

1.4.1 Certification Authorities

As defined in the CPS of ANF AC.

1.4.2 Registration Authorities

As defined in the CPS of ANF AC.

1.4.2.1 Recognized Registration Authority

As defined in the CPS of ANF AC.

1.4.2.2 Collaborating Registration Authority

As defined in the CPS of ANF AC.

1.4.3 Issuance Reports Manager

As defined in the CPS of ANF AC.

1.4.4 End entities

1.4.4.1 Subscriber

As defined in the CPS of ANF AC.

1.4.4.2 Subject

As defined in the CPS of ANF AC.

1.4.4.3 Certificate responsible

As defined in the CPS of ANF AC.

1.4.4.4 Relying parties

As defined in the CPS of ANF AC.

1.5 Scope of application

1.5.1 Allowed usage

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.

1.5.2 Limits of certificate usage

As defined in the CPS of ANF AC.

1.5.3 Prohibited usage

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

1.6 Certification entity contact details

As defined in the CPS of ANF AC.

1.7 Definitions and acronyms

As defined in the CPS of ANF AC.

2 Information Publication and Repositories

2.1 Repositories

As defined in the CPS of ANF AC.

2.2 Information publication

As defined in the CPS of ANF AC.

2.3 Frequency of updates

As defined in the CPS of ANF AC.

2.4 Access controls to repositories

As defined in the CPS of ANF AC.

3 Identification and Authentication

3.1 Name registration

3.1.1 Types of names

All certificates require a Distinguished Name (DN) under the X.500 standard.

Personal circumstances and attributes of the persons and organizations identified in the certificates are included in attributes predefined in standards and generally recognized technical specifications.

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, including a Common Name component.

The CN (Common Name) attribute of the DN must refer to the DNS domain name.

3.1.3 Anonymous or pseudonyms

Not permitted

3.1.3.1 Rules for interpreting various name formats

In any case, attention shall be paid to the X.500 standard, referred in the ISO/IEC 9594 standard.

3.1.4 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.

3.1.5 Resolution of conflicts in relation to names and trademarks.

Subscribers for certificates shall not include names in applications that may involve breach, by the subscriber, of third party trademarks.

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

ANF AC shall verify if the requested domain name may be misleading to another existing name in the network, and if this is the case, will determine by its sole discretion whether to issue or refuse the issuance of the requested certificate.

3.2 Initial identity validation

3.2.1 Proof of possession of private key

As defined in the CPS of ANF AC.

3.2.2 Authentication of the subscriber, certificate responsible and subject

Certificates issued under this Certification Policy will identify the subject under whose name a DNS domain has been registered. They will also identify the certificate subscriber and, where applicable, the certificate holder (if named by the subscriber).

ANF AC verified, by itself or through its Registration Authorities, the identity and any other circumstances of the subscribers and subjects of the certificates. The existing legal instrument between the parties shall include the necessity of compliance with the requirements stated in ETSI and CABForum.

The Issuance Reports Manager will use appropriate means to ensure the accuracy of the information contained in the certificate. These means include external registry databases and the possibility to require complementary information or documents to the subscriber.

The tax identification of the subscriber, the subject and the responsible of the certificate shall be incorporated into the certificate. Furthermore, the subscriber must provide a mobile phone number and an email address of his trust. The email address and the SMS or WhatsApp service associated with their mobile phone shall be considered as authorized mailboxes for ANF AC to be able to deliver certified electronic mail, including double authentication in the case of a centralized electronic signature service, or any other as deemed necessary. The user assumes the obligation to inform ANF AC of any change of e-mail address or mobile phone number.

The types of documentation, processing modalities, authentication and validation procedures are specified in the following sections.

3.3 Re-key requests

In the event of re-keying, ANF AC shall previously inform the subscriber about any changes that may have occurred in the terms and conditions in relation to the previous issuance.

A new certificate may be issued maintaining the previous public key, if it is considered cryptographically secure.

3.4 Revocation requests

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

4 Operational Requirements

4.1 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.

The subscriber must duly fill out the Certificate Application Form, which may be authenticated through:

- Handwritten signature
- Recognized electronic signature

In the form, it shall be stated that the subscriber assumes the responsibility of the accuracy of the information outlined. The subscriber will be able to submit it to ANF AC using any of the following means:

a) **In person**: the subscriber may appear before a Recognized Registration Authority, in whose presence will proceed to sign the application form, which shall be dully fill out.

b) **By mail**: certificate request form handwritten signed by the subscriber and his/her signature legitimized by public notary. Documentation sent by ordinary mail.

4.2 Processing procedure

4.2.1 Identity authentication

4.2.1.1 Subscriber

Except for DV Secure Server SSL certificates, the subscriber must prove his/her identity and validity of the Subject entity:

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

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

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

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

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

- National / Foreign Citizens ID Card or passport with photograph that allows to verify 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).

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

II. To non-EU citizens:

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

In case of acting on behalf of a third party, the following will be required:

- Sufficient Powers 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.

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

1. If the appropriate forms have been duly filled, and the signature of the subscriber's legal representative (or of subscriber in case of a natural person) and of the responsible of the certificate has been legitimized before a notary, and certified copies of the identity, authorization and legal representation documents have been attached. For public entities, the presence of the notary may be replaced by the one of a public officer with notary powers, in accordance to the applicable legislation.

2. Online

   The https://www.anfacmalta.com website includes an application form that should be filled and electronically sign with a qualified certificate. The certificate used must have been issued by a CA approved by ANF AC.

4.2.1.2 Subject

4.2.1.2.1 Legal persons

Except for DV Secure Server SSL certificates, it is required:

- Tax identification (VAT number) of the entity.

Per the legal form:

- Corporations or other legal persons which registration is mandatory in the Registry of Companies, shall prove their valid incorporation by providing:
  - For applications of OV SSL certificates, a certificate from the Registry of Companies in relation to the incorporation data and current management of the entity.
  - For applications of EV SSL certificates, original or certified copy of the Registry of Companies 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.

4.2.1.2.2 Natural persons

In case of natural persons, the same procedure as the one outlined in the preceding section shall be followed.

In accordance with the rules of CAB FORUM, no Extended Validation (EV) certificates shall be issued to individuals.

4.2.1.3 Certificate Responsible

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.

The certificate responsible must appear before the Registration Authority and present proof of identity, and valid original or certified copy of the following documents:

a) Physical address and other contact details. If deemed necessary by the Registration Authority or the Issuance Reports Manager, additional documents may be included 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 should personally issue and sign a Declaration of Identity *[1].

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

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

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

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

- National/Foreign Citizens ID Card or passport with photograph that allows to verify 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).

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

II. To non-EU citizens:

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

***[1]** *Declaration of Identity*

It consists of a formal declaration under oath, in which the declarant states he/she personally and directly knows a natural person or a legal entity. Besides, it states, up to their direct knowledge, that he has verified the filiation data outlined in the Application Form are true: the address, telephone and e-mail.

The Declaration of Identity incorporates the identity of the declarant, his ID card number, the data verified, the date and time of verification, the signature of the declarant and the appropriate legal warnings in case of perjury.

In case of intervention of a public notary, the authentication of the signature of the subscriber shall be required in order to issue a certificate.

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 this Certification Policy.

It will verify the existence of the subscriber, the subject, the existence of the domain and its ownership by the subscriber. Depending on the type of certificate:

Type of certificate	Procedure
DV OV EV Electronic Headquarters	• The registrant must match the subject organization. Otherwise, the subscriber must prove the right of use by the subject. Verification that the subscriber has the right to use the domain or subdomain: • Domains .com.mt: www.nic.com.mt • Domains .eu: www.eurid.eu • Domains .eus: whois.nic.eus • Remainder domains: whois.icann.org • Verification of the CAA in case they are registered and in any case following the guidelines of the RFC 6844. 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.

DV OV EV Electronic Headquarters	• Verification of the identity and validity of the subject entity • Verification of the subscriber's competence to use the name of the entity • Verification via email that the subscriber is aware of the processing of the certificate. • Verification of the mailing address in: • Data Protection Agencies • Telephone operators` pages • Registry of Companies In case of discrepancy between the documentation provided and the verification, the IRM will verify that the address stated on the request corresponds to a location in which the Subject organization operates steadily. ➢ Country verification in: • Data Protection Agency • Yellow Pages • Registry of Companies ➢ Verification of the denied list in ANF AC internal data bases ➢ Verification of high risk requests in McAfee TrustedSource
Electronic Headquarters EV	➢ 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.

Moreover, he/she will determine:

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

- That the subscriber has had access and has permanent access to all documents relating to the duties and responsibilities of the CA, the subscriber, 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, 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 1.3.6.1.4.1.18339.56.2.1.

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

4.2.2.1 SSL Certificates

The IRM shall verify the documentation given by the subscriber and the Registration Authority, and will check, in accordance with the CAB Forum standards, that the subscriber is not a natural person.

Furthermore, since in certain countries, such as the United States, legal persons register their corporate name in the state where they are incorporated, but not in other states, this may lead to the issuance of two SSL certificates to legally incorporated companies in different states. That is why, for the issuance of certificates to legal persons incorporated in these countries, it shall be included in addition to the corporate name of the organization, the state in which it was incorporated. In those cases of names of organizations of special relevance and public knowledge, ANF AC shall only issue certificates with the corporate name of the legal person, to the holding of special public recognition.

4.2.2.2 Electronic headquarters Certificates

The IRM shall verify the norm that created the Electronic headquarters and its holder.

4.2.2.3 SSL EV and Electronic EV Certificates

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

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

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

- Consultation of official public registries in which the entity must be registered to check existence, valid management positions and other legal aspects such as activity and date of incorporation.

- National or regional Official Gazettes of public bodies to which public bodies or companies belong to.

- Regarding internet addresses and domains, ANF AC shall consult only registrars assigned by ICANN / IANA the domain names and addresses associated to the certificate. In this query, it shall be verified:

    - That the holder (registrant) matches the subject.
    - Persons and contact information associated to that domain registry.

- One of the contact persons listed in the who is query shall be reached to verify compliance of the certificate issuance request associated with that domain.

- Verification of the subscriber, subject and certificate responsible contact details:

    - Telephone:
        - Subscriber: a landline (not mobile) shall be used. This shall be verified in yellow pages and by personal call.
        - Subject and certificate responsible: through personal call.

    - Mailing Address: it shall be verified in Yellow Pages, AEPD or Informa service.

    - E-mail: it shall be verified by sending an e-mail requesting confirmation of receipt.

- It is verified that the subscriber is not registered in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18339.56.3.1, or is operating in a place where the CA policies forbids the certificate issuance (document with OID 1.3.6.1.4.1.18339.56.2.1).

- It is verified that the domain is not included as risky in the Anti Phishing Workgroup website http://www.antiphishing.org/ or similar ones.

- It is verified that none of the natural persons associated with the request is listed as a criminal in public records.

ANF AC regularly updates its database with all persons appearing on search and seizure, and links this blacklist to the certificate request control.

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. If not, the IRM shall solicit clarification to the subscriber and if he/she possess supporting authorization.

  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.).

In cases where validation cannot be performed on the terms and sources defined above, this shall be justified in the verification minute issued by the IRM, and the alternative source used shall be included.

4.2.3 Time to process certificate issuance

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

4.3 Certificate issuance

As defined in the CPS of ANF AC.

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

4.3.1 Certification Entity's actions during the certificate issuance process

As defined in the CPS of ANF AC.

ANF AC will deliver the certificate, by signed electronic mail, to the Technical Responsible that is stated in the Issuance Application Form.

4.3.2 Notification to subscriber

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

4.4 Certificate acceptance

4.4.1 Acceptance

After the delivery of the certificate, the subscriber has a seven-calendar day period to verify the certificate, determine if it adequate, and if the data is consistent to the required information. The subscriber has a period of 15 days to sign the Certificate Reception and Acceptance Minute.

By signing the Certificate Reception and Acceptance Minute the subscriber confirms receipt of the certificate, acceptance to the issuance made, the correct functionality of the product, its ability to use it by signing the minute with the certificate; ratifies its submission to the CPS and Policies of ANF AC, to use it in accordance with the use limitations and within the purpose for which it was issued, the responsibility to maintain the confidentiality of the private key, and the commitment to cease its use after the loss of validity, either by expiration or revocation.

4.4.2 Return of certificates

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

In case of malfunction, or due to technical errors in the data contained in the certificate, the subscriber or the certificate responsible can send an electronically signed e-mail to ANF AC, reporting the reason for the return. ANF AC shall verify the causes for return, revoke the certificate issued and issue a new certificate within 72 hours.

4.4.3 Monitoring

ANF AC is not responsible for monitoring, investigating or confirming the accuracy of the information contained in the certificate after its issuance. In case of receiving information regarding the inaccuracy or the current non-applicability of the information contained in the certificate, it can be revoked.

4.4.4 Certificate publication

The certificate is published in the repositories of ANF AC within a maximum period of 24 hours since its emission has occurred.

4.4.5 Notification of certificate issuance to third parties

No notification is made to third parties.

4.5 Rejection

As defined in the CPS of ANF AC.

4.6 Renewal of certificates

Generally, as defined in the CPS of ANF AC.

4.6.1 Valid Certificates

ANF AC notifies the subscriber the expiration of the certificate expiration via email, forwarding the application form to proceed with its renovation. These notifications are sent 90, 30 and 15 days prior to the expiration date of the certificate.

Only valid certificates can be renewed, provided that the identification made has not exceeded the period of five years.

4.6.2 Persons authorized to request the renewal

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

4.6.3 Identification and authentication of the routine renewal applications

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:

4.6.3.1 Certificate renewal with rekeying

As defined in the CPS of ANF AC.

4.6.3.2 Certificate renewal without rekeying

As defined in the CPS of ANF AC.

4.6.4 Approval or rejection of applications for renewal

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

4.6.5 Notification of certificate renewal

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

4.6.6 Acceptance of the certificate renewal

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

4.6.7 Publication of the renewal certificate

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

4.6.8 Notification of certificate renewal

Same procedure as that specified in the section 4.4.5 "Notification of certificate issuance to third parties".

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

The renewal of expired or revoked certificates is not authorized.

4.7 Certificate modification

Not applicable.

4.8 Revocation and suspension of certificates

Generally, as defined in the CPS of ANF AC.

4.8.1 Causes of revocation

Besides those defined in the CPS, ANF AC shall:

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

  The instructions are published and permanently updated in:
  http://www.anfacmalta.com

  Any person that needs technical instructions or legal support in this area, can make their consultations for free by any of the following procedures:

  - Via telephone call during office hours:
    (+356) 2299 3100 (Monday to Friday from 9 hrs. to 18 hrs.)

  - Online. The interested must fill the form published in the website:
    https://www.anfacmalta.com

  - Sending an e-mail to: support@anfacmalta.com

- 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:
  (+356) 2299 3100 (Monday to Friday from 9 hrs. to 18 hrs.)

- Email: support@anfacmalta.com

4.8.2 Identification and authentication of revocation applications

The revocation of a certificate may be requested by:

- The subscriber of a certificate.
- The Certificate Responsible.
- The Recognized Registration Authority.

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

- Electronically: by the subscriber or certificate responsible electronically signing the revocation request on the date of the revocation request.
- By telephone: by replying to the questions asked from the telephone support service available at the number (+356) 2299 3100 (International).
- In person: the subscriber or the legal representative of the certificate holder appearing before any of ANF AC's offices published in the web address https://www.anfacmalta.com, proving their identity through original documentation, and manually signing the appropriate form.

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

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

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

4.8.3 Procedure for revocation request

The subscriber of a revocation must fill the Certificate Revocation Application Form and process it before ANF AC by any of the means provided herein. In case the revocation is made by e-mail, it shall be sent to the following address: info@anfacmalta.com.

The revocation application shall contain at least the following information:

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

The revocation application shall be processed upon receipt.

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

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

4.8.4 Revocation request grace period

As defined in the CPS of ANF AC.

4.8.5 Maximum processing time of the revocation request

As defined in the CPS of ANF AC.

4.8.6 CRL lists verification requirements

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

4.8.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.8.8 On-line verification availability of the revocation

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

4.8.9 On-line verification requirements of the revocation

Relying parties may verify online the revocation of a certificate in the website https://www.anfacmalta.com.

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.

4.8.10 Certificate suspension

Not applicable.

4.8.11 Suspension requests identification and authentication

Certificate suspension is not allowed.

4.9 Key storage and recovery

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

4.10 Good practices

a) Private keys stored in PKCS#12 files.

   It is known that some CAs generate the key pair for their subscribers and then deliver the validated SSL certificate in a PKCS #12 file. This is considered as an unsafe practice and, as outlined in this CP ANF AC, this entity issuer of certificates does not generate the keys for the

subscribers, as they are the ones generating their own key pair, in any of the software or hardware forms. In any case, ANF AC does not have access to the private key of its users.

b) Validated domains.

ANF AC has as a good practice to validate the domains of legal or natural persons requesting a SSL or an Electronic headquarters certificate in any of their modes, so that the certificate data are valid and updated.

c) Long life cycle of validated certificates.

Although the term of end-entity certificates issued by ANF AC generally does not exceeds two years, it is possible that the owner requests an automatic renewal, therefore, the life cycle of the certificate is of long duration.

However, there is the possibility that a person has bought a domain, which until a certain date was owned by someone else. If the previous owner had a DV SSL certificate that is still valid, it is possible that the previous owner, with his valid certificate and DNS spoofing, can provide secure access to a malicious site.

To avoid this scenario, ANF AC verifies that the data included in the certificate is valid and updated at time intervals of 24 months.

d) Wildcard domains.

Some entities that issue DV certificates issue certificates that can function as wildcards, for example, a certificate for *. example.com where the CA verifies only the ownership and control of the example.com domain.

This enables a subscriber to establish a malicious website with SSL protection, which objective is to mimic legitimate sites, for example, paypal.example.com, and all without the knowledge of the CA. ANF AC has as a good practice to NOT issue certificates that can be used as wildcard domains.

e) Prefixes of e-mail address of Domain Validated Certificates.

ANF AC limits the set of verification addresses by email to the following:

- admin @ domain

- administrator @ domain
- webmaster @ domain
- hostmaster @ domain
- postmaster @ domain

As well as any other address appearing in the technical contact field or registry administrative of the whois domain, regardless of the domains of the addresses.

No case-sensitive discriminations are imposed to subscribers in relation to the previous list.

f) Delegation of e-mail validation to third parties

ANF AC directly validates the identification of e-mail addresses registered in the whois, avoiding the delegation of identification to third parties.

g) End-entity issuance from the root

ANF AC issues SSL certificates from a subordinate authority which does not compromise the private key of the root, delegating the issuance to a subordinate CA.

h) Allow external entities to operate with subordinate CAs

Subordinate CA certificates issued by ANF AC, are managed directly and exclusively by ANF AC, which in no case allows its operation to external entities.

i) Certificates to HOST names or private IP addresses

ANF AC only issues SSL certificates to public domains that can be resolved on the Internet, avoiding the issuance of certificates to private IP that can use the certificates for an organization or home network and domains that cannot be resolved by DNS.

j) Minimum key lengths

ANF AC keeps track of the algorithms used and of secure key lengths, in accordance with the recommendations published by NIST or sites such as https://wiki.mozilla.org/CA:MD5and1024

5 Physical Security, Facilities, Management and Operational Controls

ANF AC maintains the following criteria in relation to the information available for audit and analysis of incidents related to certificates.

a) Control and incident detection

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

- By telephone: (+356) 2299 3100.
- By email: info@anfacmalta.com
- Filling the electronic form available on the website https://www.anfacmalta.com
- In person at one of the offices of the Recognized Registration Authorities.
- In person at one of the offices of ANF AC.

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

b) Incident Registry

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

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

5.1 Physical security controls

As defined in the CPS of ANF AC.

5.2 Procedural controls

As defined in the CPS of ANF AC.

5.3 Personnel controls

As defined in the CPS of ANF AC.

6 Technical Security Controls

6.1 Key pair generation and installation

As defined in the CPS of ANF AC.

6.2 Private Key Protection

As defined in the CPS of ANF AC.

6.3 Other management aspects of the key pair

As defined in the CPS of ANF AC.

6.4 Activation data

As defined in the CPS of ANF AC.

6.5 Computer security controls

As defined in the CPS of ANF AC.

6.6 Life cycle technical controls

As defined in the CPS of ANF AC.

6.7 Network security controls

As defined in the CPS of ANF AC.

6.8 Time-stamping

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

6.9 Cryptographic Module Security Controls

As defined in the CPS of ANF AC.

7 Certificates Profiles and List of Revoked Certificates

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

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

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

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

The subject public key is encoded per the specification RFC 5280, as well as the 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.

Proprietary fields

Internationally unambiguous identifiers have been assigned. Specifically:

- Fields referenced with OID 1.3.6.1.4.1.18339.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.

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 1.3.6.1.4.1.18339.41.1, outlining the amount in euros. In case of doubt or dispute, one must always give preference to the reading value outlined in the OID 1.3.6.1.4.1.18339.41.1.

- **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*)

Subject Alternative Name

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

- Email-based identity.

- Identity based on Distinguished Name (DN), which is often used to construct an alternative name based on proprietary attributes, which are not ambiguous in any case.

- Identity based on internet domain name (DNS).

- IP address-based identity.

- Identity based on universal resource identifier (URI).

7.1 Certificate Profiles

As defined in the technical background document.

7.2 CRL profile

As defined in the CPS of ANF AC.

7.3 OCSP profile

As defined in the CPS of ANF AC.

8 Compliance Audit

8.1 Frequency of compliance controls for each entity

As defined in the CPS of ANF AC.

8.2 Identification of the personnel in charge of the audit

As defined in the CPS of ANF AC.

8.3 Relationship between the auditor and the audited entity

As defined in the CPS of ANF AC.

8.4 List of items object of audit

As defined in the CPS of ANF AC.

8.5 Actions to be taken because of a lack of compliance

As defined in the CPS of ANF AC.

8.6 Treatment of audit reports

As defined in the CPS of ANF AC.

9 General Provisions

9.1 Fees

As defined in the CPS of ANF AC.

9.2 Financial liability

As defined in the CPS of ANF AC.

9.3 Confidentiality of information

As defined in the CPS of ANF AC.

9.4 Privacy of personal information

As defined in the CPS of ANF AC.

9.5 Intellectual property rights

As defined in the CPS of ANF AC.

9.6 Obligations and guarantees

As defined in the CPS of ANF AC.

9.7 Disclaimers of guarantees

As defined in the CPS of ANF AC.

9.8 Limitations of liability

As defined in the CPS of ANF AC.

9.9 Interpretation and execution

As defined in the CPS of ANF AC.

9.10 Management of the CP

As defined in the CPS of ANF AC.