Certification Policy

Legal Representatives of Legal Persons

Legal Representatives of Entities without Legal Personality

Legal Representatives of Sole and Joint and Several Directors 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 "Legal Representative of a Legal Person", “Legal Representative of an Entity without Legal Personality”, “Legal Representative of a Sole and Joint and Several Directors”. 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.

This document is only one of the several documents governing the PKI of ANF AC, it details and supplements the definitions in the Certification Practice Statement and its addendum. ANF AC oversees and supervises that this CP is compatible and consistent with the other documents drafted. All documentation is freely available to users and relying parties at 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 the certificates

These certificates can offer a natural person representing a legal person the electronic signature tool with which to perform procedures on behalf of the represented legal person.

The certificate in addition to identifying the natural person representative as subscriber/signatory and attests his/her powers of attorney over the represented legal person, includes information on it, on whose behalf it acts.

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

- **Legal Representative of a Legal Person Certificate**

  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity. They are linked to a legal person, the *Signatory* acts on behalf of a *legal person* as a legal representative with powers of attorney.

- **Legal Representative of an Entity without Legal Personality Certificate**

  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity for the sole purpose of being used in the tax and other Public Administration fields that are expressly allowed.

- **Legal Representative of Sole and Joint and Several Directors Certificate**

  Electronic certification issued by ANF AC which links the holder with signature verification data and confirms their identity. The *Signatory* acts in representation of a Legal Person as a legal representative with his position, as sole or joint and several directors, registered in the Mercantile Registry.

These certificates are issued in different supports and according to the security levels determined in the Commission Implementing Regulation (EU) 2015/1502 of the Commission of 8 September 2015 on setting specifications and minimum technical procedures for the security levels of electronic identification media in accordance with the

provisions of Article 8, paragraph 3 of Regulation (EU) 910/2014 of the European Parliament and of the Council, on electronic identification and trust services for electronic transactions in the internal market.

Available storage types:

- Cryptographic software token.
- HSM (hardware security module) Token. Certified with ISO 15408 Common Criteria EAL 4+ or higher.

These certificates are issued with different use modes:

- Authentication
- Electronic Signature
- Encryption

Regarding their consideration, the certificate to the have legal qualification of "qualified", shall incorporate the "QcCompliance" extension, as specified in the ETSI EN 319 412 standard.

All certificates issued under this policy are in accordance with X.509 Version 3 standard.

The maximum validity of these certificates is 5 years.

Identity verification will be done in person before a Registration Authority (RA), and based on original valid documentation. The RA is responsible for processing the application in accordance with the provisions stated in ANF AC's Certification Practice Statement. The person may waive appearance before the RA only in the cases expressly contemplated and authorized by the applicable legislation.

The verification of the information obtained by a Registration Authority, or any other provided by the subscriber, will be conducted by ANF AC, or collaborating entities classified for the purposes of this document as Issuance Reports Managers (IRM), with which ANF AC subscribe the applicable legal document.

1.2 Identification

Document name	Certification Policy for Legal Representatives of a Legal Person, Legal Representatives of an Entity without Legal Personality, Legal Representatives of a Sole and Joint and Several Directors Certificates.
Version	1.0

Policy Status	APPROVED
Document reference /OID	1.3.6.1.4.1.18339.2.5.1
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
Legal Representative of a Legal Person Certificate (AUTHENTICATION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.1
Legal Representative of a Legal Person Certificate (ENCRYPTION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.2
Legal Representative of a Legal Person Certificate (SIGNATURE). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.3
Legal Representative of an Entity without Legal Personality Certificate (AUTHENTICATION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.4
Legal Representative of an Entity without Legal Personality (ENCRYPTION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.5
Legal Representative of an Entity without Legal Personality (SIGNATURE). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.6

Legal Representative of a Sole and Joint and Several Directors Certificate (AUTHENTICATION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.7
Legal Representative of a Sole and Joint and Several Directors Certificate (ENCRYPTION). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.8
Legal Representative of a Sole and Joint and Several Directors Certificate (SIGNATURE). With SHA-256 algorithm and 2048-bit key length	1.3.6.1.4.1.18339.2.5.1.9

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

1.3 PKI Parties

1.3.1 Certification Authorities

As defined in the CPS of ANF AC.

1.3.2 Registration Authorities

As defined in the CPS of ANF AC.

1.3.2.1 Recognized Registration Authority

As defined in the CPS of ANF AC.

1.3.2.2 Collaborating Registration Authority

As defined in the CPS of ANF AC.

1.3.3 Issuance Reports Manager

As defined in the CPS of ANF AC.

1.3.4 End entities

1.3.4.1 Subscriber

As defined in the CPS of ANF AC.

1.3.4.2 Subject

As defined in the CPS of ANF AC.

1.3.4.3 Certificate Responsible

As defined in the CPS of ANF AC.

1.3.4.4 Relying third parties

As defined in the CPS of ANF AC.

1.4 Scope

1.4.1 Allowed usage

Generally, as established in the Certification Practice Statement of ANF AC; and specifically:

- " AUTENTHICATION " type certificate specially indicated to:
    - Authenticate before information systems and computer applications in general.

      The certificate incorporates the use of the key extension, allowing secure access to information systems and computer applications in general.
- "SIGNATURE" type certificate, specially indicated to:
    - Performing signature operations that require non-repudiation.
- "ENCRYPTION" type certificate, specially indicated to:
    - Perform data encryption operations.

1.4.2 Limits of certificate uses

Generally, as established in the Certification Practice Statement of ANF AC

Specifically, it must be stated that this certificate will be used by subscribers to maintain relationships with relying parties, per the uses permitted in the fields 'Key Usage' and 'Extended Key Usage' of the certificate, the limitations of use set out in the certificate, and assuming the responsibility limitation established in OID 1.3.6.1.4.1.18339.41.1 and/or in QcLimitValue OID 0.4.0.1862.1.2.

The use of keys and of the certificate by the subscriber, presupposes the acceptance of the conditions established in the CPS and its addendum.

1.4.3 Prohibited usage

As defined in the CPS of ANF AC.

1.5 Certification Entity contact details

As defined in the CPS of ANF AC.

1.6 Definitions and acronyms

As defined in the CPS of ANF AC.

2 Repositories and Information Publication

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

The encoding set for the Common Name (CN) field allows to identifies the certificate as a representation one, distinguishing it from a basic natural person one, through the literal 'R'. Likewise, it identifies the represented legal person to facilitate the certificate selection in case of a natural person representing several legal persons.

The field has a maximum size of 64 characters per RFC 5280.

Field	Content	Example	size *
Tax identification number	National/Foreign Citizens ID Card number	000000A	7
Name	As shown in the National/Foreign Citizens ID Card	John	
Surname 1	As shown in the National/Foreign Citizens ID Card	Harrison	
Literal	(R:		4
VAT number of the company	VAT number of the company per official records.	MT00000000	10
Literal	)		2
Literal by type	**AUTENTICATION SIGNATURE ENCRYPTION**		8

*(counting later blank space)

Example = 000000A John Harrison (R: MT00000000) SIGNATURE

In case of certificates of natural person legal representative of a legal person, the company name is included in the "organizationName" attribute and the VAT number in the "organizationIdentifier" attribute:

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

Attributes	Content	Example
organizationName	Corporate name, as stated in official records.	Corporate name. Ltd.
organizationIdentifier	VAT number, as stated in official records. Encoded per the European Standard ETSI EN 319 412-1	VATMT- 00000000

3.1.2 Specific fields completion guide

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

For all literal variables:

- All literals are entered in capital letters, with the exceptions of the domain name/subdomain and email that will be in lowercase.
- Do not include accent marks in the alphabetic literals
- Do not include more than one space between alphanumeric strings.
- Do not include blank characters at the beginning or end of alphanumeric strings.

- The inclusion of abbreviations based on a simplification is admitted, provided they do not difficult the interpretation of information.

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

National / Foreign Citizens ID Card

The term tax identification number covers both, the National Citizens ID Card, and the Foreign Citizens ID Card.
In case of opting on a specific ID card, instead of the tax identification number, the corresponding ID card will be used.

The following coding is allowed:

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

- Three characters to indicate the type of document per the following coding:

- "PAS" for identification based on passport number.
- "IDC" for identification based on the National/Foreign Citizens ID card.
- "PNO" for identification based on () national personal number (number of national civic register).
- "TAX" for identification based on a personal tax identification number issued by a national tax authority. This value is in disuse. The value "ID number" should be used instead. Tax Identification Number "TIN" per the European Commission - Taxation and Customs Union, specification published in:

  (Https://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

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

- Identity number with tax identification letter.

e.g.: IDCMT-000000A.

2.- Basic semantics. Consisting in:

The number and letter as stated in the ID card.
e.g.: 000000A.

3.1.3 Name restriction

The encoding of certificates follows the recommendation RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". All fields defined in the profile of the Certificates, except in fields specifically stated otherwise, use the coding UTF8String.

3.1.4 Need for names to be meaningful

Distinctive names must be meaningful

3.1.5 Anonymous or pseudonyms

The use of pseudonyms is not permitted.

3.1.6 Rules for interpreting various name formats

As defined in the CPS of ANF AC.

3.1.7 Uniqueness of names

As defined in the CPS of ANF AC.

3.1.8 Resolution of conflicts in relation to names and trademarks

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

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

It is not allowed to use distinctive signs whose right of usage is not owned by the subscriber, or is not duly authorized to do so.

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

3.2 Initial identity validation

3.2.1 Proof of possession of the private key

As defined in the CPS of ANF AC.

3.2.2 Authentication of the subscriber's identity

Certificates issued under this Certification Policy will identify the subject under whose name the certificate is issued and the certificate subscriber.

The Issuance Reports Manager shall use appropriate means to ensure the accuracy of the information contained in the certificate. Among these means it is included external registry databases and the ability to require information or documents to the subscriber.

The tax identification of the subscriber and the subject will be incorporated into the certificate.

When the qualified certificate contains other personal circumstances or attributes of the subscriber, such as its status as holder of a public office or membership of a professional association or qualification, this must be verified with official documents that prove it, in accordance with the applicable legislation.

The documentation type, processing forms, authentication and validation procedures are specified in the this document.

3.3 Re-key requests

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

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

3.4 Revocation request

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

4 Operational requirements

4.1 National interoperability scheme and National Security Scheme

4.1.1 Operation and management of the Public Key Infrastructure

Operations and procedures performed for the implementation of this Certification Policy are made following the controls required by the standards recognized for such purpose, describing these actions in sections "Physical Security, Facilities, Management and Operational Controls" and "Technical Security Controls" of the Certification Practice Statement of ANF AC.

The Certification Practice Statement of ANF AC, responds to different sections of the ETSI EN 319 411-2 standard.

4.2 Certificate application

ANF AC only accepts certificate issuance requests processed by natural persons of legal age, with complete legal capacity to act.

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

a) **Electronically**: On the website https://www.anfacmalta.com, the interested parties may access an application form that shall be filled and electronically signed with a qualified certificate. The certificate used must have been issued by a CA approved by ANF AC.

b) **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.

c) **By mail**: the subscriber may submit the application form to the offices of ANF AC certificate, having duly completed and authenticated his/her signature before a Collaborating Registration Authority.

4.3 Processing Procedure

4.3.1 Identity authentication

4.3.1.1 Subscriber

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

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

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

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

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

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

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

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

II. To non-EU citizens:

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

e) The legal representative must have sufficient powers of attorney. In addition, in case of:

1. Legal Representative of legal person certificate, it is determined if the legal representative has the absolute powers of attorney of the legal person, or at least specific powers of attorney that allow him/her to act before the Public Administration.
2. Legal Representative of entity without legal personality, it is determined if the legal representative has absolute powers of attorney of the entity, or at least specific powers of attorney that allow him/her to act before the Public Administration.

f) If the subscriber requests to include other personal circumstances such as his status as holder of a public office, his membership of a professional association or his degree, these must be verified through the official documents that accredit them, in accordance with its specific regulation.

Appearing before a Registry Authority may be foregone in any of the following situations:

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

2. Electronically. On the website https://www.anfacmalta.com, the interested parties have the application forms, which must be completed and signed electronically with a qualified certificate. The certificate used must have been issued by an CA supported by ANF AC.

[1] Declaration of Identity

It consists of a formal declaration under oath, in which the declarant states he/she personally and directly knows a natural person or a legal entity. Besides, it states, up to their direct knowledge, that he/she has verified that the filiation data outlined in the Application Form is true: the address, telephone, and e-mail. The Declaration of Identity incorporates the identity of the declarant, his/her ID card number, the data verified, the date and time of verification, the signature of the declarant and the appropriate legal warnings in case of lying under oath.

4.3.1.2 Subject

In any of the following situations, it shall be requested from the subject its VAT number or Tax Identification.

4.3.1.2.1 Legal Person

The subscriber who processes the certificate application, must submit original or certified copies of the following valid documents:

1. Per the legal form:
    - Corporations and other legal entities which registration is compulsory in the Mercantile Registry, shall attest their valid incorporation by providing original or certified copy of the Mercantile Registry regarding their incorporation data and current directors of the entity.

    - Associations, Foundations, and Cooperatives shall attest their valid incorporation by providing original or certified copy of a public record certificate detailing the registration of their incorporation.

    - Civil societies and other legal entities shall provide an original or certified copy of the document attesting their incorporation in an irrefutable manner.

    - Public Administrations and entities belonging to the public sector:

        - Entities whose registration is mandatory in a Registry attest their valid incorporation by providing original or certified copy of a certificate in relation to the incorporation data and their legal personality.
        - Entities incorporated in accordance to a regulation, shall provide reference to such regulation

4.3.1.2.2 Legal Representative of an entity without legal personality

The legal representative processing the certificate application, must submit original or certified copies of the following valid documentation:

1. A document certifying the valid incorporation of the entity:
    - Tax identification of the subscriber.
    - Certificates or certified copies evidencing registration, issued on the date of the application or on the preceding 15 days:
        - In the case of investments funds, venture capital funds, mortgage securities market regulation funds, mortgage qualifications funds, assets titling funds, investment guarantee funds and pension funds: certificate of registration in the corresponding registry the Ministry of Finance or the National Securities Market Commission, the identification of the management body must be recorded in the certificate.

        - In the case of joint ventures that have benefited from the special tax regime, shall provide certificate of such registration. In case they are not registered, a document signed by a majority of members or partners, confirming the validity of the entity.

- When the entity does not correspond to any of the types outlined above and, therefore, does not need to be registered in any Registry, it shall be submitted alongside the application, all documents the subscriber deems as valid, being the IRM the responsible to determine the sufficiency or insufficiency thereof.

4.3.1.2.3 Legal Representative of sole and joint and several directors

The legal representative processing the certificate application, must submit original or certified copies of the following valid documentation:

1. Per the legal form:

   Type of certificate exclusively for legal representatives of corporations and other legal entities whose registration is compulsory in the Mercantile Registry, and which meets the condition of being the sole or joint and several director of these.

   They shall attest the validity of the corporation and their position, as well as providing proof of their registration in the Mercantile Registry by providing certified copies of the corresponding deeds, subject to verification by the IRM.

4.3.2 Approval or rejection of certificate applications

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

Moreover, he/she will determine:

- That the subscriber has 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 obligations and responsibilities of the CA, the subscriber, subject, certificate responsible and relying parties, especially to the CPS and Certification Policies.

- Shall monitor compliance with any requirement imposed by the legislation on data protection, as established in the security document included in the CPS.

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:

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

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

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

- It is verified that none of the natural or legal persons associated with the request appear in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18339.56.2.1.

4.3.3 Time to process certificate issuance

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

4.4 Certificate issuance

As defined in the CPS of ANF AC.

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

4.4.1 Certification entity's actions during the certificate issuance process

As defined in the CPS of ANF AC.

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

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

4.4.2 Notification to subscriber

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

4.5 Certificate acceptance

4.5.1 Acceptance

As established in the ANF AC CPS.

4.5.2 Return

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.

4.5.3 Monitoring

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

4.5.4 Certificate Publication

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

4.5.5 Notification of certificate issuance to third parties

No notification is made to third parties.

4.6 Rejection

As defined in the CPS of ANF AC.

4.7 Renewal of Certificate

Generally, as defined in the CPS of ANF AC.

4.7.1 Valid Certificates

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

Only valid certificates can be renewed.

4.7.2 Persons authorized to request the renewal

The renewal application form must be signed by the subscriber, or by the legal representative with enough powers of attorney.

The personal circumstances of the subscriber should not have changed

4.7.3 Identification and authentication of the routine renewal applications

Identification and authentication for certificate renewal can be done in person using one of the methods described in this section, or processed electronically by completing the corresponding form and signing it with a valid certificate electronically issued as “qualified”, and stating as holder the certificate subscriber of which renewal is requested.

Certificate renewal by electronically signed applications requires that less than five years have passed since the personal identification took place.

To ensure compliance and to not exceeding the period of 5 years from the initial identification, ANF AC applies the following procedures and technical security measures:

- Certificates of ANF AC shall be always generated using a token that must be used to perform any renewal process.

  This token is unique to any other provided by ANF AC and is programmed so that the user may be able to make a single renewal. This technical procedure prevents an automatic processing once 5 years have passed since the initial identification, since certificates of end users emitted by ANF AC are limited to maximum term of 5 years.

- ANF AC follows a system of registration of applications, distinguishing date of request, -which coincides with the identification - and of issuance of the certificate. This control allows a second renewal if the period of 5 years has not been reached since the initial identification. The technical system requires a specific request of the user, the direct intervention of an ANF AC operator, which in turn, requires validating the application by applying coherent security verification. If 5 years have exceeded, the application itself blocks the process, otherwise facilitates the operator the process until the certificate renewal.

4.7.3.1 Renewal of certificates that have exceeded 5 years from the initial identification

The formalization of the application is done with the handwritten signature of the subscriber, done in-situ by the interested party, and using the necessary original documents. This formality can be carried out before:

- Recognized Registration Authority which, per the definition of the CPS of ANF AC, are the natural or legal persons to whom ANF AC has equipped with the necessary technology to perform the functions of a registry entity, having formalized the corresponding liability assumption and collaboration agreement.

- Collaborating Registration Authority which, per the definition of the CPS of ANF AC, are persons who, in accordance to current legislation, have powers of public notary.

- Trust Entities which, per the definition of the CPS of ANF CP, are entities that have the necessary capacity to determine the identity, capacity, and freedom of action of the subscribers.

4.7.4 Approval or rejection of applications for renewal

Same procedure as that performed in the issuance process specified herein.

4.7.5 Notification of certificate renewal

Same procedure as that performed in the issuance process specified herein.

4.7.6 Acceptance of a certificate renewal

Same procedure as that performed in the issuance process specified herein.

4.7.7 Publication of the renewal certificate

Same procedure as that performed in the issuance process specified herein.

4.7.8 Notification to third entities

It is not contemplated.

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

The renewal of expired or revoked certificates is not authorized.

4.8 Certificate modification

Not applicable.

4.9 Revocation and suspension of certificates

Generally, as defined in the CPS of ANF AC.

4.9.1 Circumstances for revocation

Besides those defined in the CPS, ANF AC shall:

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

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

    - Nature of the incident.
    - Received information.
    - Legal standards and regulations on which the revocation order is substantiated on.

4.9.2 Identification and authentication of revocation applications

The revocation of a certificate may be requested by:

- The certificate subscriber

- The legal representative of the subscriber

- A representative duly authorized

- ANF AC

- The Recognized Registration Authority that intervene in the processing of the certificate issuance application

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

- **Electronically**: by the subscriber or certificate responsible electronically signing the revocation request on the date of the revocation request.

- **By telephone**: by replying to the questions asked from the telephone support service available at the number (+356) 2299 3100.
- **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 has been compromised, or any other fact that would recommend taking such action.

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

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

4.9.3 Procedure for revocation request

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

The revocation application shall contain at least the following information:

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

The revocation application shall be processed upon receipt.

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

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

4.9.4 Revocation request grace period

As defined in the CPS of ANF AC.

4.9.5 Maximum processing time of the revocation request

As defined in the CPS of ANF AC.

4.9.6 CRL lists verification requirements

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

4.9.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.9.8 On-line verification availability of the revocation

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

4.9.9 On-line verification requirements of the revocation

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

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

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

Access to this system is free.

4.9.10 Certificate suspension

Not applicable.

4.9.11 Suspension requests identification and authentication

Certificate suspension is not allowed.

4.10 Key storage and recovery

ANF AC does not store nor has the ability to store the private key of the subscribers, and therefore offers no key recovery service.

5 Physical Security, Facilities, Management and Operational controls

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

a) Control and incident detection

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

- By telephone: (+356) 2299 3101.
- 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 minimum sample of 3% of the issued certificates.

b) Incident Registry

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

The Security Manager determines the severity of the incident and names a responsible and, in case of significant security incidents, reports to the PKI Governing Board.

5.1 Physical security controls

As defined in the CPS of ANF AC.

5.2 Procedural controls

As defined in the CPS of ANF AC.

5.3 Personnel controls

As defined in the CPS of ANF AC.

6 Technical security controls

6.1 Key pair generation and installation

As defined in the CPS of ANF AC.

6.2 Private Key Protection

As defined in the CPS of ANF AC.

6.3 Other management aspects of 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 CPS of ANF TSA CA.

6.9 Cryptographic Module Security Controls

As defined in the CPS of ANF AC.

7 Certificate Profiles and CRL and OCSP

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

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

- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI) Certificate Profiles, Part 5: QCStatements
- 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 1 is outlined

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

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 audited

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 Regulations

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.