Certification Policy for Public Employee 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 7
1.1 Description of certificates 8
1.2 Identification 10
1.3 Parties of the PKI 12
1.3.1 Certification Authorities 12
1.3.2 Registration Authorities 12
1.3.2.1 Recognized Registration Authority 12
1.3.2.2 Collaborating Registration Authority 12
1.3.3 Issuance Reports Manager 12
1.3.4 End entities 12
1.3.4.1 Subscriber 12
1.3.4.2 Subject 12
1.3.4.3 Certificate Responsible 12
1.3.4.4 Relying parties 13
1.4 Certificates usage 13
1.4.1 Allowed usage 13
1.4.2 Limits of certificate usage 13
1.4.3 Prohibited usage 13
1.5 Certification Entity contact details 14
1.6 Definitions and acronyms 14

2 Repositories and Information Publication 15
2.1 Repositories 15
2.2 Information publication 15
2.3 Frequency of updates 15
2.4 Access controls to repositories 15

3 Identification and Authentication 16
3.1 Name registration 16
3.1.1 Types of names 16
3.1.2 Specific fields completion guide 17
3.1.3 Need for names to be meaningful 18
3.1.4 Anonymous or pseudonyms 18
3.1.5 Rules for interpreting various name formats 18
3.1.6 Uniqueness of names 18
3.1.7 Resolution of conflicts in relation to names and trademarks 18
3.2 Initial identity validation 19
3.2.1 Proof of possesion of the private key 19
3.2.2 Authentication of the identity 19

3.3 Re-key requests 19
3.4 Revocation requests 19

4 Operational Requirements 20
4.1 Certificate application 20
4.2 Processing procedure 20
4.2.1 Identity authentication 20
4.2.1.1 Subscriber 20
4.2.1.2 Subject / Certificate Responsible 22
4.2.2 Approval or rejection of certificate applications 22
4.2.3 Time to process certificate issuance 23
4.3 Certificate issuance 23
4.3.1 Certification entity's actions during the certificate issuance process 23
4.3.2 Notification to subscriber 24
4.4 Certificate acceptance 24
4.4.1 Acceptance 24
4.4.2 Return 24
4.4.3 Monitoring 24
4.4.4 Certificate publication 24
4.4.5 Notification of certificate issuance to third parties by the CA 25
4.5 Rejection 25
4.6 Renewal of certificates 25
4.6.1 Valid Certificates 25
4.6.2 Persons authorized to request the renewal 25
4.6.3 Identification and authentication of the routine renewal applications 25
4.6.4 Approval or rejection of applications for renewal 26
4.6.5 Notification of certificate renewal 26
4.6.6 Acceptance of the certificate renewal 26
4.6.7 Publication of the renewal certificate 26
4.6.8 Notification of certificate renewal 26
4.6.9 Identification and authentication of re-keying applications after revocation (non-compromised key) 26
4.7 Certificate modification 27
4.8 Revocation and suspension of certificates 27
4.8.1 Causes of revocation 27
4.8.2 Identification and authentication of revocation applications 27
4.8.3 Procedure for revocation request 28
4.8.4 Revocation request grace period 28
4.8.5 Maximum processing time of the revocation request 29
4.8.6 CRL lists verification requirements 29
4.8.7 CRL issuance frequency 29

4.8.8 On-line verification availability of the revocation 29
4.8.9 On-line verification requirements of the revocation 29
4.8.10 Certificate suspension 29
4.8.11 Suspension requests identification and authentication 29
4.9 Key storage and recovery 30

5 Physical Security, Facilities, Management and Operational Controls 31
5.1 Physical security controls 31
5.2 Procedural controls 31
5.3 Personnel controls 31

6 Technical Security Controls 32
6.1 Key pair generation and installation 32
6.2 Private key protection 32
6.3 Other management aspects of the key pair 32
6.4 Activation data 32
6.5 Computer security controls 32
6.6 Life cycle technical controls 32
6.7 Network security controls 32
6.8 Time-stamping 32
6.9 Cryptographic Module Security Controls 32

7 Certificate Profiles , CRL and OCSP 33
7.1 Certificate profiles 35
7.2 CRL profile 35
7.3 OCSP profile 35

8 Compliance Audit 36
8.1 Frecuency of compliance controls for each entity 36
8.2 Identification of the personnel in charge of the audit 36
8.3 Relationship between the auditor and the audited entity 36
8.4 List of items subject to audit 36
8.5 Actions to be taken because of a lack of compliance 36
8.6 Treatment of audit reports 36

9 General Provisions 37
9.1 Fees 37
9.2 Financial liability 37
9.3 Confidentiality of information 37
9.4 Privacy of personal information 37
9.5 Intellectual property rights 37
9.6 Obligations and guarrantees 37

9.7 Disclaimers of guarrantees 37
9.8 Limitations of liability 37
9.9 Interpretation and execution 37
9.10 Management of the CP 37

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 certificates of the type "Public Employee" issued by ANF AC, in which the signatory is an employee of the Public Administration, being public servant, staff or temporary personnel, and the certificate subscriber is a Public Administration. These certificates are issued with 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 Certificates

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

- **Public Employee Certificate**

The purpose of this certificate is to allow its subscribers to authenticate in online services and to generate electronic signatures.

This is a certificate in which the subscriber is a representative of a Public Administration with sufficient competences to solicit the certificate. and the subject, which is in possession of the signature creation device, is personnel from the Public Administration., being public servant, staff, or temporary personnel. The subject, by being in possession of the signature creation device, and acting as personnel of the Public Administration, adopts the obligations and responsibilities of the certificate responsible.

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, only the certificate “electronic signature” is issued by ANF AC with the consideration of “qualified”. The certificate, to have this legal consideration, incorporates the extension of “qualified” as described in this document per 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

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 whom ANF AC subscribes the necessary legal document.

This policy, in terms of the certificates of the type "Public Employee", follows the definitions set by the Directorate of Information and Communications Technology in its document "Electronic certificates Profiles" of April 2016.

Two levels of assurance are defined:

The following assurance levels are defined:

a. **Medium level/Substantial:**

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

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

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

Minimum acceptable security mechanisms include X.509 software certificates. In the case of certificates issued to natural persons, it corresponds to a "qualified certificate", as defined in the Regulation (EU) 910/2014 for qualified electronic seal without a qualified signature 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.

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

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

b. High level:

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

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

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

Acceptable security mechanisms include X.509 certificates in hardware. In the case of certificates issued to natural persons, it corresponds with the "qualified certificate", 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.

1.2 Identification

Document name	Certification Policy for Public Employee Certificates
Version	1.0
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.4.1
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
High Level Public Employee Certificate (AUTHENTICATION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.4.1.1.22
Medium Level Public Employee Certificate with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.4.1.2.22
High Level Public Employee Certificate (SIGNATURE) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.4.1.3.22
High Level Public Employee Certificate (ENCRYPTION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.4.1.4.22

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

- 2.16.724.1.3.5.7.1

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

- 2.16.724.1.3.5.7.2

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

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

qcp-natural-qscd (0.4.0.194112.1.2). When the signature qualified certificate, is stored in qualified device per Regulation UE 910/2014

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

1.3 Parties of the PKI

1.3.1 Certification Authorities

As defined in the CPS of ANF AC.

1.3.2 Registration Authorities

As defined in the CPS of ANF AC.

1.3.2.1 Recognized Registration Authority

As defined in the CPS of ANF AC.

1.3.2.2 Collaborating Registration Authority

As defined in the CPS of ANF AC.

1.3.3 Issuance Reports Manager

As defined in the CPS of ANF AC.

For the purposes of this policy only the Chairman of the PKI Governing Board can intervene as Issuance Reports Manager.

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 Certificate usage

1.4.1 Allowed usage

Generally, as defined in the CPS of ANF AC, and specifically:

- Public Employee Certificate of the type AUTHENTICATION: to authenticate before information systems and computer applications in general.

  The certificate incorporates key usage extension, enabling secure access to computer information systems and computer applications in general.

- Public Employee Certificate of the type SIGNATURE, particularly suitable for signature operations that do not require repudiation.

- Public Employee Certificate of the type ENCRYPTION, particularly suitable for asymmetric encryption operations.

1.4.2 Limits of certificate uses

The subject can only use the private key and the certificate for uses authorized on this PC, per the role and security level granted in accordance with the provisions of the 'KeyUsage' and 'ExtendedKeyUsage' certificate fields and in accordance to the usage limitations stated in the certificate, assuming the limitation of liability contained in the OID 1.3.6.1.4.1.18339.40.1. and / or in QcLimitValue OID 0.4.0.1862.1.2.

The subject may only use the key pair and the certificate after accepting the conditions of use established in the CPS.

1.4.3 Prohibited uses

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 of repositories

As defined in the CPS of ANF AC.

3 Identification and Authentication

3.1 Names registration

3.1.1 Types of names

ETSI has developed European standards in compliance with the European Commission Mandate M / 460 for the streamline of standards in the field of electronic signatures. The ETSI EN 319 412 family specifies the content of the certificates issued to natural persons.

Specifically, part 2 of this document, ETSI EN 319 412-2 v2.1.1 (*Part 2: certificate profile for certificates issued to natural persons*) defines the content requirements of certificates issued to natural persons. The profile is based on IETF RFC 5280 recommendations and the ITU-T X.509 standard.

All certificates contain a Distinguished Name (DN) of the natural person holder of the certificate, defined per Recommendation ITUT X.501 and contained in the Subject field, including a Common Name (CN) component.

The CN (CommonName) attribute of the DN must refer to the subscriber's name. It must:

- Include the **NAME**, in accordance with what is stated in the National/Foreign Citizens ID Card or passport, and in capital letters.
- Blank space
- Include the **FIRST AND SECOND SURNAME**, in capital letters, separated only by a blank space, in accordance with what is pointed out in the National/Foreign Citizens ID Card. In case there is not a second surname, the field shall be left blank (without any character).
- Blank space
- Include a **hyphen** that separates the name and surname from the National/Foreign Citizens ID Card number, with no space between the values nor punctuation signs.
- Blank space
- Include the **tax identification number**, per the National/Foreign Citizens ID Card. The tax identification number for natural persons is also the National/Foreign Citizens ID Card number. No space between the number and control letter; the control letter shall be in uppercase.

  e.g.: John Harrison Smith – 000000A

Personal circumstances and attributes of the persons and organizations identified in the certificates are included in predefined attributes in regulations and technical specifications for general recognition.

3.1.2 Specific fields completion guide

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

For all variables literal:

- 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 difficulty in the interpretation of information.

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

Tax Identification Number and Personal Identification Number (PIN, PRN)

The tax identification number, shall be in accordance with current regulations. Examples:

Entities: *include the letter and numbers. E.g.: “*MT00000000*”*

Persons: *include numbers and letter at the end, without hyphen separation. E.g.: “000000A”*

The Personal Identification Number (PIN) in the Personnel Central Registry is composed by eight numerical positions and an alphanumeric control position. The PIN is the key that identifies people in the Personnel Central Registry Information System.

The PIN is built depending on:

1. The kind of document that provided the person in his first relationship with the General State Administration.
2. The date of incorporation in its first relationship with General State Administration.

PIN		Document presented at the first Service Relationship with the SGA		Examples
Number (8 positions)	**Control (1 position)**			
ID without letter	Blank, 1, 2	ID		000000 000000-1 000000-2
Sequential generated by the system	N	From 01/01/2003	Other document	000000-A
Built based on the document presented	3, 4, 5, 6, 7, 8, 9	Before 01/01/2003		000000-3

3.1.3 Need for names to be meaningful

In all cases the distinctive names should make sense.

3.1.4 Anonymous or pseudonyms

Not allowed.

3.1.5 Rules for interpreting various name forms

As defined in the CPS of ANF AC.

3.1.6 Uniqueness of names

As defined in the CPS of ANF AC.

3.1.7 Resolution of Conflicts in relation to names and trademarks

Certificate subscribers shall not include names in applications that may involve breach of third party trademark rights.

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

3.2 Initial Identity validation

3.2.1 Proof of possessionof the private key

As defined in the CPS of ANF AC.

3.2.2 Authentication of the identity

Certificates issued under this Certification Policy will identify the subscriber under whose name the certificate issuance is request, the subject and where appropriate the certificate responsible.

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.

The documentation, processing forms, 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 applicant's ability to handle this requirement.

4 Operational Requirements

4.1 Certificate application

ANF AC only accepts certificate issuance requests processed by natural persons of legal age, with full legal capacity to act and with sufficient powers of attorney.

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.

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.

ANF AC does not generate the keys of its users. The subscriber must generate his/her own key pair and the request certificate in PKCS#10 / CSR format, providing it to ANF AC along with the certificate Application Form.

4.2 Processing procedure

4.2.1 Identity authentication

4.2.1.1 Subscriber

The application of certificates defined in this Certification Policy is limited to public authorities or entities with which it has been established a certification agreement, contract or some other formula that implements the service provision by ANF AC.

The identification of the administration or public institution is made in the registration process of the Entity, which will be subscribed by a natural person with the capacity to represent the Administration or Entity.

The subscriber's identification will be done in person before a Recognized Registration Authority. In such act, he/she must prove their legal capacity to represent the Public Administration in whose behalf the application for the certificate is being processed.

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 Citizens 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 subscriber shall possess sufficient powers of attorney or competence.
f) If the subscriber requests to include other personal circumstances, these must be verified through the official documents that accredits 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.

4.2.1.2 Subject / Certificate Responsible

In the application form, the subscriber must identify and expressly authorize the certificate subject. This authorization shall be perfected with a voluntary and express acceptance by the natural person who assumes the consideration of Certificate Subject, and undertaking the obligations and responsibilities of a Certificate Responsible.

The Subject must appear before the Registration Authority, prove its identity in the same manner the Subscriber's identification is done, which is detailed in the preceding section.

4.2.2 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.

Specially, shall verify the existence and legality of the Public Administration, the competence of the subscribe to solicit the certificate, the subject and their affiliation to the Public Administration as an employee.

Moreover, 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 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 applicant 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.

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 certificate must be made within 48 hours, once issued the report of the IRM, 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 duringthe 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.

4.3.2 Notification to subscriber

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

4.4 Certificate acceptance

4.4.1 Acceptance

As defined in the CPS of ANF AC.

4.4.2 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.

4.4.3 Monitoring

ANF AC is not responsible for the monitoring, investigation, or confirmation of the accuracy of the information contained in the certificate after issuance. For information on the inaccuracy or no current 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 by the CA

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.

4.6.2 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 that process the application of the certificate.

The personal circumstances of the subscriber should not have changed, especially its capacity as legal representative or sufficient competences to solicit the certificate.

4.6.3 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 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.

- 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.

4.6.4 Approval or rejection of applications for renewal

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

4.6.5 Notification of certificate renewal

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

4.6.6 Acceptance of the certificate renewal

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

4.6.7 Publication of the renewal certificate

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

4.6.8 Notification of certificate renewal

As specified in paragraph 4.4.5 "Notification of the 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.

- 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.

4.8.2 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 with sufficient powers of attorney.

- 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 3101.

- **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.

4.8.3 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.

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 Maximun 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 offers relying third 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 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.

4.8.10 Certificate suspension

Not applicable.

4.8.11 Suspension requests identification and authentication

Certificate suspension is not allowed.

4.9 Key storage and recovery

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 (International).
- 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, 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 subject to audit

As defined in the CPS of ANF AC.

8.5 Actions to be taken because of a lack of compliance

As defined in the CPS of ANF AC.

8.6 Treatment of audit reports

As defined in the CPS of ANF AC.

9 General Provisions

9.1 Fees

As defined in the CPS of ANF AC.

9.2 Financial liability

As defined in the CPS of ANF AC.

9.3 Confidentiality of information

As defined in the CPS of ANF AC.

9.4 Privacy of personal information

As defined in the CPS of ANF AC.

9.5 Intellectual property rights

As defined in the CPS of ANF AC.

9.6 Obligations and guarrantees

As defined in the CPS of ANF AC.

9.7 Disclaimers of guarrantees

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.