



Certification Policy for Issuance Reports Manager and PKI Operator Certificates



Maltese Registrar of Companies Number C75870 and VAT number MT 23399415



© ANF AC MALTA, LTD
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

This document is property of ANF AC MALTA

Distribution and reproduction prohibited without authorization by ANF AC MALTA

Copyright © ANF AC MALTA 2016

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

Telephone: (+356) 2299 3100

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



Index

1	Introduction	6
1.1	Description of the certificates	7
1.2	Identification	7
1.3	PKI Parties	9
1.3.1	Certification Authorities	9
1.3.2	Registration Authorities	9
1.3.3	Issuance Reports Manager	9
1.3.4	End entities	9
1.3.4.1	Subscriber	9
1.3.4.2	Subject	9
1.3.4.3	Relying parties	10
1.4	Scope	10
1.4.1	Allowed usage	10
1.4.2	Limits of certificate usage	10
1.4.3	Prohibited usage	10
1.5	Certification entity contact details	10
1.6	Definitions and acronyms	10
2	Repositories and Information Publication	11
2.1	Repositories	11
2.2	Information publication	11
2.3	Frequency of updates	11
2.4	Access controls to repositories	11
3	Identification and Authentication	12
3.1	Name registration	12
3.1.1	Types of names	12
3.1.2	Specific fields completion guide	13
3.1.3	Need for names to be meaningful	14
3.1.4	Anonymous or pseudonyms	15
3.1.5	Rules for interpreting various name formats	15
3.1.6	Uniqueness of names	15
3.1.7	Resolution of conflicts in relation to names and trademarks	15
3.2	Initial identity validation	15
3.2.1	Proof of possession of the private key	15
3.2.2	Authentication of the subscriber's identity	15
3.3	Re-key requests	15
3.4	Revocation requests	15



4	Operational requirements	16
4.1	Certificate application	16
4.2	Processing procedure	16
4.2.1	Identity authentication	16
4.2.1.1	Subscriber	16
4.2.2	Approval or rejection of certificate applications	18
4.2.3	Time to process certificate issuance	19
4.3	Certificate issuance	19
4.3.1	Certification entity's actions during the certificate issuance process	19
4.3.2	Notification to subscriber	19
4.4	Certificate acceptance	20
4.4.1	Acceptance	20
4.4.2	Return	20
4.4.3	Monitoring	20
4.4.4	Certificate publication	20
4.4.5	Notification of certificate issuance to third parties	20
4.5	Rejection	20
4.6	Renewal of certificates	20
4.6.1	Valid Certificates	21
4.6.2	Persons authorized to request the renewal	21
4.6.3	Identificaton and authentication of the routine renewal applications	21
4.6.3.1	Renewal of certificates that have exceeded 5 years from the initial identification	22
4.6.4	Approval or rejection of applications for renewal	22
4.6.5	Notification of certificate renewal	22
4.6.6	Acceptance of the certificate renewal	22
4.6.7	Publication of the renewal certificate	22
4.6.8	Notification to third entities	23
4.6.9	Identification and authentication of re-keying applications after revocation (non-compromised key)	23
4.7	Certificate modification	23
4.8	Revocation and suspension of certificates	23
4.8.1	Circumstances for revocation	23
4.8.2	Identification and authentication of revocation applications	23
4.8.3	Procedure for revocation request	24
4.8.4	Revocation request grace period	25
4.8.5	Maximum processing time of the revocation request	25
4.8.6	CRL lists verification requirements	25
4.8.7	CRL issuance frequency	25
4.8.8	On-line verification availability of the revocation	25
4.8.9	On-line verification requirements of the revocation	25
4.8.10	Certificate suspension	26



4.8.11	Suspension requests identification and authentication	26
4.9	Key storage and recovery	26
5	Physical Security, Facilities, Management and Operational Controls	27
5.1	Physical security controls	27
5.2	Procedural controls	27
5.3	Personnel controls.....	27
6	Technical Security Controls	28
6.1	Key pair generation and installation	28
6.2	Private key protection.....	28
6.3	Other management aspects of the key pair	28
6.4	Activation data	28
6.5	Computer security controls	28
6.6	Life cycle technical controls	28
6.7	Network security controls.....	28
6.8	Time-stamping	28
6.9	Cryptographic Module Security Controls.....	28
7	Certificate Profiles and CRL and OCSP Lists.....	29
7.1	Certificate profiles.....	31
7.2	CRL profile	31
7.3	OCSP profile.....	31
8	Compliance Audit	32
8.1	Frecuency of compliance controls for each entity	32
8.2	Identification of the personnel in charge of the audit	32
8.3	Relationship between the auditor and the audited entity	32
8.4	List of items audited.....	32
8.5	Actions to be taken because of a lack of compliance.....	32
8.6	Treatment of audit reports	32
9	General Provisions	33
9.1	Fees.....	33
9.2	Financial liability	33
9.3	Confidentiality of information.....	33
9.4	Privacy of personal information.....	33
9.5	Intellectual property rights.....	33
9.6	Obligations and guarantees	33
9.7	Disclaimers of guarantees	33
9.8	Limitations of liability	33
9.9	Interpretation and execution	33
9.10	Management of the CP	33



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 "Issuance Reports Manager Certificate" and "PKI Operator". 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

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

- **Issuance Reports Manager Certificate**

This is a certificate used by the Issuance Reports Manager (IRM) to electronically sign the issuance acts, other processes associated with its role as IRM and to electronically authenticate with ANF AC trusted servers.

The maximum validity of these certificates is 5 years.

- **PKI Operator Certificate**

This is a certificate used by ANF AC employees, or by external collaborators who are authorized to access and make use of ANF AC systems.

The maximum validity of these certificates is 5 years.

The issuance of these certificates requires the prior agreement of the Governing Board of the PKI.

The identity and other information contained in these certificates will be processed by any of the members of the Governing Board of the PKI, which will perform the functions of Registration Authority.

The verification of the information obtained by a Registration Authority will be made by the Chairman of ANF AC's Governing Board, which will perform the functions of Issuance Reports Manager (IRM).

1.2 Identification

Document name	Certification Policy for Issuance Reports Manager and PKI Operators Certificates
Version	1.0
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.23.1



Issuance date	November 15 th , 2016
Expiration date	Not applicable
Related CPS	Certification Practice Statement (CPS) of ANF AC
Location	https://www.anfacmalta.com

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

Certificate	OID
Issuance Reports Manager Certificate (AUTHENTICATION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.1.22
Issuance Reports Manager Certificate (ENCRYPTION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.3.22
Issuance Reports Manager Certificate (SIGNATURE) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.4.22
PKI Operator Certificate (AUTHENTICATION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.2.22
PKI Operator Certificate (ENCRYPTION) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.5.22
PKI Operator Certificate (SIGNATURE) with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18339.23.1.6.22

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 qualified device according to Regulation (UE) 910/2014.

1.3 PKI Parties

1.3.1 Certification Authorities

As defined in the CPS of ANF AC.

1.3.2 Registration Authorities

For the purposes of this policy only members of the Governing Board of the PKI can intervene as Registration Authority.

1.3.3 Issuance Reports Manager

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

1.3.4 End entities

1.3.4.1 Subscriber

This is the natural person holder of the certificate, by agreement of the Governing Board of the PKI, he/she is authorized to process and receive a certificate of these features.

Depending on the type of certificate:

- **Issuance Reports Manager**
This is staff that has made specific training as Issuance Reports Manager, and has obtained the corresponding qualification to perform this task.
- **PKI Operator**
This is staff that has made specific training as PKI Operator, and has obtained the corresponding qualification to perform this task.

1.3.4.2 Subject

This is the certificate subscriber, which processes the request on its own behalf, personally and in person.

The certificate subscriber holds the signature creation device, and is responsible for its use and custody.



1.3.4.3 Relying third parties

As defined in the CPS of ANF AC.

1.4 Scope

1.4.1 Allowed usage

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

- **PKI Operator**
Using ANF AC computer equipment, for the development of work that falls under its responsibility.
To electronically authenticate with ANF AC trusted servers.
- **Issuance Reports Manager**
Using the certificates only in applications that have been specifically designed for the intervention as Issuance Reports Manager.
To electronically authenticate with ANF AC trusted servers.

1.4.2 Limits of certificate usage

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 OcLimitValue 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 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

Attribute O (Organization), in case of inclusion, needs to refer to the collegiate certification: Name of the Official College of which he/she is an active member. Moreover, the collegiate number is included, separated by the character "/". E.g. O = Collegiate Name / collegiate number.

In the case of professional training: it may be included the name of the association, guild, or group to which he/she belongs. Or issuer of the professional training qualification. Additionally, it may be included the associate number as specified in the previous paragraph.

In the case of freelancers may include: registered trade name or registered trademark on behalf of the subscriber.

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 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.: ID000000A.

3.1.3 Need for names to be meaningful

In all cases the distinguished names must make sense.

3.1.4 Anonymous or pseudonyms

It is not permitted.

3.1.5 Rules for interpreting various name formats

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 will not include names in applications that may involve infringement, by the subscriber of third parties' 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 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 subscriber who applies for the issuance of the certificate.

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 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.

Likewise, when the subscriber wants to include a representative capacity which has been granted by a third party, either by mandate or powers of attorney, the subscriber shall prove such condition with the original document.

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 requests

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



4 Operational Requirements

4.1 Certificate application

ANF AC only accepts certificate issuance request processed by a natural person who has been expressly authorized by the Governing Board of the PKI.

ANF AC only accepts certificate issuance request processed by a natural person, of legal age, and complete legal capacity to act.

The subscriber must complete the Application Form of the certificate assuming responsibility for the accuracy of the information reviewed, and process it before ANF AC using any of the following means:

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

4.2 Processing procedure

4.2.1 Identity authentication

4.2.1.1 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 Citizens 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) In case the subscriber has a representation mandate or powers of attorney, and request that the document be attached to the certificate. It will be required to:
1. Representation mandate. The document must be in pdf format and signed by the client with an interpretable eSign signature, using an electronic certificate issued by ANF AC. The request for inclusion of the mandate presupposes for the subscriber the full acceptance of the representation mandate.
 2. Powers of attorney. The original document will be digitized by the RA operator who will sign it electronically.
- 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.

***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.

4.2.2 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.

4.2.3 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 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.

4.3.2 Notification to subscriber

ANF AC notifies the subscriber via e-mail of 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.

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.

The personal circumstances of the subscriber should not have changed.

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, 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.

4.6.3.1 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.

4.6.4 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 to third entities

As defined in section 4.4.5 "Notification of issuance of the certificate 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 Circumstances for revocation

Besides those defined in the CPS, ANF AC shall:

- The loss of personnel status attached to the Recognized Registry Authority that supported the issuance of this certificate.
- 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.
- 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 (International).
- **In person:** the subscriber or the legal representative of the certificate holder appearing before any of ANF AC's offices published in the web address <https://www.anfacmalta.com>, proving their identity through original documentation, and manually signing the appropriate form.

ANF AC, or any of the Recognized Registration Authorities that form the National Proximity Network, may request the revocation of a certificate if they knew or suspected the private key associated to the certificate 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 Maximum processing time of the revocation request

As defined in the CPS of ANF AC.

4.8.6 CRL lists verification requirements

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

4.8.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.8.8 On-line verification availability of the revocation

ANF AC 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 3100 (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 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 Lists

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) N° 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 Provisions

9.1 Fees

As defined in the CPS of ANF AC.

9.2 Financial liability

As defined in the CPS of ANF AC.

9.3 Confidentiality of information

As defined in the CPS of ANF AC.

9.4 Privacy of personal information

As defined in the CPS of ANF AC.

9.5 Intellectual property rights

As defined in the CPS of ANF AC.

9.6 Obligations and guarantees

As defined in the CPS of ANF AC.

9.7 Disclaimers of guarantees

As defined in the CPS of ANF AC.

9.8 Limitations of liability

As defined in the CPS of ANF AC.

9.9 Interpretation and execution

As defined in the CPS of ANF AC.

9.10 Management of the CP

As defined in the CPS of ANF AC.

