Certification Practice Statement (CPS)

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

Security Level

Public Document

Important Notice

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

Telephone: (+356) 2299 3100

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

Index

1 Introduction

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

This document is ANF AC's Certification Practice Statement (CPS).

The Public Key Infrastructure (PKI) of ANF AC in the process of adaptation the legal framework of Regulation [EU] 910/2014 of the European Parliament and Chapter 426 Electronic Commerce Act and standard ETSI EN 319 412 *(Certificate Profiles)*. ANF AC's PKI is in conformity with the standards ETSI TS 101 456, *(policy requirements for certification Authorities issuing qualified certificates),* ETSE 101 862 *(Qualified Certificate Profile),* RFC 3739 *(Internet X.509 Public Key Infrastructure: Qualified Certificates Profile).* Also, in accordance with ETSI standard TS 102 042 v.2.1.1 Policy Requirements for Certification Authorities issuing public key certificates) and Chapter 426 Electronic Commerce Act.

This CPS details the general terms and conditions of ANF AC's certification services in relation to the management of specific information related to the creation and verification of electronic signatures and certificates; conditions applicable to the application, delivery, use, suspension and extinction of certificate usage; technical and organizational security measures; information mechanisms and profiles of certificate usage; and especially the checking processes to which data provided by applicants is subjected in order to establish its veracity. The CPS is also the security document used to support personal data protection legislation

This CPS includes a section which answers all security regulation queries. It constitutes a general compendium of rules applicable to ANF AC's role as a Certification Services Provider. However, ANF AC handles various types of certificates, and so for each there are specific Certification Policies (PCs). As a consequence, applicants for any type of certificate must have read and understood this CPS and the CP relevant to the certificate in question in order to be able to apply for and use it correctly. Any regulations stipulated in the specific Certification Policies take preference over this CPS.

This DPC is a general compendium of rules applicable to all ANF AC's activity as a Certification Services Provider. However, ANF AC emits various types of certificates, for which there are specific Certification Policies (PC). Accordingly, the applicant of any kind of certificate must know the CPS and CP in each case that is applicable for using the certificate correctly. What is stipulated in each specific Certification Policy shall prevail over the regulations stated in this CPS.

In this CPS and the CP related, it is established the delimitation of responsibilities of the various parties involved and the limitations of these for possible damages is established.

ANF AC is certified according to EV Webtrust under the guidelines of issuance and management of Extended Validation SSL certificates *(CA / Browser Forum guidelines for the issuance and management of*

extended validation certificates). These guidelines defined by the CA / Browser Forum specify the minimum requirements that need to be applied by the Certification Authorities in order to issue SSL-EV certificates with the aim of providing reliability in the identification and control of the identity of the accessed services.

ANF AC is up to date to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published in https://www.cabforum.org. In the event of any inconsistency between this document and the requirements stated in the Baseline, these requirements take priority over this document, as long as these requirements do not conflict with legal requirements.

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

1.1 Presentation

ANF AC, as a Certification Service Provider, manages a Public Key Infrastructure, in order to provide the following services:

- **Certification Services**, providing qualified and nonqualified certificates without legal consideration of the qualified certificates.
- **Timestamp Authority** (henceforth, TSA) **Services**, which guarantees users that some information existed at a specific moment in time.
- **Validation Services** which allows its users and trusted third parties to benefit from verification at the origin and checking of certificates based on OCSP (Online Certificate Status Protocol), as well as free access to CRL and ARL revocation lists.
- **Maintenance Service of electronic signatures**, which aims to extend the data reliability of electronic signatures beyond the technological validity period.
- **Certified electronic delivery service** that allows the transmission of data between third parties by electronic means.
- **Authentication Service for websites**, issuing a certificate of authentication of a website.
- **Custody Service and provision of signature generation data**, certified in Cloud.
- **PKI enabled services.** It is based on a set of electronic certifications, products and public key-based instruments for the end user, as well as computer components and techniques for developing applications using electronic signatures.
- **Training Services.** Specialized courses and workshops for knowledge transfer on electronic signatures, their applications, benefits and potential risks.
- **RA Services Manager**. This is an International Proximity Network of Recognized Registry Authorities, that ANF AC offers to users in order to process license applications and deliver to subscribers, in person, electronic signature instruments.

In developing its activities, ANF AC has implemented a management system for information security for operation processes and maintenance of the infrastructure, issuance, validation and revocation of electronic certificates in accordance to the ISO 27001 standard.

It is an objective of ANF AC, within the adjustment period established by eIDAS, that all certificates issued, meet all the requirements of the Regulation eIDAS and European standards ETSI EN 319 412 "Certificate Profiles", without using proprietary OIDs in order to facilitate adaptation to profiles.

Specifically, they must contain QcStatements extensions according to ETSI EN 319 412-5 "Certificate Profiles. Part 5: QcStatements".

1.2 Identification

ANF AC uses OID's according to the ISO / IEC 9834-1:2005 and ITU-T Rec X.660 standards (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs). 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-).

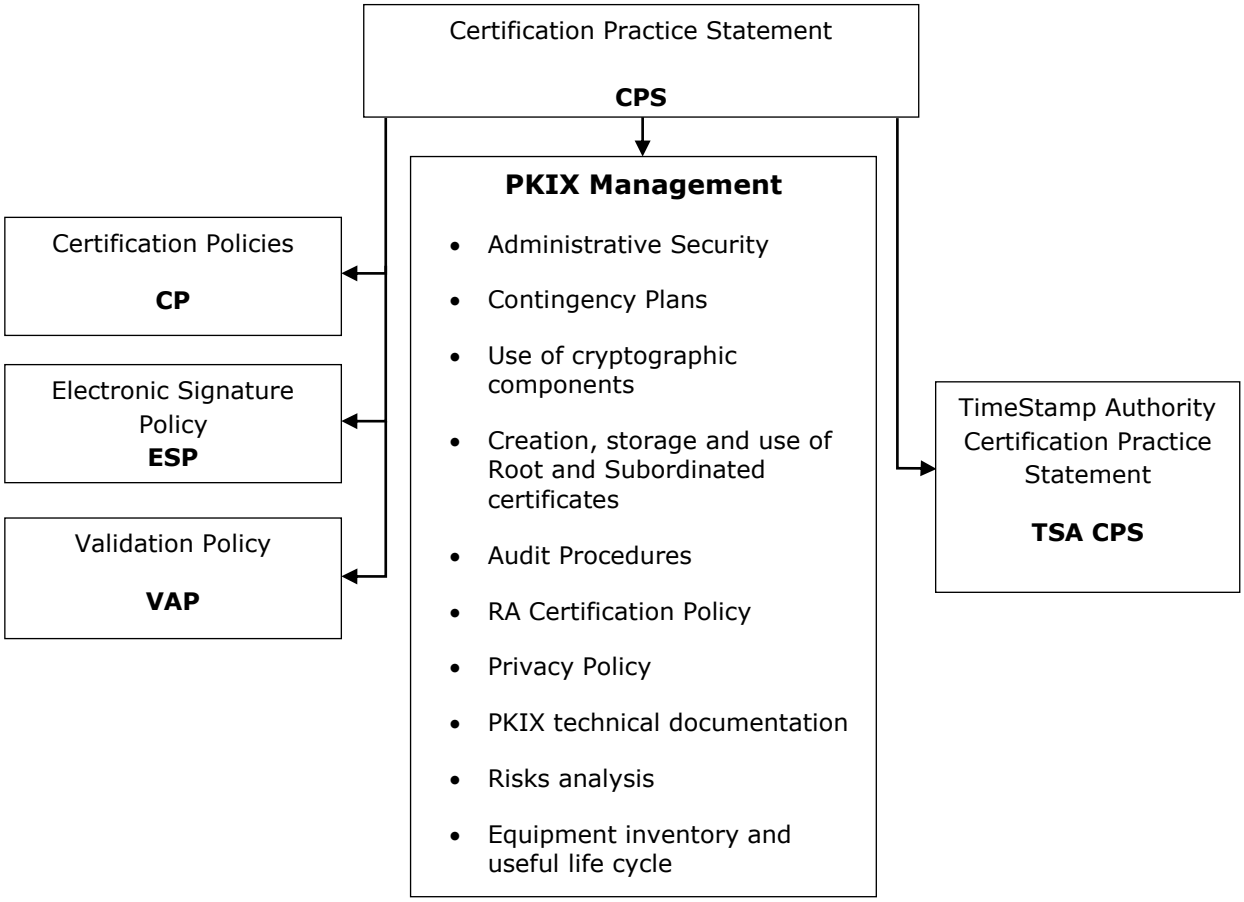
In order to identify each type of certificate issued in accordance with the present Certification Practice Statement, and especially with the Certification Policy to which it is subjected, an object identifier (OID) is individually assigned. This OID appears in the corresponding section of the Certificate Policies. This OID always begins with the following sequence:1.3.6.1.4.1.18339.

1.2.1 Document title

This document is known as ANF AC's Certification Practice Statement, known internally by its acronym "CPS".

1.2.2 Document structure

The document structure of the policies, the CPS and other documents related to ANF AC-managed certification services is laid out as in the following scheme:



1.2.3 OID identifiers

The significance of the OID sequence "1.3.6.1.4.1.18339.1.9.1.1" is the following:

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- ANF AC MALTA, LTD. (18339)
- Certification Practice Statement (1.9.1.1)

1.2.4 Specifications

Document name	Certification Practice Statement of ANF AC
Version	1.01
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.1.9.1.1
Publication date	June 17th, 2016
Expiration date	Not applicable
Location	http://www.anfacmalta.com/en/documents/

This document does not specify any aspects of the various certification, validation or time stamp practices and policies implemented by ANF AC to provide certification services. Said specifications are developed in the corresponding documents, taking this CPS as a general application framework.

Conditions of use, limitations, responsibilities, properties and all other information considered to be specific to each type of certificate is reflected in the various Certification Policies to the certificate is subject to.

The publication of a new document entails the repeal of the former. An X.Y version specifies the version number, which sequentially identifies the different versions that have been published.

1.3 Community

1.3.1 Intervening persons and entities

- Certification Entity
    - Certification Services Provider
    - PKI Governing Board

- Certification Authority
    - Root Certification Authority
    - Intermediate Certification Authorities
- Issuance Report Managers
- Certificates Issuance Managers
- Validation Authority
- Time Stamp Authority
- End entities
    - Applicants
    - Those responsible of the Certificates
    - Subscribers
    - Trusted Third Parties

1.3.1.1 Certification Entity

1.3.1.1.1 Certification Services Provider

ANF AC MALTA, LTD. (hereinafter, ANF AC) is a corporate entity, duly registered with the Registry of Companies in Malta with registration number C75870 and VAT number MT 23399415. It is the Certification Service Provider issuing public certificates to those who apply this Certification Practice Statement.

1.3.1.1.2 PKI Governing Board

The Governing Board of the ANF AC Public Key Infrastructure is the body that manages the PKI and is responsible for the approval of this Certification Practice Statement, as well as any possible changes in it.

1.3.1.2 Certification Authority

ANF AC's PKI is composed of various Certification Authorities. These Certification Authorities are as listed below:

1.3.1.2.1 Root Certification Authorities

This is the root entity whose public key certificate has been self-signed and which, within the hierarchy of certification, has the capacity to issue certificates to other intermediate certification authorities.

ANF AC MALTA, LTD. currently has the following Root Certification Authorities:

- Root Certificate with CN = **ANF Trusted Root CA** with serial number 01 55 5e f7 ff c6 which expires on June 12th 2036.

The identification data of this Root Certificate is:

Serial Number	01 55 5e f7 ff c6
Subject	CN = ANF Trusted Root CA SERIALNUMBER = MT23399415 OU = ANF Malta Certification Authority O = ANF AC MALTA, LTD C = Malta
Validity Period	From 2016-06-17 to 2036-06-12
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Fingerprint	0f ee a8 e7 96 5a a5 63 f3 9c 97 9b 23 b1 14 38 92 21 78 d0

1.3.1.2.2 Intermediate Certification Authorities

They are entities within the certification hierarchy, which issue end-entity certificates, and whose public key certificate has been digitally signed by the Root Certification Authority.

ANF Trusted Root CA, which expires on 2036, currently has the following Intermediate Certification Authorities:

- **ANF Trusted ID CA1**

  With SHA-256 algorithm:

Serial Number	01 55 5f 09 41 71
Issuer	CN = ANF Trusted Root CA SERIALNUMBER = MT23399415 OU = ANF Malta Certification Authority O = ANF AC Malta Ltd C = MT
Subject	CN = ANF Trusted ID CA1 SERIALNUMBER = MT23399415 OU = ANF Malta Identity Authority O = ANF AC Malta Ltd C = MT
Validity	From 2016-06-17 to 2026-06-15
Public Key	RSA (4096 Bits)

Signature Algorithm	Sha256RSA
Fingerprint	d9 69 56 39 5a 72 cf d6 d0 bf c6 f8 4b be 40 0b 9c 29 35 b2

Intermediate CA **ANF Trusted ID CA1** issues end-entity certificates.

- **ANF Trusted PA CA1**

With SHA-256 algorithm:

Serial Number	01 55 5f 1ª 34 c7
Issuer	CN = ANF Trusted Root CA SERIALNUMBER = MT23399415 OU = ANF Malta Certification Authority O = ANF AC Malta Ltd C = MT
Subject	CN = ANF Trusted PA CA1 SERIALNUMBER = MT23399415 OU = ANF Malta PA Authority O = ANF AC Malta Ltd C = MT
Validity	From 2016-06-17 to 2026-06-15
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Fingerprint	2f 73 31 81 90 f4 80 f1 f9 4d 7d 70 09 f3 74 95 ab a7 17 0f

Intermediate CA **ANF Trusted pa CA1** issues end-entity electronic certificates for Public Administrations.

- **ANF Trusted EV CA1**

With SHA-256 algorithm:

Serial Number	01 55 5f 13 98 a1
Issuer	CN = ANF Trusted Root CA SERIALNUMBER = MT23399415 OU = ANF Malta Certification Authority O = ANF AC Malta Ltd C = MT

Subject	CN = ANF Trusted EV CA1 SERIALNUMBER = MT23399415 OU = ANF Malta Extended Validation Authority O = ANF AC Malta Ltd C = MT
Validity	From 2016-06-17 to 2026-06-15
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Fingerprint	23 e0 e4 61 98 09 44 10 24 14 31 2f 8e 6e 4c d5 38 78 61 ad

Intermediate CA **ANF Trusted EV CA1** issues electronic technical certificates for authentication services SSL, SSL EV, Encryption and Code Signing.

- **ANF Trusted PKI CA1**

  With SHA-256 algorithm:

Serial Number	01 55 5f 1d f5 20
Issuer	CN = ANF Trusted Root CA SERIALNUMBER = MT23399415 OU = ANF Malta Certification Authority O = ANF AC Malta Ltd C = MT
Subject	CN = ANF Trusted PKI CA1 SERIALNUMBER = MT23399415 OU = ANF Malta PKI Authority O = ANF AC Malta Ltd C = MT
Validity	From 2016-06-17 to 2026-06-15
Public Key	RSA (4096 Bits)
Signature Algorithm	Sha256RSA
Fingerprint	79 f7 e3 bb 94 dd f1 68 41 83 d3 d1 d0 ff 48 5b 9d a8 3c 7c

Intermediate CA **ANF Trusted PKI CA1** issues electronic certificates for the management and administration of the PKI of ANF AC.

1.3.1.3 Registration Authorities.

1.3.1.3.1 Recognized Registration Authorities

These are legal or natural persons to whom ANF AC has given the necessary technology to carry out the functions of a registration authority after a process of training and agreeing to an agreement in which they assume all appropriate responsibilities and a collaboration agreement.

Registration entities carrying out these functions require natural person operators who have carried out an official training designed by ANF AC called "Operator RA" and have passed it, in order to be prepared for the official operating functions of a Recognized Registration Authority. The Registration Authority operators are legal persons under the supervision, control, management and operate under their own exclusive responsibility.

ANF AC entrusts these officially recognized operators with identifying and checking the personal conditions of certificate applicants.

With this aim in mind, they are in charge of guaranteeing that:

- The application is made in person by the persons involved in the application, custody and use of the certificate requested.
- The documents provided for identifying and verifying the credentials of the applicants must be originals and thorough enough to complete the application.
- To the extent of their possibilities, they ensure that:
    - the application is made with the free will of the applicant and any other intervening parties without coercion;
    - the applicants and any other intervening parties are of legal age and have the mental capacity to apply;
    - the applicants and any other intervening parties have sufficient intellectual capacity to assume the responsibility and correct use of the certificates and associated technology.
- Deal with requests for information and clarify doubts on any questions with respect with the forms.
- Make the CPS, associated Certification Policies, Electronic Signature Policy and service rates available to the applicant and any other intervening parties involved in the application, as well as information related with the renewal and revocation processes: causes, obligations and procedure.
- Inform the applicants of the exact conditions for the use and limitations of use of the certificate.
- Verify that the information owner gives his consent to the use of the data and knows how the information will be used and stored in the file kept by ANF AC, as well as the rights to access, correction, cancellation and opposition and how to exercise said rights.
- Physically give the Cryptography Device to the applicant as well as other utilities used for:
    - The generation of the key pair, the activation data and the request certificate;
    - The generation of the activation data;

- The generation of the request certificate;
- Giving a connection to the trusted ANF AC servers through a secure communications protocol;
- The certificate download when it has been issued, the generation of electronic signature;
- The electronic signature and the making of verification processes;
- The authentication processes faced with computer applications, and encryption processes;

This device gives the user access, storage, control and management of their certificates and private keys. As such, its destruction implies the destruction of the certificate and its keys.

- Deliver to the applicant their identification certificate, electronically signed by the RA operator.
- Check that all documentation submitted by the applicant, and anyone involved in the application process, is original, obtaining a copy of the same which is signed electronically by the RA operator. This documentation, along with other information collected and compiled by the operator RA (application form, statement of identity, biometrics...etc.), form the "application file". The application file is sent by electronic means to trusted servers of ANF AC.

  The process of digitalization and transmission of the application is made by the "AR Manager" application of ANF AC, which guarantees the security and privacy of information. AR Manager incorporates the following security measures for the correct completion of the forms:

  - It verifies that e-mail addresses given are properly formatted. And they are checked for validity.
  - It disallows the e-mail address of the certificate to be the same as the AR Operator. It verifies that the identifications indicated are properly formatted.
  - It verifies that the Identification card numbers indicated are properly formatted.
  - It verifies that the VAT numbers indicated are properly formatted.
  - It verifies that the bank accounts listed are properly formatted.
  - It verifies that the minimum documents are attached, according to the type of certificate requested.
  - All alphanumeric fields are capitalized, except for electronic mail addresses and URLs.
  - Disallows the introduction of blanks at the beginning or end of any displayed value, as well as several blank spaces in a row.
- At the end of the application process, the AR Operator generates and signs the ID Act, transferring it to the Electronic Signature Cryptographic Device, and generating in paper the Activation Letter. All of it is given to the certificate applicant. These documents contain:

  - The ID Act features all the structured information that will enable the subscriber to make the request certificate PKCS#10. This Act is previously encrypted with double key.
  - The Activation Letter contains one of the passwords necessary to decipher the Identification Act. The second password is sent by e-mail to the account given in the application.

- Based on the accredited data, they proceed to:
    - Complete the application forms and the contract for the provision of certification services.
    - Print these documents, which will be signed by hand by the operator of the Registration Authority who performs the process and for the requesting user; one of these documents is the Application Form.
    - Submit to ANF AC all the documentation for the processed application.
    - Generate the ID Act.

ANF AC has launched a technological renovation plan that includes the addition of new identification tools, specifically:

- Image capture of the applicant.
- Capture of applicant's fingerprints.
- Electronic ID reader which incorporates authenticity validator.

Those RA already equipped with these instruments, assume the obligation of carrying out the corresponding processes of biometric data capture and validation of electronic ID cards, provided formal user authorization to process and transmit this information to Trusted Servers of ANF AC.

Once documents are formalized, the applicant must have been given:

- Signature Creation Data Generation Device.
- Electronic Signature Creation Device.
- Verification Device.
- ID Act which allows you to generate your "request certificate".
- Activation Keys record.

The application form is a document in which the applicant agrees to an explicit statement of his knowledge on the use of Electronic Signature Device and Digital Certificate and its duties, limitations and obligations as a user. The obligations referred to are:

- Generating the signature creation data without third party mediation, and that only the user knows the activation password.
- Understanding the obligations of keeping data signature creation and activation password.
- Knowing the means for reporting the loss or potential misuse of certificate data and electronic signature, as well as the obligation to revoke the certificate if that happened.
- Knowing how to use the device certification that has been delivered.

Each Certification Policy associated with this CPS incorporates the corresponding application form.

In the case of delivery of a cryptographic device that incorporates biometric reader, the Recognized Registration Authority must ensure that, in its presence, the applicant proceeds to identify itself through the device with his/her fingerprints. By this method the device will be activated and customized. Only the subscriber may, after undergoing appropriate biometric verification, activate the certification system.

It should also require, prior to the execution of the request for issuance of the certificate, a lecture on the applicants Rights and Obligations, informing him about the doubts that he may have. It cannot formalize the request to issue the certificate until the applicant believes it has a full understanding of the texts. With the signing of the license application, the applicant acknowledges that he understands and accepts all the rights and obligations set forth in this PKI.

In any case, if the operator of the RA estimates that the consultations held by the applicant are outside the scope of its knowledge or obligations, or it fails to resolve the doubts that arise, he/she will instruct the applicant to contact the Customer Office of ANF AC, which will freely assist and provide the advice required.

The RA assumes the obligation to revoke the certificates processed, or to deny a pending certificate whenever:

- It is known that the circumstances of the owner or legal representative, if any, have changed.
- It is known that there has been a mishap affecting the safety of signature creation data.
- In any case where it considers that its validity can adversely affect the reliability of ANF AC PKI, its use is not framed in good faith, or it is used to the detriment of third parties or in illegal operations.

The endpoints that the RA will follow on the documentation provided by the applicant to prove identity or other data to be included in the certificate will be those normally accepted in law. The Recognized Registration Authority always requires the physical presence of the applicant. The RA will always require the physical presence of the applicant.

All representations made by the RA are electronically signed by operators who perform them, thus taking full responsibility for the process.

The RA has the authorization to charge fees of identification, application, activation and inclusion of attributes in the requested certificate.

The final assessment of the adequacy or otherwise of the investigation carried out by the RA, as well as the documents provided, will be always run by staff from ANF AC.

Once the certificate is issued, the Registration Authority receives an acknowledgment of the issuance via e-mail.

1.3.1.3.2 Collaborating Registration Authorities

These are persons who, in accordance with legislation in force, have the powers of a public notary.

1.3.1.3.3 Trustworthy entities

Other entities in the view of this CPS, have the capacity to determine the identity, capabilities and freedom of action of the applicants. Their intervention will be carried with physical presence of the applicant, comparing original documents with copies thereof provided by the user, or information included on processing forms.

The applicant will sign on paper the processing forms. The Trustworthy Entity will issue and sign a Certificate of Proof of Life. The original documentation shall be submitted to the Head of Issuance Report Manager (IRM).

The Issuance Report Manager will assess the adequacy of the capacity of the Trustworthy entity based on their prestige, independence and prior relationship it may have with the user. It can order new managements, inquiries or even reject the processing performed because of insufficient guarantees.

The intervention of Trustworthy Entities is limited to the renewal process of electronic certificates which have passed the period of 5 years or not from the initial identification process.

1.3.1.4 Issuance Report Managers

These are staff incorporated to the ANF AC Legal Department, responsible for checking the documentation provided by the Registration Authorities. They determine whether the documents are sufficient or not, they check the reliability of the information, and, if they consider it necessary, order further investigations.

The Issuance Report Managers determine the need for completing these checks in each case through telecommunication consultations directly with registries, or through third party services.

The Issuance Report Managers' responsibilities are to:

- Ensure that the certificate application contains verifiable and complete information.
- Check that the application meets all requirements in the corresponding Policy according to the type of certificate requested.
- Check that documents have been signed, and that all formalities demanded by this CPS and its corresponding certification policies have been met.
- Analyze powers of attorney and other public documents.
- Verify that information contained in the certificate is exact and that no typing errors have been made.
- Verify that all information required has been included and, if there is any information which is not required, that the applicant authorizes its inclusion in the certificate.
- Apply the corresponding cryptographic verification process on the requested certificated to check the integrity of the certificate's contents and that the signing party is in possession of the signature creation details.

Based on all the work done, the Issuance Report Managers decide:

- To issue the certificates, generating and signing a favorable issuance report, or
- refuse the issuance, generating an unfavorable report, or
- requesting further accrediting documents or the signature of complementary certificates.

1.3.1.5 Certificate Issuing Managers

There are a minimum of three operators who have the capacity to access and activate ANF AC certificate issuing devices.

To activate the issuance service, the presence of at least two of these operators is required.

1.3.1.6 Validation Authority

A Validation Authority is a Certification Services Provider which provides certainty on the validity of electronic certificates.

ANF AC is a Validation Authority (VA) which acts as a trusted third party, validating electronic certificates.

ANF AC manages an IT system formed by a combination of Trusted Servers which provides information on the current state of all of ANF AC's issued certificates.

These servers are given the name of OCSP Responder and answer validation requests through the Online Certificate Status Protocol (OCSP). They determine the current status of an electronic certificate and the entire trust chain, issuing signed validation report. The repositories accessed by OCSP Responder servers are constantly updated and comply with the IETF RFC 6960, Online Certificate Status Protocol Algorithm Agility.

OCSP requests can be answered 24/7/365 completely free. These requests must be made in accordance with IETF RFC 2560. This validation process is complementary to the publication of the Certificate Revocation Lists (CRLs) web service.

1.3.1.7 Time Stamp Authority

A Time Stamp Authority is a Certification Services Provider which provides certainty about the existence of certain electronic documents before a given moment in time. The Time Stamping Authority signs the time stamp of the time, along with the hash of the associated document.

ANF AC is a Time Stamp Authority (TSA) which manages an IT System formed by a combination of Trusted Services whose time system is synchronized with a safe time source.

These servers are given the name Time Stamp Units (TSU), and their function is to place time stamps on requested forms made by ANF AC users. As such, they allow determining the existence of a certain object at a certain time.

1.3.1.8 End entities

As per this Certification Practice Statement and the various Certification Policies, the end entities of ANF AC's certification system are the following:

- Applicant
- Responsible of the certificate
- Subscriber
- Trustworthy third parties

1.3.1.8.1 Applicant

These are the natural persons who apply for a certificate to be issued, either themselves or representation third party.

If a third party representative is chosen, this representative must be given sufficient legal power and, if the representative is a legal person, this power must be written in the corresponding registry.

1.3.1.8.2 Subscriber

Subscriber shall have the status of the certificate holder, which is the sole owner of the key pair (public and private) associated with it.

The personal identity is linked to data creation and verification of signature, electronically signed with a public key certified by ANF AC.

The subscriber assumes full responsibility for the use of the signature creation data, even in the event that a third party has transferred the custody and management of their use.

1.3.1.8.3 Responsible of the certificate

These are the natural persons who are expressly authorized by the subscriber to hold and make use of the signature creation information.

This is only authorized in certificates whose Certification Policy expressly recognizes this.

1.3.1.8.4 Trustworthy third parties

In general, they are all natural or legal persons, entities, organizations, Public or Corporate Administrations which are voluntarily trusted in these certificates, in the electronic signatures generated by them, and in the authentication processes made by the application of this PKI.

These "Trusted third parties" must complete public key operations satisfactorily to be trusted by the certificate, such as assume the responsibility for verifying the status of the certificate, using means described in this CPS and the corresponding certification policy.

1.4 Use of the certificates

Certification Policies corresponding to each type of certificate issued by ANF AC are those documents in which the uses and limitations of each certificate are specified and published in

http://www.anfacmalta.com/en/documents

However, the permitted and prohibited uses of the certificates issued by ANF AC are established in the paragraph below.

1.4.1 Appropriate uses

1.4.1.1 Qualified certificates

On the employment of qualified certificates:

- The electronic signature qualified certificates ensure the identity of the subscriber and the holder of the private signature key. The intervention of secure signature creation devices are ideal for providing support to electronic signature as this allows the electronic signature to have the same legal effects as the handwritten one without having to meet any additional requirements.

- Qualified certificates can also be used, if so defined in the type of certificate, to sign authentication messages, client challenges including SSL or TLS, Secure Email S/MIME encryption without key recovery, or other. This electronic signature has the effect of guaranteeing the identity of the signer of the certificate signature.

In order for the certificate to be deemed as qualified, it must have been issued with this indication. The Certification Policy specifies how this qualification shall be noted. Qualified certificates also follow technical standard ETSI TS 101 456 by the European Telecommunications Standards Institute.

1.4.1.2 Non-qualified certificates

On the employment of non-qualified certificates:

- Non-qualified certificates ensure the identity of the subscriber and, if applicable, the holder of the signature key.

- Non-qualified certificates can also be used, if so defined in the type of certificate, to sign authentication messages, client challenges including SSL or TLS, Secure Email S/MIME encryption without key recovery, or others. This electronic signature has the effect of guaranteeing the identity of the signer of the certificate signature.

- Additionally, these certificates can support various forms of authentication and electronic signature. These certificates follow the technical standard ETSI TS 102 042, European Telecommunications Standards Institute.

These certificates follow the technical rule ETSI TS 102 042 by the European Telecommunications Standards Institute.

1.4.2 Scope of use of certificates

Regarding The scope of use, the following situations are considered:

- Certificates issued by ANF AC and directed to the general public, private companies and corporations, and intended to be used by subscribers for any use not prohibited. The user should always respect the limitations set in the certificate or in the Certification Policy to which it is subjected, assuming, and thereby accepting the limitations of liability stated by the issuer in the certificate itself, in this CPS and the corresponding CPs.

- Certificates issued by ANF AC and directed to persons connected with public administration bodies, or the scope of the powers of the administrative body and the position or office held in a Public Administration. Key holders must use these certificates to the uses identified in the application, and always within the limits of use specified in former paragraph a).

Specifications on the scope of use of each certificate should be consulted in the Certification Policy specific to each certificate.

1.4.3 Limits on the use of certificates

Certificates must be used for their proper function and purpose set, and may not be used in other functions and for other purposes. Similarly, the certificates should be used only in accordance with the applicable law, especially considering the import and export restrictions on cryptography in each moment.

Certification Policies for each type of certificate can determine additional limitations and restrictions on the use of certificates.

1.4.4 Prohibited uses

Certificates issued by ANF AC and its VA or TSA services are to be used exclusively for the aims specified in the corresponding Policies, arranged by the guidelines in force, taking into account any cryptographic material import and export restrictions which may exist at any moment.

Apart from in the cases specified in each Policy, certificates may not be used to act as a Registration Authority, Certification Authority, to sign public key certificates of any kind, Certificate Revocation Lists (CRL), OCSP validation, Digital Time Stamps, or for any validation or signing service.

Certification Policies corresponding to each type of certificate specifies the limitations and other restrictions of the use of certificates. This CPS is not used to specify said limitations and restrictions.

Certificates are not designed or can be allocated to control equipment from dangerous situations or for uses requiring fail-safe performance, such as the operation of nuclear facilities, navigation systems or air communications, or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage, neither is authorized it use or resale for such uses.

Certification Policies for each type of certificate can determine additional prohibitions on the use of certificates.

1.5 Certification Entity contact details

1.5.1 Certification Services Provider

Name	ANF AC MALTA, AC
E-mail address	info@anfacmalta.com
Address	B2 Industry Street, Qormi, QRM 3000
Locality	Qormi (Malta)
Postcode	QRM 300
Telephone number	(+356) 2299 3100

1.5.2 PKI Governing Board

Name	PKI Governing Board
E-mail address	juntapki@anfacmalta.com
Address	B2, Industry Street, Qormi, QRM 3000
Locality	Qormi (Malta)
Postcode	QRM 3000
Telephone number	(+356) 2299 3100

1.6 Definitions and acronyms

1.6.1 Definitions

Activation data (PIN): Secret key which the subscriber uses to activate signature creation data.

Applicant: Natural person who requests a certificate for himself, while representing a third party, or for an IT component.

Authentication: The procedure of checking the identity of an owner or applicant of an ANF AC certificate.

Authority Revocation List (ARL): List which exclusively includes all revoked or suspended CA intermediate or subordinate certificates (not including expired ones).

Certificate Revocation List (CRL): List which exclusively includes all revoked or suspended end-entity certificates (not including expired ones).

Certificate serial number: Unique integer number unequivocally associated with a certificate issued by ANF AC.

Certification Services Provider (CSP, CA): Natural or legal person which issues electronic signatures or loans other services in relation with the electronic signature.

Device: An instrument which is used to apply signature creation information.

Directory: Information store which follows the ITU-T X.500 standard.

Electronic certificate: A certificate signed electronically by ANF AC which links signature verification data (public key) to an owner and confirms their identity.

Hash function (hash or digital fingerprint): Operation run on a group of data of any size such that the result is another group of data of a fixed size, independent of the original size, which has the property of guaranteeing the integrity of the original data and making its falsification impossible.

Identification: The procedure of recognizing the identity of an owner or applicant of an ANF AC certificate.

IT component (or component): Any software or hardware devise suitable for using electronic certificates.

PKCS#10 (Certification Request Syntax Standard): Standard developed by RSA Labs, internationally accepted, which develops the syntax for a certificate request.

Public key and private key: ANF AC's PKI cryptography is based on asymmetrical cryptography. This uses a key pair: whatever is encrypted by one can only be decrypted by the other, and vice versa. One of these keys is called public is kept in the electronic certificate while the other is called private and is kept by the certificate's owner.

Public Key Infrastructure (PKI): Group of persons, policies, procedures and IT systems necessary for providing authentication, encryption and integrity services through the use of public and private key encryption, and electronic certificates.

Qualified certificate: A certificate issued by ANF AC as a Certification Services Provider which complies with the requirements of identifying the identity and checking other circumstances of the applicants and regarding their reliability and the guarantee for the certification service provided.

Qualified electronic signature: Advanced electronic signature based on a qualified certificate and generated by a secure signature creation device.

Security Hardware Cryptographic Module: Hardware module used to carry out cryptographic actions and securely store keys.

Session key: Key which establishes encryption for communication between two entities. The key is established specifically for every communication or session; its lifespan lasts until this communication or session ends.

Signature Creation Data (Private Key): Unique data, a private encryption key, which the subscriber uses to create electronic signatures.

Subscriber: Person or IT component for whom a certificate is issued. This certificate is accepted by the owner or another responsible person in the case of technical certificates.

Trusted hierarchy: Group of certification authorities which keep trust relationships and, as a result, a higher-level CA guarantees the reliability of one or more lower-level CAs.

Trusted third party: Person or entity, separate from the owner, who decides to accept and trust in a certificate issued by ANF AC.

X.500: Standard developed by UIT which defines directory recommendations. It corresponds with the ISO/IEC 9594-1 standard: 1993. This gives rise to the following recommended standards: X.501, X.509, X.511, X.518, X.519, X.520, X.521 and X.525.

X.509: Standard developed by UID which defines the basic format for electronic certificates.

1.6.2 Acronyms

AC / CA: Certification Authority.

AR / RA: Registration Authority.

ARL: Authority Revocation List.

AV / VA: Validation Authority.

CRL: Certificate Revocation List.

C: Country. Distinguished Name (DN) attribute of an object, within the X.500 directory structure.

CDP: CRL Distribution Point.

CEN: European Committee for Standardization (Comité Européen de Normalisation).

CN: Common Name. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

CPS / DPC: Certification Practice Statement.

CSR: Certificate Signing Request. A group of data containing owner information and a public key, all of which is self-signed by the owner using the relevant private key.

CWA: CEN Workshop Agreement.

DN: Distinguished Name. Univocal identification of an entry within the X.500 directory structure.

eIDAS: 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 and repealing Directive 1999/93/EC

ETSI: European Telecommunications Standard Institute.

HSM: Hardware Security Module, comply with the ISO 15408 standard: EAL 4 (or superior), in accordance to what is established in the CEN CWA 14169.

IETF: Internet Engineering Task Force.

LDAP: Lightweight Directory Access Protocol

O: Organization. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

OCSP: Online Certificate Status Protocol. This protocol allows online checking of an electronic certificate's status.

OID: Object Identifier.

OU: Organizational Unit. Distinguished Name (DN) attribute of an object within the X.500 directory structure.

PIN: Personal identification number. Password which protects access to a cryptographic card.

PKCS: Public Key Infrastructure Standards. PKI standards developed by RSA Laboratories and internationally accepted.

PKI: Public Key Infrastructure.

PKIX: A workgroup within the IETF with the aim of developing specifications related to PKI and the Internet.

PSC: Certification Services Provider.

RFC: Request For Comments (Standard issued by the IETF).

UUID: Universally Unique Identifier. Code used in software construction, standardized by the Open Software Foundation (OSF). It enables distributed systems to uniquely identify information without significant central coordination, avoiding name conflicts.

2 Publication and repository responsibilities

2.1 Repositories

To download Root CA certificates and Intermediate CA certificates:

- Web: http://www.anfacmalta.com/en/pki- ac/certificates.html

To access the Certificate Practice Statement:

- Web: http://www.anfacmalta.com/en/documents/

To access the Certification Policies:

- Web: http://www.anfacmalta.com/en/documents/

To access the Certificate Revocation Lists (CRLs)

- Web: http://www.anfacmalta.com/en/CRL/

2.2 Certification Entity information Publication

The ANF AC Publishing Service is a system which publishes all documents produced by ANF AC, relative to their digital certification services and complementary ones. It also publishes the certificates obtained by the entity and credentials that are available.

Access is always available on

http:/www.anfacmalta.com/en/documents

Through this service, ANF AC ensures the integrity of the information.

Access to this repository of documents is regulated in accordance to the level of security by which each document is classified as specified in the "Classification of the documents produced by ANF AC" of this CPS.

2.3 Publication and Notification Policy

Changes in the specifications or in the conditions of service shall be communicated by ANF AC to subscribers and relying parties through the website of ANF AC

http://www.anfacmalta.com/en/documents.

For 30 days, the website of ANF AC refers to changes related to the changed document or any annex document. After 30days, references are removed and all information is published in the appropriate repository.

2.3.1 Items not published in the Certification Practice Statement

The full list of components, subcomponents and elements that exist but that are confidential and not public, are those reported in this Certification Practice Statement, under the sections "Confidentiality of Information" and in "Classification of documents produced by ANF AC".

2.4 Approval of the publication

Final modifications as well as aspects related to publication and notification are approved by the PKI Governing Board, after checking the compliance with the requirements set herein.

2.5 Publication of status of issued certificates

ANF AC provides a fast and safe consultation service of the Registry of Issued Certificates. An updated system of certificates is maintained, which identifies the license and if they are valid or if their application has been suspended or expired.

In the publication of CRLs, safe and quick access to users and subscribers is guaranteed, as indicated in the relevant section of this CPS.

Unless expressly authorized in writing by the PKI Governing Board of ANF AC, it is prohibited to use any of these publishing services to provide validation services to third parties or to use the information for purposes other than as specifically authorized herein.

2.6 Frequency of updates

The Certification Practice Statement and Certificate Policies are published each time they are modified, unless the PKI Governing Board considers the update as minor, in which case it will publish an annex built to the respective DPC or affected policy, as stated in Section "Management of CPS and Certification Policies" of this document.

The certificates issued by the CA are published immediately following such issuance. ANF AC revoked certificates added to the relevant CRL within the period of time stipulated in the "Next Update".
OCSP queries are made on updating states.

2.7 Repository access control

ANF AC's Publishing Service has a security system that allows adequately control access to information as Document Classification and Operators Security Level. This system also prevents unauthorized persons from adding, modifying or deleting records of the Service, and protects the integrity and authenticity of the information stored, so that:

- Only authorized persons can make entries and changes.
- The authenticity of the information can be verified.
- The certificates are only available for consultation if the subscriber has formally given consent in the corresponding services agreement.
- Any technical change affecting the safety requirements can be detected.

ANF AC only allows access to classified information to people who are specifically authorized. We have implemented security measures that protect reasonable access to information, determining at each visit:

- Identity of the applicant
- Security Level accredited

Servers managed a Log system which:

- Manages an access log
- Manages denial of access log

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

All certificates contain a DN (Distinguished Name) X.500.

In all end-entity identity certificates, the Common Name field contains the full name of the certificate subscriber.

ETSI has developed European standards pursuant to the Mandate M / 460 from the European Commission to streamline standards around electronic signatures. The set ETSI EN 319 412 specifies the contents of certificates issued to natural personas.

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

The information used to define the identity and attributes of the signer of a certificate of natural person, without pseudonyms, is broken down into the following fields:

- "Subject", using the attributes commonName, surname (or givenName) and countryName. In the SerialNumber attribute it includes the ID of the signer.
- "Subject Alternative Names". No restrictions included.
- "Subject Directory attributes". No Subject field attributes are included.

In the event of a link or relationship with a corporation, for example, certificates of natural person legal representative of a legal person, it is established that the company's name may be included in the "organizationName" attribute and the VAT number in the "organizationIdentifier" attribute:

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

The Certification Policy for each certificate contains particular specifications determined thereon.

3.1.1.1 Issuer

This field contains the ANF AC identification which is the Certification Entity which signed and issued the certificate. The field cannot be left blank and always contains a Distinguished Name (DN).

A Distinguished Name is composed of a combination of attributes, consisting of a name or label and an associated value. In certificates issued by ANF AC, every single field of the Subject makes the Distinguished Name (DN).

The issuer of the intermediate CAs matches the Subject of the CA that issued the certificates.

3.1.1.2 Subject

This field contains the identification of the owner or subscriber of the certificate issued by the CA identified in the corresponding Issuer field. The field cannot be left blank and always contains a Distinguished Name (DN).

A Distinguished Name is composed of a combination of attributes, consisting of a name or label and an associated value. In certificates issued by ANF AC, every field of the Subject makes the Distinguished Name (DN).

The Certification Policy to which each certificate is submitted provides a detailed profile of each certificate issued by the Certification Service Provider.

3.1.2 Need for names to be meaningful

As defined in the Certification Policy to which the electronic certificate is submitted.

3.1.3 Interpretation of name formats

RFC 3280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile") states that all certificates issued on or after December 31, 2003 must use the UTF8 String encoding for Directory String all attributes in Issuer and Subject fields.

In certificates issued by ANF AC, the attributes of these fields are encoded in UTF8 String, except in Country and Serial number fields, which are encoded in Printable String according to its definition.

3.1.4 Uniqueness of names

The DN of the certificates must be unique. The use of every field of the Subject ensures the uniqueness of the DN.

Certification Policies may provide for the replacement of this uniqueness mechanism.

3.1.5 Resolution of name and brand conflicts

Applicants for certificates shall not include names in applications that may involve breach by the Subscriber of third party rights.

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

The conflicts of those responsible for the certificates that appear identified with their real name are solved by the inclusion in the distinguished name of the certificate, of the Identification Card of the person or other identifier assigned by the subscriber.

3.1.6 Recognition, authentication and role of trademarks

Distinguished names are the property of the people that support the relevant trade mark on them, in case it exists. If this fact is unknown, ANF AC uses the name proposed by the user under full liability.

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

3.2 Initial identity validation

3.2.1 Proof of private key possession

In the event that the key pair be generated by the certificate applicant, the possession of the private key corresponding to the public key used to generate the certificate is guaranteed through the sending of the Certificate Signing Request (CSR) in PKCS#10 format in which the signed public key through the associated private key is included.

This CSR is sent to ANF AC to be processed which will help detect errors in generation of the certificate and proves that the applicant is in possession of the key pair and with the capacity to use it.

3.2.2 Authentication legal person identity

Each Certification Policy establishes the authentication procedure of a legal person's identity. Generally, the following aspects are determined:

- Types of valid documents for identification.
- Identification procedure to be performed by the RA.
- Whether facial identification is needed.
- How to establish membership in a particular organization and sufficient legal powers of representation.

3.2.3 Authentication of individual identity

Each Certification Policy establishes the authentication procedure of a physical person's identity. Generally, the following aspects are determined:

- Types of valid documents for identification.
- Identification procedure to be performed by the RA.
- Whether facial identification is needed.
- How to report a possible representation on behalf of third.

3.2.4 Non-verified information about the applicant

Non-verified information is not included on certificates issued by ANF AC.

3.2.5 Verification of representation authority

The Issuance Reports Manager is in charge of verifying representation authority, determining its validity in public records where it needs to be inscribed, and confirming that it is sufficient.

3.3 Identification and authentication of key renewal requests

3.3.1 Identification and authentication for routine key renewals

Each Certification Policy establishes the authentication procedure of a subscriber's identity.

3.3.2 Identification and authentication for key renewals after revocation

Keys in revoked certificates cannot be renewed.

4 Certificate life-cycle operational requirements

This section establishes the operational requirements common to different types of certificates issued by ANF AC.

4.1 Certificate application

Once accredited the identity of the applicant before the Registration Authority, any applicant desiring a certificate must:

- Complete the application form with all required information. However, not all required information will be written on the certificate; it is only required for various obligations which ANF AC must meet to correctly issue the certificate and manage its PKI. This information will be kept confidentially by ANF AC in agreement with the Personal Data Protection legislation in force.
- Signing the corresponding certification provision document with ANF AC and paying the appropriate fees. The signing of the service provision contract assumes that the applicant accepts the certificate and all obligations and responsibilities specified in this CPS and in the corresponding Certification Policy.

A new "Issuance Request" will not be necessary in the case of issuances made as a result of a revocation due to a technical failure in the transmission and /or distribution of the certificate or its related documentation.

The data that identify the holder of the certificate keys in the application are contained in the required identification documents. This information is recorded accurately within length limits derived from the technical conditions set out in the certificate content.

Any material changes to the information contained in the certificate or completed documents to process the application, produced after the issuance of the certificate, must be communicated to ANF AC, as it can lead to a certificate revocation.

4.1.1 Who can submit a certificate application

Each Certification Policy specifies who can own a certificate and the documentation that must be submitted.

4.1.2 Registration of certificate applications

The Recognized Registration Authority will advise applicants on whether the requested certificates are adequate for the intended use and owner profile. The Recognized Registration Authority can authorize or reject the application.

Using technical means provided by ANF AC to Recognized Registration Authorities, the application is registered online, using the Trusted Servers of ANF AC.

In the event that there are no Recognized Registration Authorities involved, the certificate applicant assumes responsibility for processing, authenticating and registering the documentation to ANF AC, according to the procedure specified in the corresponding Certification Policy.

4.1.3 Verification of certificate applications

The Issuance Report Managers assume the responsibility of ensuring that the documentation provided by the applicants is sufficient, and of making the necessary checks to determine the truth of the information which is requested to be included in the certificate.

The Issuance Report Manager, based on the checks made, will issue a report to the applicant announcing the approval, rejection, or need for more documentation.

4.1.4 Time to process certificate applications

A maximum deadline of 15 days for certificate application has been established. ANF AC will not assume responsibility for any delays which may arise, but if the deadline is reached, they must inform the applicant of the causes for the delay, and the applicant has free choice to cancel the application and ANF AC must refund the applicant any fees paid.

4.2 Certificate issuance

The issuance of a certificate means the complete and final approval of an application by the Issuance Reports Manager. Depending on the type of certificate, the issuance may be made on a cryptographic device or software support.

4.2.1 Actions during certificate issuance

The Issuance Reports Manager issues an Act of conformity, which is incorporated in the certificate request sent by the applicant as well as the identification certificate issued by the Registration Authority intervened in the identification process. The subscriber is notified via signed e-mail of the conformity of the application.

These documents are automatically processed by the issuance service of ANF AC. This service performs safety checks of the integrity of the documents received, checks the consistency between them and their correspondence with the Certification Policy which the requested certificate is submitted. In case of compliance, ANF AC proceeds to the issuance of certificates.

Once the certificate is issued, ANF AC notifies the subscriber via signed e-mail, and proceeds to activate the computer mechanisms necessary for the certificate to remain enrolled in the corresponding repository and available for download. The subscriber, using the same e-signature cryptographic device used to generate the key pair and certificate request, can download it and install it.

For technical certificates (SSL, Electronic Seal, Administrative Offices, Application or Code Signing) ANF AC will deliver the certificate by a secure way (e.g., e-mail signed, physical delivery, etc.), to the certificate responsible.

ANF AC signs with its private key the public key certificates it issues.

4.2.2 Notification to subscriber of certificate issuance

ANF AC's cryptographic devices automatically establish secure connections to the trusted server which allows the automatic download of a certificate once it has been issued.

Moreover, a signed e-mail is sent to the applicant and subscriber of the certificate, reporting the issuance and publication of the issued certificate.

4.3 Certificate acceptance

4.3.1 Manner in which the certificate is accepted

Each Certificate Policy determines the method of acceptance. Generally, it is established that:

- The certificate acceptance is formalized by the applicant signing the Certification Services Delivery Contract, as written in the 4.1 section of this document. Moreover ANF AC will be able to request the perfection of the certificate acceptance requesting the applicant to sign a Certificate Reception and Acceptance Act. This requirement will have to be attended by the applicant within 15 days maximum. After that time, if the applicant has not attended it, ANF AC will be able to revoke the Certificate.
- In the corresponding CP, the acceptance procedure may be written in more detail or widened.
- ANF AC guarantees the correct functioning of the devices it provides and that they work in agreement with necessary characteristics. The subscriber has 7 natural days to check the certificate, the software and the cryptographic device.
- In the case of any technical problems (including, but not limited to, the certificate support not working, problems with program compatibility, technical error in the certificate, etc.) or errors in the data within the certificate itself, ANF AC will revoke the certificate and issue a new one within 72 hours maximum.

4.3.2 Publication of the certificate

ANF AC, once issued the certificate, proceeds to publish it in the repositories for this purpose.

4.3.3 Notification of certificate issuance to third parties

No notification is sent to third parties.

4.4 Rejection

Besides any potential Issuance Report Managers' decision to refuse an application, ANF AC also reserves the right to refuse the issuance or renewal of any certificate freely, whenever deemed appropriate.

A PKI system is developed within a framework of mutual trust and in relationships of good faith. Those persons who directly maintain or have maintained any type of conflict of interests with this certification service provision entity, or with the members of its Board, may not apply for any certificate issue nor have third parties apply for one on their behalf.

Persons belonging to or dependent on entities which are competitors to ANF AC may also not apply for certificates.

4.5 Pair of keys and use of the certificate

4.5.1 Private Key and certificate usage by the owner

The responsibilities and limitations of use of the key pair and of the certificate are established in the corresponding CP.

In general, the subscriber may only use the private key and certificate for uses authorized in the CP and in accordance with that written in the "Key Usage" and "Extended Key Usage" fields on the certificate.

After the expiration or revocation of the certificate, the owner will no longer use the private key.

4.5.2. Public key and certificate use by trustworthy third parties

Trusted third parties may only place their trust in certificates as specified in the CP and in accordance with that written in the "Key Usage" and "Extended Key Usage" fields on the certificate.

Third parties must complete public key operations satisfactorily to be trusted by the certificate, such as assume the responsibility for verifying the status of the certificate, using means described in this CPS and the corresponding CP.

4.6 Certificate renewal without key change

With sufficient notice, the user will be informed, through the e-mail address indicated on the electronic certificate that the certificate is close to its expiry date. This same e-mail will indicate the steps to follow for the renewal of the electronic certificate.

For requests of certificate renewal without key change, ANF AC, before issuing the new certificate, will ensure that these keys are still cryptographically reliable.

If they are found to be so, they will verify that all registered information is still current and valid and, if any information has changed, be verified, saved and confirmed by the subscriber that they are in agreement as specified in the corresponding section of this policy.

If the legal service provision conditions have changed since the previous issuance, ANF AC will inform the subscriber of this fact.

The procedure applicable to this renewal without key renewal requires the secure return of the cryptographic devices holding the keys before securely erasing the device and generating the new certificate.

The procedure applicable to this renewal without key renewal requires the previous existence of a certificate in force, that the keys to this certificate are cryptographically reliable for the new certificate, and that there is no suspected compromise of the subscriber's private key, or that of the certificate's owner.

In any case, the renewal of certificate is subjected to:

- The application being completed correctly and in time, following all instructions and rules established in ANF AC's CPS.
- ANF AC or the RA intervening in the application process having no certain knowledge of the concurrence of any reason for revoking the certificate.
- The application form completed referring to the same type of certificate originally issued.
- That the certificate to renew is valid in the moment of request.

If a period longer than 5 years has elapsed since the identification was made by physical presence of the applicant, a formalization of the request is required under a handwritten signature of the applicant, procedure performed with a physical presence of the person concerned and using sufficient original documentation to a Recognized RA, a Collaborating RA or a Trustworthy Entity.

Once the certificate renewal process is completed, the user will receive a notice in their Cryptographic Device that ANF AC has already issued the renewed certificate which can be downloaded to the device after introducing an activation PIN. The end-user can immediately make use of the renewed certificate.

4.7 Certificate renewal with key change

4.7.1 Circumstances for certificate renewal with key change

If the reason for renewing the certificate is:

- Compromised keys or loss of their reliability.

The renewal will always be made changing the keys.

When this application is made, all registered information will be checked to make sure it is still current and valid and, if any information has changed, be verified, saved and confirmed by the subscriber that they are in agreement as specified in the corresponding section of this policy.

If the legal service provision conditions have changed since the previous issuance, ANF AC or the Recognized Registry Authority will inform the subscriber of this fact.

4.7.2. Processing certificate renewal requests with key change

The procedure applicable to renewal of certificates is the same as that for issuing a brand new certificate. ANF AC checks for any errors or omissions on the application.

In any case, a certificate's renewal is subjected to:

- The application being completed correctly and in time, following all instructions and rules established in ANF AC's CPS.
- ANF AC or the AR intervening in the application process having no certain knowledge of any reason for revoking the certificate.
- The application form completed referring to the same type of certificate originally issued.
- The certificate being currently in force at the moment of application.

If it has been more than 5 years since the identification was made physically by the applicant, it is required to formalize the application required by handwritten signature of the applicant, a procedure performed physically by the person concerned and using sufficient original documentation before an Recognized RA, a Collaborator RA or a trusted entity.

4.8 Certificate modification

This is not authorized.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Revocations occur when a certificate loses its validity before it expires. Revocation is definitive. It is effected due to:

1. Circumstances which affect the information contained in the certificate:
    - Any information contained within the certificate is modified.
    - Any information on the certificate application is found to be incorrect, including when any verified information used to issue the certificate are altered or modified.
    - Any information contained within the certificate is found to be incorrect.
2. Circumstances which affect the security of the key or the certificate:
    - The private key, infrastructure, or systems belonging to the entity which issued the certificate are compromised whenever they affect the reliability of certificates issued after that incident.
    - Infraction, by the Certification Entity, of agreed requirements in certificate management procedures, established in the Certification Entity's CPS.
    - Compromise or suspicion of compromise, of the security of the subscriber's or owner's key or certificate.
    - Non-authorized access or use of the subscriber's or owner's private key by a third party.
    - Irregular use of the certificate by the subscriber or the owner, or lack of diligence in use of the private key.
3. Circumstances which affect the security of the cryptographic device:
    - Compromise or suspected compromise of the security device.
    - Loss or damage of the cryptographic device.
    - Non-authorized access of the subscriber's or owner's activation details by a third party.
4. Circumstances which affect the certificate subscriber or owner:
    - End of the relationship between certificate subscriber and owner.

- Modification or expiry of the underlying legal relationship or the cause which brought about the issuance of the certificated.
- Infraction by the applicant of the pre-established application requirements.
- Infraction by the subscriber or owner of the certificate of their obligations, responsibility and guarantees established in the corresponding legal instrument or in the corresponding Certification Entity's Certification Practice Statement.
- Sudden incapacity or death of the certificate subscriber or owner.
- Extinction of the legal person subscriber, the expiration of the authorization of the subscriber to the owner of the certification, or of the relationship between them.
- Application for the revocation of the certificate by the subscriber, in agreement with section 3.4 of this policy.

5. Other circumstances:

    - The expiration of the service of this electronic certification service provider, as written in section 4.16 of this policy.

The legal instrument which links the Certification Entity with the subscriber establishes that the subscriber must request the revocation of the certificate if they come into any knowledge for any of the circumstances mentioned above.

4.9.2 Who can request revocation

ANF AC or the Registration Authority that made the request may apply for the revocation of a certificate if they have knowledge or suspect the owner's private key has been compromised or any other determining fact which would require such action.

The subscriber, the legal representative who intervened in the application process and the certificate owner can also apply for the certificate's revocation.

4.9.3 Procedure for revocation request

Any entity which needs to revoke a certificate must apply to ANF AC or the Registration Authority which issued the certificate.

Any revocation application is to contain at least the following information:

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

The revocation application will be processed upon receipt. It must be authenticated in accordance with the requirements laid out in the corresponding section of this policy. Once the request is authenticated, ANF AC can immediately and directly revoke the certificate.

When a certificate is revoked, all of its instances are also revoked. The subscriber and the certificate owner will be informed when the status of the certificate changes. ANF AC will not reactivate a certificate once it is revoked.

The Cryptographic Device can also be checked to see if the certificate has been revoked.

All revoked certificates are included in all CRL publications until at least three months after its expiry date.

Each Certification Policy includes an example revocation form and the media available to complete the application in its Appendix III.

4.9.4 Time to process the revocation request

Revocation applications will be processed more or less immediately when knowledge as to the reason for the revocation is available, the applicant has been authenticated and their suitability has been checked. As such, there is not grace period associated with this process in which the revocation application can be annulled.

4.9.5 Obligation to consult the certificate revocation information

Trusted third parties must check the status of those certificates they wish to be entrusted to.

ANF AC provides a service to trusted third parties by which they can check the status of certificates base on the OCSP and also, at least, another form to access and download certificates revocation lists (CRLs) (in agreement with Section 2.7 "National identification and electronic signature scheme in public Administrations. Paragraph III: Additional general condition proposals in the AGE"). These two methods are available without any extra cost.

4.9.6 Frequency of publication of certificate revocation lists (CRLs) and ARLs)

In each certificate, the address of the corresponding CRL is specified through the CRL Distribution Points extension.

ANF AC publishes a weekly CRL, even when there are no changes or updates and therefore ensures published information is up-to-date.

Each CRL specifies the date and time when the next CRL will be published. This follows information specified in the RFC 5280 document.

ANF AC publishes an ARL every six months, even when there are no changes or updates.

4.9.7 Maximum publication period for CRLs and ARLs

The change in status of a certificate must be indicated in the CRL or ARL after fewer than five minutes have passed since said change was made. As a result, ANF AC will publish a new CRL or ARL in the repository the moment that any revocation is produced.

All CRLs and ARLs published by ANF AC are available on the website.

In any case, ANF AC will publish new CRL at intervals no greater than 7 days, and ARLs at intervals no greater than a year.

4.9.8 Certificate status verification services availability

Trusted third parties can check certificates published in ANF AC's repository through a certificate status information service using OCSP or by consulting the CRLs and ARLs.

Both services are available 24 hours a day, 7 days a week, using a secure protocol.

4.9.9 Obligation to consult the certificate status verification services

One way to verify the status of certificates is by checking the most recent CRL and ARL published by the Certification Entity that issued the relevant certificate.

ANF AC supports trusted third parties in how and where to find the certificate status checking service based on OCSP or the relevant CRL and ARL.

If, for any reason, it were not possible to obtain information on a certificate's status, the relevant system must not be used, or depending on the risk, level of responsibility and consequences which may be produced, it may be used without the guarantee of authenticity status in the terms and standards of this policy.

4.9.10 Other forms of revocation advertisements available

In addition to the online consultation service using OCSP(Online Certificate Status Protocol), and consulting Revocation Lists(CRL) /(ARL), ANF AC makes available to the public the following methods:

4.9.10.1 Personalized service

In case of urgent need, ANF AC's Client Attention Service can be contacted 24x7x365 in the telephone (+356) 2299 3100 (Malta), or in person in ANF AC offices, during office hours from 9 to 18h, Monday to Friday.

4.9.10.2 SOAP service

This allows telephonic incremental updates of certificate revocation lists.

4.9.10.3 Web service

It allows checking the certificate status by consulting the website of ANF AC:

http://www.anfacmalta.com/en/documents

4.9.11 Special requirements in case of private key compromise

In case of compromise of the private key of the certificate the subscriber, or those responsible for the use of the certificate must notify it to ANF AC, in order to proceed to the revocation of the certificate.

In case of compromise of the private key of the CA, it will be notified to all the key participants in this hierarchy, in particular:

- PKI Governing Board.
- all RAs.
- all owners of certificates issued by that CA.
- any known trustworthy third parties.

Revocation will take place immediately and will be published on ANF AC's website.

The Root CA will publish the revoked certificate in the ARL (Certification Authorities Revocation List).

After resolving any matters caused by the revocation, ANF AC may:

- Generate a new certificate for the issuing CA.
- Ensure that all new certificates and CRLs issued by the CA are signed using the new key.
- The issuing CA will issue certificates to all affected subscribers who require them.

4.9.12 Circumstances for suspension

ANF AC does not authorize temporary suspension of certificates.

4.9.13 Who can request suspension

Not authorized.

4.9.14 Procedure for suspension request

Not authorized.

4.9.15 Limits on suspension period

Not authorized.

4.10 Certificate recovery

The CA has recovery services available to all subscribers. This service meets the requirements established in Personal Data Protection legislation and only provides copies of these certificates to correctly-authorized third parties.

The recovery process is as follows:

- Identification of an applicant for retrieving certificate and verifies that it is authorized to require recovery certificate.
- Verify that the certificate is neither expired recover or revoked.
- Verification that the data contained in the certificate is correct.
- Notice to Applicant of recovery shall revoke the certificate that will be replaced by the new certificate.
- Delivery to the email account appears in the digital certificate an email what are the steps to follow for retrieving the certificate.
- After the new certificate generated and assigned a PIN activation and validation process is exactly the same as issuing a new certificate.

The procedure for the recovery of the certificate is the same as for the issuance of a certificate entirely new. The findings of omission or error in the application will be checked by ANF AC. The recovery of a certificate means renewal of the certificate key change.

4.11 Key escrow and recovery

4.11.1 Key escrow and recovery procedures and policies

ANF AC does not generate its subscribers' keys and therefore has no way of storing or recovering their keys.

4.12 Security audit logging procedures

Log files are used to reconstruct the significant events that have been made by software of ANF AC, the Recognized Registration Authorities, the subscriber or the event that originated it. The logs are evidence that can be used as a possible means of arbitration in disputes.

4.12.1 Audits and incidents

ANF AC maintains the following criteria in relation to information available for audits and incident analysis which may exist in issued certificates. Certificate users can make complaints or suggestions to ANF AC via the following methods:

- Telephone: (+356) 2299 3100

- E-mail: support@anfacmalta.com
- In person: List of addresses at

  http://www.anfacmalta.com/en/documents
- Completing the complaints/claims forms available at registration points.

There is an internal incident register which is produced together with issued certificates (security incidents managed by ANF AC's Security Committee). These incidents are registered, analyzed and resolved using ANF AC's SGSI procedures.

The Administrative Security Policy contains formal processes for managing incidents and functional failures. Specifically, it establishes the method to follow in terms of documenting, quantifying potential damage, applying a solution and control the causes and consequences of the incident. It also specifies the information to be sent to the PKI Board.

In annual audit planning, the processes of at least 2% of all issued certificates are audited.

In the CPS, the document conservation period is specified.

4.12.2 Types of events recorded

There is a register containing, at least, the following events related to PKI security:

- Booting and shutting down of systems.
- Starting and closing the certification authority or central registry authority applications.
- Attempts to create, delete or change passwords or user permissions within the system.
- Generation and changes in certification service provider keys.
- Changes in certificate issuing policies.
- Attempts to enter and exit the system.
- Unauthorized attempts to enter the certification service provider network.
- Unauthorized attempts to access system files.
- Failed attempts to read a certificate, and to read or write within a certificate repository.
- Events related to a certificate's lifecycle, including its initial application, issuance, revocation and renewal.
- Events related to the cryptographic device's lifecycle, such as its receipt, use and uninstallation.

ANF AC saves the following information, either manually or automatically:

- The generation of keys and the key management databases.
- Physical access records.
- System configuration maintenance and changes.

- Staff changes.
- Incidents.
- Records of destruction of materials containing key information, activation data or personal information.
- Possession of activation information used for certification service provider private key operations.

For all events identified in this section, auditing records must contain at least the following:

- The type of event recorded.
- The time and date in which it occurred.
- For messages from the Registry Authority requesting Certification Entity actions, the origin of the message, the recipient and the contents.
- For certificates issuance or revocation requests, an indication as to whether the request was approved or denied.

4.12.3 Types of events recorded in life management of the keys

The following types of events related to key lifecycle management are registered:

- How the keys were generated.
- The installation of manual cryptographic keys and their results (as well as the operator's ID).
- The CA's key security copy.
- The CA's key storage copy.
- The CA's recovery keys.
- The CA's key activities (if any are carried out).
- The use of CA keys.
- CA key files.
- The disposal of service key material.
- The destruction of the CA’s key.
- The ID of those in charge of handling any material associated with the keys (such as key components, portable devices storing keys, or transmission media).
- Escrow of keys, devices, or key usage methods and possible compromise of a private key.

4.12.4 Types of events recorded related to the cryptographic device

The following events related to the cryptographic device are recorded:

- The receipt and installation of the device and the packaging.

- The connection or disconnection of a storage device.
- The activation and use of the device.
- The installation process.
- The designation of a device for service and repair.
- The end of the device's lifecycle.

4.12.5 Types of events recorded related to use of the subscription

The following events related to the use of the subscription are recorded:

- How the keys were generated.
- Distribution of keys.
- Security copies of keys.
- Storage of keys.
- Destruction of keys.

4.12.6 Types of information to be recorded by the RA during certificate applications

The following information is recorded and required by ANF AC from the Officially Recognized RAs:

- The ID method used.
- Registration of unique ID information (for example, ID document numbers).
- Storage location of copies of ID documents and application forms.
- The ID of the operator who processes the application.
- Method used to valid the ID documents.
- Name and identifier of the AR which processes the application.
- The subscriber's acceptance of the Agreement, the subscriber's consent to allow the CA to keep within its repositories the records containing personal details, the authorization for third-party access to these records (if applicable), and the publication of the certificates.
- Storage location of copies of ID documents and application forms.

4.12.7 Types of information on keys life management

The following information is recorded:

- Reception of certificate applications.
- Initial applications for certificates, renewal certificates and requests for key renewal.

- Public key requests for certification.
- Certificate generation.
- Public key distribution.
- Certificate revocation applications.
- Generation and publication of certificate revocation lists.

This CA does not record information on the reactivation of certificates since temporary suspension is not authorized and revocation is permanent.

4.12.8 Types of events recorded

The following events are recorded:

- Security profile changes.
- The use of identification and authentication mechanisms, whether authorized or denied (including multiple denied attempts).
- System or hardware failures or other anomalies.
- The measures taken by individuals in trusted roles, computer operators, system administrators and system security officers.

4.12.9 Frequency of processing log

Auditing records are examined regularly by the auditor.

The processing of the auditing records consists in a revision of the records (to check that they haven't been manipulated), a random inspection of all record entries, and a deeper check of any alert or irregularity in the records.

Detected incidents are documented, detailing measures taken and staff implied in decision-making.

There is access control to the auditing tools, avoiding their use or abuse. The use and access to these tools is only available by persons with special authorization.

4.12.10 Period of retention of audit logs

Auditing logs are held for a minimum of three months after being processed. After that moment, they are archived in accordance with section 4.13.2 of this policy.

4.12.11 Audit logs protection

Registration files, both manual and electronic, are protected from being read, modified, deleted or any other type of unauthorized manipulation, applying logical and physical access checks. Private keys used for auditing logs are only used for that purpose.

These protective measures make the deletion of auditing logs impossible before their storage period has finished.

4.12.12 Audit log back-up procedures

Back-up copies of auditing logs are made according to the back-up procedures established in the Databases.

4.12.13 Audit collection system (internal vs. external)

The logs are stored on the internal systems through a combination of automatic and manual processes and carried out by PKI applications.

List of possible risks:

- Fraudulent insertion or alteration of a session log.
- Fraudulent suppression of intermediate sessions.
- Fraudulent insertion, alteration or suppression of a historical log.
- Fraudulent insertion, alteration or suppression of a change table log.

4.12.14 Notification to the subject that caused the event

It is not anticipated the audit registration files action automatic notification to the subject that caused the event.

4.12.15 Risk analysis

A periodic risk analysis will be carried out on all ANF AC internal systems.

4.13 Information and log archive

All information relative to certificates is saved for an appropriate period of time according to that established in section 5.5.2 of this document.

It should be noted that, in relation to confidential documentation, ANF AC does not use documents in a support role. All documents are digitalized, encrypted according to its security level, and stored in secure repositories created for this purpose.

Support papers are held in closed stores, only accessible to specially-authorized staff, which has permanent 24/7/365 security with a monitoring system and alarms.

4.13.1 Type of records archived

ANF AC records all events which take place during a certificate's lifecycle, including its renewal.

The certification services provider must keep a register of, at least, the following information:

- Data related to the registration procedure and certificate request.
- Audit records specified in paragraph5.4 of this document.
- Incidents detected.

4.13.2 Retention period for the file

ANF AC saves all logs specified in the previous section of this policy for a period of at least 15 years.

4.13.3 Protection of file

Measures are taken to protect the file, so it cannot be tampered with or destroyed its contents.

4.13.4 File backup procedures

ANFAC makes daily incremental backups of all electronic documents, and also completes backup weekly and monthly historical copies are undertaken and kept.

There is a backup policy that defines the criteria and strategies for action in case of an incident.

4.13.5 Requirements for time-stamping of records

Information systems used by ANF AC guarantee that information is saved with time stamps. Time information used by the systems comes from a secure source which keeps the time and date.

Specifically, the time signal is synchronized with the Royal Armada Institute and Observatory - San Fernando, Cádiz (Spain), "ROA", which is responsible for maintaining the basic unit of time, "Coordinated Universal Time" (UTC).

This laboratory maintains various servers which distribute time through the NTP protocol. This highly stable and precise system uses a group of cesium atomic clocks which tell the time with a precision greater than a microsecond and with a stability of 32 sec/year.

All systems are synchronized with this source.

4.13.6 File collection system (internal or external)

The information collection system is internal and belongs to ANF AC.

4.13.7 Procedures to obtain and verify file information

Access to this information is restricted to authorized personnel for this purpose, protecting against physical and logical access.

4.14 Renewal of certificates or keys of a CA

The validity of a CA certificate is greater than the validity period of the certificates they issue, in such a way that certificates cannot be issued which exceed the validity period of the certificate belonging to the CA which issues them.

Prior to a CA certificate's expiry date, ANF AC can renew the certificate with or without renewing the corresponding keys.

4.14.1 Renewal of certificates without key change

Renewing a certificate without changing the keys means creating a new CA certificate with a new expiry date while keeping the same cryptographic keys. This renewal procedure allows the hierarchy (the current one and the new one) to be used to validate any certificates issued using these certificate hierarchies.

Both certificates are valid until their expiry dates. Both certificates use the same private key, the same public key, the same CA name and the same CRL. This model of certification with shared keys is known as "Cross-Certification *[1]".

Thanks to this, issued certificates can be validated with either hierarchy, but when consulting the CRL, each hierarchy has its specific CRL and ARL.

4.14.2 Renewal of certificates with key change

Changing of keys ("rekeying") is carried out before the CA certificated expires. Changes can be introduced to the certificate's contents in order to better suit it to current legislation, ANF AC's PKI, and the market reality. This procedure generates a new CA with a new private key.

The old CA and its private key are only used to sign the CRL and ARL which there are active certificates issued by the old CA.

4.15 Compromise of a key or disaster recovery

There is a Contingency Plan that defines the actions to be taken, resources to use and staff to employ in the event of an intentional or accidental event that disables or degrades the resources and services of ANF AC certification. The main objectives of the Contingency Plan are:

- Maximize the effectiveness of recovery operations by establishing three stages:
    - Notification/ Evaluation/ Activation stage to detect, assess damage and activate the plan.
    - Recovery stage to temporarily and partially restore the services until the recovery of the damages caused in the original system.
    - Reconstitution stage to temporarily and partially provide services until the recovery of the damages caused in the original system.
- Identify the activities, resources and procedures necessary for the partial provision of certification services.

- Assign responsibilities to staff designated by the Safety Committee and provide guidance for the recovery of normal operations.

- Ensure coordination of all operators involved in the planned contingency strategy.

The assessment of damage and the action plan are described in the Contingency Plan.

In the event of the circumstances of weak cryptographic system: the algorithm, the combination of the key sizes used, or otherwise significantly technique that weakens the technical security of the system, the Contingency Plan will be applied.

4.15.1 Alteration of hardware, software or data resources

When resources, applications or information become corrupted, a procedure will be activated which begins the necessary management processes in agreement with the Contingency Plan that has the action strategy to this type of situations.

4.15.2 Entity public key revocation

In the event that one of ANF AC's Certification Hierarchies is revoked, the following will take place:

- Notify the fact, once it occurs, to the General Public Administration.

- Publish a ARL announcing the occurrence.

- Make all efforts necessary to advise all subscribers that received certificates from the certification service provider about the revocation as well as trustworthy third parties on those certificates.

- In the case that the revocation was not due to termination of the service by the certification service provider as per that written in this CPS, renew the keys and send them out.

Causes of revocation considered in this section are compromised keys, technical reasons, organization reasons, or disaster.

4.15.3 Entity private key compromise procedures

ANF AC's Business Continuity Plan considers the compromise or suspected compromise of a CA's private key as a disaster.

If an intermediate or subordinate CA is compromised, the following actions, at least, must be completed:

- Verify the compromise and, if confirmed, inform all subscribers.

- Indicate that the certificates and information revocation status information which were issued using this CA's key are no longer valid.

- Proceed as indicated in section 4.9.11.

In the case that the compromised key is the CA root, the certificate will be removed from all applications and a new one will be distributed.

ANF AC's Business Continuity Plan establishes that in the case of a CA's key being compromised, the associated certificate will be immediately revoked, as will all certificates issued by that certificate, offering

affected end entities a new certificate issued by the new CA, free of charge and with the same expiry date as the revoked certificate.

A re-stamping service will also be offered free of charge for all documents signed with the revoked certificates.

4.15.4 Business continuity capabilities after a disaster

ANF AC's Contingency Plan develops, maintains and considers the possibility of testing and, if necessary, carrying out an emergency plan in case of disaster on its installations, whether through natural causes or caused by man, which would indicate how to restore the information systems services.

The location of the disaster recovery systems has physical security protection as detailed in the Security Plan.

ANF AC's Contingency Plan establishes the capacity to restore normal operation of revocation services and suspension in the 24 hours after a disaster, restoring availability of at least the following actions:

- Suspension of certificates.
- Revocation of certificates (where applicable).
- Revocation information publication.

The disaster recovery database used by the certification service provider must be synchronized with the production database within the time limits specified in the security plan.

The certification service provider's disaster recovery equipment has the physical security measures specified in the security plan.

4.16 Certification Services Provider Termination

The recommendations specified in ETSI TS 101.456 v.1.4.3 section 7.4.9 are the ones followed. With the aim of minimizing the effects on subscribers and third parties as a consequence of the cessation of services, ANF AC promises to carry out, at least, the following procedures:

- Notification to the holders of electronic signature certificates and the regulation control organisms at least ninety days in advance of the termination of activities.
- Informing all affected subscribers and trusted third parties.
- Removal of certificate issuance authorization from all sub-contractors who work in the certification service provider's name.
- Carrying out necessary tasks for transferring the log information and archive maintenance obligations during the respective time periods indicated to the relevant subscriber and the trusted third parties.
- Destruction of all CA private keys.
- Revocation all certificates issued by the CA.
- Transfer of all certification service provider obligations to another certification entity and must therefore receive the certificate owner's express authorization.

If the obligations are not transferred to another certification entity or the certificate owner does not authorize the process, the certificate will be revoked with notice given in advance.

4.17 Recognized Registration Authority Termination

Once Recognized Registration Authority cease to hold functions, all transfer records, documentation, technological equipment and devices at given at the disposal of ANF AC.

4.18 Completion of the subscription

The certificate, when its term ends or when revoked, is not valid for use.

Each Certification Policy specifies the expiration of the different certificates.

5 Facility, management, and operational controls

5.1 Physical controls

Controls are maintained in all places where ANF AC provides services.

5.1.1 Site location and construction

Buildings, in which ANF AC infrastructure is found, have access control security measures which only allow authorized persons to enter.

Installations in which information is processed must comply with the following physical requirements:

a. The building containing the information processing units is physically solid, the external walls are of solid construction, and only allows access to authorized persons.

b. All doors and windows are locked and protected against unauthorized access.

c. The generation of keys and publishing of CA certificates are done in a banking bunker, situated underneath a high-security building. This building has a physical structure which guarantees that the place is free of electromagnetic radiation.

d. The IT equipment which provides public services (main and mirrored back-ups) are installed in data centers belonging to primary European operators governed by the corresponding contract which specific the necessary security measures, and the compromises of confidentiality and SAL according to current legislation.

e. The building where ANF AC's central infrastructure is physically secure with up to six levels of security to reach critical machines and applications.

Systems are physically separated from others in the same place in such a way that only authorized ANF AC can access them, guaranteeing the independence of third-party equipment and systems in the building.

f. Among the various measures for protection these installations possess, it should be pointed out that:

- These buildings have 24-hour surveillance and permanent CCTV. Cameras are set not to be able to see ANF AC server operations in order to avoid any risk of seeing the activation PIN or any other confidential data.
- They are placed away from the basements to prevent any possible flooding.
- The building is modern and built for the specific purpose and use of the operator. Located in a prestigious business park which is easy for Fire and Public Services to access in case of need.
- The building is located in an area of low seismic activity without any previous natural disasters.
- The building is located in an low-crime area.
- Neither the building nor its location is considered terrorist targets.

- The premises contain no exterior windows.
- The premises are constantly protected by staff belonging to a security company authorized by the Ministry of the Interior.

  These staff have updated, detailed lists of all persons that ANF AC authorizes to enter the central core (where ANF AC's IT equipment is kept) and will keep a record of entry and exit times and days, the identity and signature of all persons entering, handing over staff access cards. Computers will not be removed in any case without express authorization.
- Access to the central core is controlled through various checks. Staffs that accesses the core must always be accompanied by staff responsible for information center administration. Any job carried out on ANF AC's IT equipment is done in the constant presence of a technician belonging to the staff responsible for information center administration.
- All installations have back-up power and air-conditioning systems which comply with industry standards with the aim of creating a suitable operating environment.
- All installations have prevention mechanisms designed to reduce the effect of contact with water.
- All installations have fire protection and prevention mechanisms. These mechanisms all comply with industry standards.
- All cables are protected against damage, telephone and data interception.
- Partitions protecting the central core areas are transparent and have permanent lighting to enable observation of the area through surveillance cameras and from corridors or administrative office areas in order to prevent illicit activities inside the vault.

5.1.2 Physical access

- Physical security perimeter:

  Besides these above-mentioned measures, various personalized access control systems have been implemented which register the movements of people through each area. Visiting staff are to be constantly supervised by a data center manager.
- Physical entry controls:

  There is an exhaustive physical control system upon entry and exit which consists of various rings of security which is regularly updated.

  Diverse security systems, both human and technical, are combined into the following physical entry controls:

  - Access through showing national ID card to the security service, monitoring and registering person, time of arrival, exit, authorization, and being provided with a personal ID number.
  - Use of personal number for identification in security devices, checking authorization and registering access.
- Installing or removing equipment:

These operations require the express authorization of the Data Controller, taking an inventory of existing equipment, and of all equipment taken away or received.

5.1.3 Power and air conditioning

The rooms where the ANF AC certification system equipment is located are provided with sufficient electricity and air conditioning to create a reliable operating environment. The installation is protected against power cuts or any other electricity supply anomaly by a secondary power line independent from the main electricity supply.

Mechanisms which maintain heat and humidity at agreed levels have been installed in the appropriate rooms.

Those systems which require them have power generators and uninterrupted power supply units.

The installations where the certification servers are found and from where certificates are issued have the following facilities:

- Servers which provide certification services have a system of protection against electrical anomalies or cuts, and all cabling is protected against damage and interception.
- Equipment used for issuing certificates is permanently disconnected from the electrical supply. When used, they exclusively use independent sources free of any possible anomaly.

5.1.4 Water exposures

Suitable measures have been taken to prevent water exposure to all equipment and cabling.

5.1.5 Fire prevention and protection

Rooms are all fitted with detectors to protect their contents against fires. Cabling is found under a false floor or a false roof and have further detectors in the floor and roof to protect them against fires.

5.1.6 Media storage

ANF AC has established procedures necessary to have available back-up copies of all information in its productive infrastructure.

Plans have been established for taking back-up copies of all sensitive information considered necessary to continue activities.

ANF AC stores and guards all certificates issued for a period of time never less than 15 years after their various expiry dates.

5.1.7 Waste disposal

A policy of waste management has been adopted which guarantees the destruction of any material which may contain information as well as a policy of removable media management.

Media which contains confidential information are destroyed in such a way that the information is irretrievable after being thrown away.

5.1.8 Off-site backup

ANF AC has security copies held in two separate buildings, with sufficient physical separation and security measures.

Each device has a unique identifier, description, model and brand.

5.1.9 Bank security box

ANF AC has hired a security box in a Spanish banking entity in which copies of the devices which regenerates the system in case of emergency.

Access to the Security Box is restricted to personnel expressly authorized by ANF AC who carry keys which are able to open the Security Box.

Among the various measures for protection these banking installations possess, it should be pointed out that:

- These buildings have 24-hour surveillance and permanent CCTV.
- The building architecture and plating correspond to the design commonly used in buildings known as "banking bunkers".
- The premises are constantly protected by staff belonging to a security company authorized by the appropriate department in the Spanish Ministry of the Interior.
- All access to the banking entity will be entered into the register, recording the entry and exit date and time, identity and signature of the person entering, by the responsible of this.
- Access to the central core is controlled through various checks. The person accessing the box must be constantly accompanied by the person responsible for the administration of the banking bunker and the operation of the security box using a double key: one in the hands of the ANF AC staff and the other held by the banking entity.
- All installations have power and air conditioning systems which comply with legislation in effect.
- All installations have fire protection and prevention mechanisms. These mechanisms all comply with industry standards.
- To access the Security Box requires the presence of at least two authorized operators and the use of the bunker supervisor's master key.

5.1.10 Security against intruders

Installations where certification servers are found and where CA and end entity certificates are issued have fire doors and intruder detection systems which are installed and regularly tested to cover all external doors.

The installations holding the servers are permanently operational, 24 hours a day, 365 days a year.

Also, when the installations in which CA keys are generated and certificates are issued are not used, they are physically locked and their security alarms are activated.

5.1.11 Terminal security

To identify terminals and especially portable equipment, a model has been established according to the terminal's location and the services they are trying to access:

- Local access: Identification is made through electronic signature technology, accessed through internal IP address and authorization control according to the terminal's MAC.
- Remote access: It is only possible to access equipment configured specifically for this aim. According to the sensitivity of the service, access is restricted to certain previously authorized IP addresses.

5.2 Procedural controls

For reasons of security, information regarding procedure checks is considered confidential information.

5.2.1 PKI control and management roles

The following roles are defined for control and management of the system:

a. Certificate Issuing Managers.

b. Area Managers.

c. System Administrators.

d. Certification Authority Operators.

e. Training and Selection Manager.

f. Security Manager.

g. Auditors.

h. Manager responsible for preparing issuance reports and revocation of certificates.

i. Documentation Manager.

5.2.1.1 Certificate issuance managers

There are a minimum of four operators who have the capacity to access and activate ANF AC's certificate issuing devices.

To activate the keys, it is necessary to have at least three persons present: two of them assume the role of Certificate Issuing Managers and a third belonging to the data center security team (without access to the keys).

5.2.1.2 Area managers

They are people who manage each section of ANF AC. Their staff is found under their control and supervision. It is their responsibility to:

- Receive and start processing reports for infringements which may affect their staff, proposing appropriate disciplinary measures.
- Effect permanent control of the technical and human resources available in their Department with the aim of answering the needs of the service provided.

5.2.1.3 System administrators

They are responsible in the areas of IT and Telecommunications, but they have no responsibilities in internal audit tasks. Their responsibilities include:

- They are responsible for the installation and configuration of operating systems and software, and maintenance and updating of installed programs. They configure and maintain systems without having access to data.
- They are responsible for activating CRL, OCSP and Timestamping services through specific certificates.
- They are in charge of establishing and documenting system and service monitoring procedures as well as controlling tasks carried out by Certification Authority Operators.
- They are responsible for designing program architectures, controlling and supervising trusted developments, and correctly documenting applications.
- They are responsible for the correct execution of the Copies Policy, particularly for maintaining sufficient information to be able to restore any system in as little time as possible, completing local security copies and transferring them in accordance with the Security Plan.
- They are responsible for maintaining the inventory of servers and other ANF AC certification system components.
- They manage router and firewall rule services, manage and maintain intruder detection systems and other related tasks.
- They are responsible for installing and uninstalling CA cryptographic hardware.
- They are responsible for the maintenance and repair of CA cryptographic equipment (including the installation of new hardware, firmware or software), and making the devices available for use.

5.2.1.4 Certification Authority operators

- They work in the administrative area.
- They perform administrative tasks which require no physical access to Certification Servers.
- They carry out traditional administrative tasks: filling, data entry, reception and sending of mail, receiving visitors and telephone calls, etc.

- They carry out work required by the Area Manager under whose criteria their work is organized and responsibilities delegated.
- They must have been trained specifically in data protection and IT security, passing all corresponding tests. They are required to have completed at least one year's experience in admin function.

5.2.1.5 Training and selection manager

- They work in the legal department.
- They are in charge of keeping ANF AC staff training plans up-to-date.
- They supervise and rate staff training courses, and carry out the appropriate tests to evaluate the knowledge received during the course.
- They manage the selection of new staff, ensuring references are received and that they meet established levels.
- A minimum of three years' experience is required on a similar role.

5.2.1.6 Security manager

- This task is assigned to the ANF AC Information Security Committee: comprising the Managing Director and the Heads of the Technical and Legal Departments.
- They are responsible for updating and implementing security policies and procedures which have been approved by the ANF AC Board.
- They control the formalization of agreements between ANF AC and its staff.
- They communicate all agreed disciplinary measures and ensure compliance.
- They ensure all staff comply with ANF AC's security policies and must take charge of any matter related to PKI security, including physical security, application security, and network security.
- They are in charge of managing perimeter protection systems and, specifically, verifying that firewall rules are managed correctly.
- They are in charge of checking Intrusion Detection Systems (IDS) and all related tools are correctly installed, configured and managed.
- They are responsible for making sure any security incident produced is resolved, eliminating detected vulnerabilities and other related tasks.
- They are responsible for the management and control of physical security systems and of movements of material outside of CA installations.
- They must take charge of selecting and contracting third-party specialists who can help improve ANF AC security.
- They are required to have completed at least one year's experience in a similar role.

5.2.1.7 Auditors

- They work in the legal, and IT and telecommunications areas.
- They perform Internal Audit tasks.
- They are responsible for carrying out Internal Auditing in agreement with Certification Service Auditing Rules and Criteria (ANF AC) OID 1.3.6.1.4.1.18339.11.1
- They are able to access system logs.
- They are required to have worked at least one year in a related role.

5.2.1.8 Issuance reports and certificates revocation manager

They are responsible for issuing certificates or revoking them. They are required to have worked at least one year in a related role.

5.2.1.9 Documentation manager

- They work in the administrative area.
- They ensure that ANF AC's electronic documentation and paper document repositories are up to date.
- They supervise the updating of documents when necessary.
- They are the only people able to store, delete or modify documents in ANF AC's documentation repository.
- They are required to have worked at least one year in a related role.

5.3 Personnel controls

5.3.1 Qualifications, experience, clearance and authentication requirements

In accordance with the Administrative Security Plan.

The Administrative Security Policy and the CPS establish the requirements for staff necessary to adequately carrying out the AC operations. They always follow the principle of genuine need to authorize the access of an AC transaction. Area managers are responsible for establishing the number of operators and the qualifications that they need to have according to the job role, and of selecting the correct candidate.

In especially sensitive operation, they will always rely on personnel already within the company. These are personnel who have received the necessary training to complete these operations and whose number is always greater than that necessary so as to face any possible incident.

5.3.2 Background check procedures

According to the procedures set out in the Administrative Security Plan. It should be noted that staff that carry out trust functions are subject to the same plan.

5.3.3 Training requirements

ANF AC develops training exercises each time staff join the AC who need extra training regarding any of their functions. A minimum of 40 hours of training is carried out annually in the material considered necessary to ensure functions are being completely correctly, and, in general, continuous training is given in terms of Administrative Security on the following aspects:

- Access control.
- Media management.
- Incident register.
- User register.
- Identification and authentication.
- Back-up and recovery copies.
- Analysis of files, data and IT systems.
- Security System access through terminals.
- Administrative Security. Security Plan.

The following aspects are included in the training:

- Handing out a copy of the Certification Practice Statement.
- Physical, logical and technical security awareness.
- Software and hardware operation for each specific role.
- Security procedures for each specific role.
- Operation and administration procedures for each specific role.
- PKI operation recovery procedures in case of disasters.

5.3.4 Retraining frequency and requirements

According to ANF AC Annual Training Plan.

5.3.5 Job rotation frequency and sequence

Not stipulated.

5.3.6 Sanctions for unauthorized actions

Staff is subject to a disciplinary procedure previously made known to all operators within the business. The operational procedure followed is found in Annex II of this CPS.

Carrying out unauthorized operation is subject to disciplinary measures. The penalty could lead to loss of employment, irrespective of that established by law which may lead to facing a Judicial Authority.

5.3.7 Third parties contracting requirements

All staff with access to ANF AC certification services signs a confidentiality agreement as part of the terms and conditions of their incorporation. This agreement includes information on control or supervision tasks which ANF AC security staff carries out on staff, software and hardware.

The aim of this is to guarantee the highest possible level of security for the services this CA provides, and for the goods they have the obligation to protect.

5.3.8 Documentation supplied to personnel

Access will be provided to the obligatory security regulations which the employee will sign, along with this CPS and all applicable CPs.

5.3.9 Unauthorized activities

Unless express authorization has been given, it is not permitted to install, use or request information which may be used to evaluate or compromise the security of ANF AC certification systems. It is also not possible to install or use, without express authorization, instruments to attempt to evaluate services which ANF AC uses or receives.

This extends to any attempt to check or compromise ANF AC security measures even if no instrument is used. It also extends to unauthorized evaluation of any services provided or received by ANF AC, whether or not devices are used.

The use of software or hardware which is not authorized by the company is also expressly prohibited, as well as the installation, storage or distribution by any media.

It is forbidden to share usernames and passwords. If a user suspects that another person knows their access or identification details, they must change their password.

The user are prohibited from using information, the corporate network, the entity's or third-party Intranet to engage in activities which could be considered illicit or illegal, which infringe on the rights of the company and/or third parties, or which could go against the moral or ethical rules of ICT networks.

It is also forbidden to:

- Share usernames and passwords provided by the Entity to another natural or legal person. If this prohibition is breached, the user will be the person responsible for any actions carried out by the natural or legal person under the user's identification.
- Trying to decrypt the key, systems or encryption algorithms or any other security element which participates in the telecommunications processes of the Entity.

- Trying to read, delete, copy or modify any other users' e-mail messages or files.
- Trying to distort or falsify system logs.
- Use the system to try to access restricted areas in the Entity's and/or third parties' IT systems.
- Trying to increase the privilege level of a user in the system.
- Destroy, alter or damage the Entity's or third parties' information, programs or electronic documents.
- The user must not store personal data on the hard drive of a PC nor on the corporate network.
- Deliberately hinder other users' access to the system by massive consumption of IT or telecommunications resources, nor carry out actions which harm, interrupt or generate errors in said systems.
- Send massive amounts of e-mails, or e-mails with commercial aims without consent of the recipient.
- Voluntarily introduce programs, viruses, macros, applets, ActiveX components or any other logical device or sequence of characters which cause or may cause any type of alteration in the IT systems of the company or related third parties. It should also be noted that the system automatically runs antivirus programs and their updates to prevent the introduction of any element which may destroy or corrupt information.
- Introduce, download from the Internet, run, and use or distribute any IT program not expressly authorized by the company. This prohibition includes any other type of materials whose intellectual or industrial property rights belong to third parties and have not been authorized for use.
- Install illegal copies of any program, even those that are standardized.
- Delete any program installed legally.
- Send or forward chain or pyramid messages.
- Use company IT or telecommunications resources, including the Internet, for activities which are not directly related to the user's job role.
- Introduce content which is obscene, immoral, offensive and, in general, lacking in use to the aims of the business.
- Encrypt information without being expressly authorized to do so.
- Physically or logically access ANF AC installations outside of working hours.

5.3.10 Periodic compliance controls

In agreement with the Administrative Security Plan.

5.3.11 Expiration of contracts

In agreement with the Administrative Security Plan.

6 Technical security controls

ANF AC uses reliable systems and products which are protected against any alterations and which guarantee technical security and cryptography for all certification services which they support.

In order to develop its activities as a Certification Service Provider, ANF AC has a R&D department and a cryptography section which determines the security status of all encrypted elements used in its PKI.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Elements where the key pair for each of the different entities and participant persons in the ANF AC PKI are generated:

- Root CA: the machine where the Root CA resides has a cryptographic device(HSM) for key generation of the Root CA.
- Issuing CAs: the machine where the Issuing CAs resides has a cryptographic device(HSM) for key generation of the Issuing CAs.
- End-entity certificates. The keys may be generated using:
    - Cryptographic software device held by the subscriber. The keys are generated by the same subscriber, which determines the signature data generation to employ.
    - Cryptographic hardware device (HSM) held by the subscriber. The keys are generated by the same subscriber, which determines the signature data generation to employ.

ANF AC provides its users the cryptographic devices needed to generate privately and with no third party involved, the pair of keys and their activation data.

ANF AC does not store, nor has the opportunity to store the private keys of subscribers.

6.1.2 Private key delivery to end-entity

Not applicable. ANF AC does not generate keys for its end-users.

6.1.3 Public key delivery to certificate issuer

The public key to be certified is generated by the subscriber and is delivered to the Certification Authority through the sending of a certificate request using the format CSR (Certificate Signing Request), which follows the specification PKCS#10.

6.1.4 CA public key delivery to trustworthy third parties

The public keys of the Root and Intermediate CAs are available to trusted third parties ensuring the key's integrity and verifying its origin.

The Certification Service Provider public key is published in the Repository as a self-signed certificate in the case of the CA Root, and as a certificate signed by the Root CA in the case of Intermediate CAs, together with a Certification Practice Statement which specifies that the key is authentic of ANF AC.

Further measures are included to trust the self-signed certificate such as checking the certificate's digital fingerprint. Users can access the Repository to obtain ANF AC's public keys through the website

http://www.anfacmalta.com/en/pki-ac/certificates.html

6.1.5 Key sizes

The algorithm used in all cases is theRSAwithSHA-1, except for the CA Root and its Intermediate CAs, issued with a second SHA-256 certificate.

Key sizes are, depending on the cases:

- At least 2048 bits for keys of end-entity certificates.
- At least 4096 bits for keys of Root CAs and its Intermediate CAs from 2013.

6.1.5.1 Certificates signature algorithms

The algorithm identifier (Algorithm Identifier) used by ANF AC to sign certificates is SHA-256 (hash algorithm) with RSA(signature algorithm) that corresponds to the identifier for "Identifier for SHA-256 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."

SHA1 Sunset

ANF AC, as a CAB Forum member, joins to the policy of ceasing to use cryptographic algorithms considered by the industry as potentially breakable. That is why it has been set this schedule in order to end the usage of the SHA1 digestion algorithm in favor of its evolution, the SHA2 (SHA256 – SHA512).

6.1.6 Public key parameters generation

- Keys generated in HSM support: following the FIPS 140-2 Level 3 recommendations. Key generation in HSM devices requires the approval of at least two people.
- Cryptographic keys generated on a cryptographic device: following the recommendations of FIPS140-2Level 2orequivalent.

6.1.7 Public key parameters generation quality checking

Specifications of section 6.1.5.1 “Certificate Signature Algorithm” are applied.

6.1.8 Key generation in software or in equipment

The keys are generated as follows:

- CA: on the HSM device itself.
- End-entity: in their own devices or in the systems that support them.

6.1.9 Key usage purposes

Authorized uses of keys for end-entity certificate issued by ANF AC are defined in the Certification Policy for each certificate.

All certificates contain the extension "Key Usage" which contains critical information defined by the standard X.509 v3. There are also additional limitations on the Extended Key Usage which are also classified as critical. This classification allows limiting the use of the certificate to the purpose for which it was issued.

6.2 Private Key Protection

6.2.1 CA cryptographic module standards

ANF AC uses the following cryptographic modules:

- The software device contains libraries and cryptographic algorithms that allow the generation of the private keys and then its storage.

  The software device is designed to generate a key store in accordance with the specifications published in the 5.4. section, according to the implementation of Keystore.UBER. Available specifications in:

  https://www.bouncycastle.org/specifications.html

  The software device is distributed by ANF AC to end-users with the registered trademark Plug & Sign®

- The HSM (Hardware Security Module) is a cryptographic hardware security device that generates and protects private keys.

  It is required that HSM devices meet FIPS 140-1 Level 3 or equivalent. ANF AC uses two models:

  1. Used by ANF AC in servers of the infrastructure that provides a service to the ANF AC PKI.

     Thales nShield device of ISO 15408 Common Criteria EAL4+ security level, and

     Black Box Sign® device of ISO 15408 Common Criteria EAL5+ security level, and

  2. Cryptographic token. Distributed by ANF AC to end-users with the registered trademark Critical Access ®

     This device has the ISO 15408 Common Criteria EAL5+ security level certification.

6.2.2 Private key multi-person control

For using the CA private keys, it is necessary the approval of at least two operators authorized by the PKI Governing Board.

6.2.3 Private key storage

A backup copy of the private key of the CA is obtained by applying the procedure specified in section 6.2.4. The private key is encrypted and is contained in a Smart Card Device (HSM).

The Smart Card is deposited in a safe-deposit box in a banking bunker. Access to the safe-deposit box requires the intervention of at least two operator authorized by the PKI Governing Board.

6.2.4 Private key backup

There is a key recovery procedure of the CA cryptographic modules (Root or Intermediate) that can be applied in case of contingency, and that is applied during the CA Certificate Issuing Ceremony.

The key recovery process of cryptographic modules corresponds to the context of certified processes of the HSM device. Only SmartCard (HSM) devices are employed.

6.2.5 Private key transfer into a cryptographic module

Only in the case of contingency, the procedure described in section 6.2.4 is used, in order to enter the private key into cryptographic modules.

6.2.6 Method of activating private key

In all cases, the use of PIN numbers is required for using private key cryptographic devices. They are delivered through a system that maintains the necessary confidentiality.

For the CAs, private keys are used by an authorized operator that uses a SmartCard (HSM).

6.2.7 Method of deactivating private key

The extraction of the cryptographic device from the issuing machine implies the completion of any action being carried out.

6.2.8 Method of destroying private key

There is a procedure for destruction of CA keys, and cryptographic devices that contain subscriber's private keys incorporate a key destruction process.

6.3 Other aspects of key pair management

6.3.1 Public key file

The certificates generated by the CA, are stored during the time period required by law, and in any case for a minimum period of 15 years.

6.3.2 Public and private key usage periods

This is the duration of each of the certificates.

6.4 Activation data

6.4.1 Activation data generation

- **Identity certificates issued in cryptographic device**: Using the private key associated with each certificate requires activation data(PIN).
    - It provides the authorized operator to use the cryptographic device, a system that allows maintaining the confidentiality and free choice of PIN.
    - The PIN is generated by the authorized operator of the cryptographic device during the process of creating keys.
    - The device employs cryptographic security logic that only allows the choice of activation data(PIN) that meet basic safety requirements.
    - The cryptographic device features a function that allows the operator to change the authorized PIN.
    - The PIN is never stored or printed in any medium.
- **End-entity technical certificates** issued in software support: the installation and commissioning of the private key associated with the certificate, requires the use of the safety systems that the user has defined. ANF AC cannot control or define how to access the private key in these cases.

6.4.2 Activation data protection

Regarding the signature activation data (PIN), the following is required for the authorize operators:

- To memorize them.
- To maintain their privacy.

6.4.3 Other activation data aspects

It provides life time activation data. However, the data must be changed periodically to reduce the possibility of being discovered.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

There are a number of controls on the location of the different elements of the certification service of ANF AC (CA, data bases, telecommunication services, CA operation and network management):

- There is a Contingency Plan.
- Operational controls:
    - All operating procedures are properly documented in the corresponding operating manuals.
    - Virus and malicious code protection tools are implemented.
    - Continuous maintenance of equipment is conducted, in order to ensure their continued availability and integrity.
    - There is a procedure of saving, deleting and eliminating information carriers, removable media and obsolete equipment.
- Data Exchanges. The following data exchanges are encrypted to ensure the confidentiality:
    - Data transmission between ANF AC Trusted Servers and Recognized Registration Authorities (RA).
    - Data transmission between ANF AC Trusted Servers and subscribers.
- The revocation publishing service has the functionality necessary to ensure 24/7/365 operation.
- Access control:
    - Identity certificates reused, so that the users are related to the actions performed and may be accountable for their actions.
    - The assignment of rights is carried out following the principle of least privileges granted.
    - Immediate removal of the access rights of users who change jobs or leave the organization.
    - Periodic review of the access levels assigned to users.

- Special privilege assignments are done "case by case" and are deleted once ended the cause which led to their allocation.
- Logical controls exist to ensure quality in passwords.

6.5.2 Computer security rating

The products used for the issuance of certificates have the international certificate “Common Criteria" or ISO/IEC 15408:1999 standard, or equivalent.

6.6 Life cycle technical controls

6.6.1 System development controls

ANF AC carries out analyses of security requirements during design and specifications of any component's requirements used in this PKI's applications in order to guarantee the systems are secure.

Change control procedures are used for new versions, updates and emergency patches of said components. The installation of software on production systems is controlled.

To avoid possible system incidents, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) in production.
- Before rolling out any software, it must be installed in a test environment where the relevant tests are carried out.
- A log file of all updates is kept in libraries.
- All previous software versions are kept.
- In processes affecting the security of certification systems, software is only installed in the Engineering Dept. has the source code and has carried out the corresponding safety checks in the presence of Technical Management.

6.6.2 Life cycle security controls

ANF AC carries out checks to ensure security on devices which generate keys. To avoid possible system incidents, the following controls are established:

- Key generation software/hardware is tested before being rolled out.
- Key generation is produced within cryptographic devices which meet the technical and business requirements.
- Procedures for secure storage of cryptographic hardware and activation materials are produced after the key generation procedure.

The products used for the issuance of certificates have the international certificate "Common Criteria" or ISO/IEC 15408:1999 standard, or equivalent. These products shall be replaced in case of loss of certification.

Certificates generated in the process of developing and testing, as they have not been put into production, will be discarded without requiring revocation notice to third parties or activation of the Contingency Plan.

6.6.3 Test environment controls

ANF AC carries out analyses of business requirements during design and specifications of any component used in this PKI's applications in order to guarantee the systems are secure.

Change control procedures are employed in the test environment and follow a procedure strictly controlled by the systems manager in the test environment. Every user is identified upon accessing the test environment in the same way as the live environment. New versions, updates and emergency patches of said components are first installed in the test environment and revised under the change control procedure.

To avoid possible system incidents, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) in the test environment.
- The test environment is a replica of the production environment, both at hardware and software level.
- The same access checks exist in both environments.
- The information found in the test environment is test data, generated by the engineering department.
- Before rolling out any software, it is verified in a test environment where the relevant tests are carried out.
- A log file of all updates is kept in libraries.
- Previous versions of software are kept in case of need to recover the system.
- In processes affecting the security of certification systems, software is only installed if the Engineering Dept. does not have the source code and has carried out the corresponding safety checks in the presence of the Technical Management.

6.6.4 Changes control procedure

Changes procedures controls are employed for development of access to libraries in which software is maintained (through version control). Each employee is identified by a unique ID and any modification, reading, download or loading of the code is registered in the library.

Control is therefore maintained over access of the program's source code. To avoid possible incidents, the following controls are established:

- There is a formal authorization procedure for updating software libraries (including patches) in the test environment.

- Before rolling out any software, it must be installed in a test environment where the relevant tests are carried out.
- Changes to files or independent developments which don't follow ANF AC's business plans are discarded.
- The buying or modification of software is controlled, the procedure authenticated and the application version is controlled.
- A log file of all updates is kept in libraries.
- All previous software versions are kept.
- In processes affecting the security of certification systems, software is only installed if the Engineering Department does not have the source code and has carried out the corresponding safety checks in the presence of the Technical Management.

6.6.5 Security management controls

ANF AC maintains an inventory of all active information and classifies them in agreement with their protection and coherence needs by running a risk analysis.

Capacity requirements will be constantly checked and procedures planned to guarantee sufficient availability of electricity and storage for IT equipment.

6.7 Network security controls

Access to different ANF AC networks is limited to authorized persons. Specifically:

- Checks are implemented to protect the internal network of external domains accessible by third parties. Firewalls are configured to prevent access and protocols which are not necessary to normal service operations.
- Sensitive data is encrypted when transferred through non-secure networks (including subscriber registration information).
- It is guaranteed that local network components are located in secure environments as well as periodic auditing of all configurations.

6.8 Cryptographic modules security controls

Cryptographic modules used for the generation of the keys of Root CAs and Intermediate CAs, and those used to issue end entity certificates, follow the standard FIPS 140-1 Level 3 or FIPS 140-2 Level 3.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile, OCSP and CRL lists

Certificates issued by ANF AC MALTA, LTD. comply with the following technical standards:

- Generally in all certificates:
    - Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) April 2002 updated by 6818
    - Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 5280) December 2005
    - Update to Directory String Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280) August 2006
    - ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
- Certificates issued as Qualified:
    - ETSI TS 101 867 Qualified Certificate Profile.
    - RFC 3739: Internet X.509 Public Key Infrastructure– Qualified Certificate Profile.

7.1.1 Version number(s)

Electronic certificates issued under this Certification Practice Statement use, theX.509 standard, version 3.

7.1.2 Certificate extensions

Used extensions are:

1. Authority key Identifier
2. subject Key Identifier
3. basic Constraints
4. key Usage
5. certificate Policies
6. subject AltName
7. issuer AltName
8. ext. Key Usage
9. CRL Distribution Points
10. Subject Directory Attributes
11. Authority Information Access

7.1.2.1 Generic certificate profile

The profiles are defined in their respective Certification Policies.

7.1.2.2 Algorithm object identifiers (OID)

The Algorithm Identifier used by ANF AC to sign certificates is SHA-256/RSA, which corresponds to the identifier for "Identifier for SHA-256 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."

- SHA256withRSAEncryption (1.2.840.113549.1.1.11)

Public Key Object Identifier (OID):

- RSA Encryption (1.2.840.113549.1.1.1)

7.1.2.3 Proprietary fields

International and unambiguous Object Identifiers are assigned. Specifically:

- Fields referenced with OID1.3.6.1.4.1.18339.x.x, are ANF AC proprietary extensions.

Further information about ANF AC's proprietary extensions can be found referenced in the Section "Proprietary fields of ANF AC", of this CPS.

7.1.3 Name forms

As specified in the section “Names” of this document.

7.1.4 Name restrictions

No name restrictions are used.

7.1.5 Certification Policy object identifier

As specified in the section “Identification” of this document.

7.1.6 Usage of "Policy Constraints" extension

No policy restrictions are stipulated.

7.1.7 Policy qualifiers syntax and semantics

The Certificate Policies extension contains the following "Policy Qualifiers":

- Policy Identifier: This identifies the type of certificate profile within a certain certification policy to which is it associated.
- Policy Qualifier ID: Identifies the Certification Policy which is applied.
- CPS Pointer: contains a pointer to the Certification Practice Statement and Policies published by ANF AC.
- User Notice: A CPS released by the issuing CA which makes reference to certain legal regulations.

7.1.8 Processing semantics for the critical "Certificate Policies" extension

Following standard S/MIME secure e-mail application recommendations [RFC 3850] and SSL/TLS web authentication [RFC 6176], the extension is defined as non-critical.

7.1.9 Guidelines for the completion of certificate fields

According to RFC5280recommendations, the fields will be encoded in UTF8.On this basis international character sets are encoded including Latin alphabet characters with diacritics ("Ñ", "ñ", "Ç", "ç", "Ü", "ü", etc.) such as the character "ñ", which is represented in Unicode as 0x00F1.

Furthermore, in order to establish a common framework for all certificates issued in the field of the PKI of ANF AC, the following recommendations are regarded in the emission of certificates:

- All literals are entered in uppercase, except the domain name/subdomain and email, which will be in lower case.
- Names are coded names as they appear in supporting documentation.
- Regarding the names of individuals, first and second surnames, must be necessarily included, separated only by a blank space, as indicated in the Identification Card / Passport identification documents. In case there is no second surname, its field will be left blank (with no characters).
- Necessarily include the number of Identification Card, along with the letter of control, as indicated in the Identification Card.
- Optionally, the text string "ID" can be included before the Identification Card.
- Optionally, a text string identifying can be included, for example (AUTHENTICATION) for authentication, (SIGNATURE) for signature or (ENCRYPTION) for encryption. This identifier will always be at the end of the CN and between parentheses.
- Not including more than one space between strings.
- Not including blank characters at the beginning or end of strings.
- The inclusion of abbreviations is supported based on simplification, provided they do not difficulty in interpreting the information.
- The "User Notice" field will not have more than 200 characters.

- Each Certification Policy may define specific rules and constraints.

7.1.10 Proprietary fields of ANF AC

Below are proprietary extensions that can be introduced into the certificates issued by ANF AC issued. Together with the OID assigned, the contained value is specified.

OID	Value contained
1.3.6.1.4.1.18339.10.1	Name of legal representative (applicant)
1.3.6.1.4.1.18339.10.2	Surname of legal representative (applicant)
1.3.6.1.4.1.18339.10.3	Last name of legal representative (applicant)
1.3.6.1.4.1.18339.10.4	VAT number of legal representative (applicant)
1.3.6.1.4.1.18339.10.5	Document evidencing legal representative (applicant)
1.3.6.1.4.1.18339.10.6	Joint powers (only in case of existing)
1.3.6.1.4.1.18339.10.7	E-mail address of legal representative (applicant)
1.3.6.1.4.1.18339.10.8	Identity card type submitted by the applicant
1.3.6.1.4.1.18339.10.9	Nationality (applicant)
1.3.6.1.4.1.18339.10.10	Legal document or powers of attorney of the legal representative; the original digitized
1.3.6.1.4.1.18339.10.10.1	URL for downloading the legal document or powers of attorney digitized from the original.
1.3.6.1.4.1.18339.11	Full name of the natural or legal person, which provides representation to the subscriber
1.3.6.1.4.1.18339.12	First Name of the individual who provides representation to the subscriber
1.3.6.1.4.1.18339.13	Surnames of the natural person which provides representation to the subscriber.
1.3.6.1.4.1.18339.14	VAT number or ID number of the legal entity or natural person who provides a representation to the subscriber
1.3.6.1.4.1.18339.19	Localizer of the application (sequential filing– Identifier of the RA operator or IRM that filed it.
1.3.6.1.4.1.18339.19.1	RA operator identifier which processed the application. NOTE: In case of RA Operator Certificates, IRM or PKI, this OID corresponds to the operator identifier holder of the certificate, outlined in the first part of the code)
1.3.6.1.4.1.18339.20.1	Company name(subscriber)

1.3.6.1.4.1.18339.20.2	VAT number (subscriber)
1.3.6.1.4.1.18339.20.3	Name(subscriber)
1.3.6.1.4.1.18339.20.4	Surname (subscriber)
1.3.6.1.4.1.18339.20.5	Last name (subscriber)
1.3.6.1.4.1.18339.20.6	VAT number (subscriber)
1.3.6.1.4.1.18339.20.7	Address(subscriber)
1.3.6.1.4.1.18339.20.8	Identity card type submitted by the applicant
1.3.6.1.4.1.18339.20.13	Nationality (subscriber)
1.3.6.1.4.1.18339.20.10	Numeric code defining the term of address to the certificate subscriber
1.3.6.1.4.1.18339.20.11	ID for test certificates, with three possible statuses ("active", "revoke" o "expired")
1.3.6.1.4.1.18339.29.1	Name of certificate responsible
1.3.6.1.4.1.18339.29.2	Surname of certificate responsible
1.3.6.1.4.1.18339.29.3	Last name of certificate responsible
1.3.6.1.4.1.18339.29.4	VAT number of certificate responsible
1.3.6.1.4.1.18339.29.5	E-mail of certificate responsible
1.3.6.1.4.1.18339.29.6	Position, title, role of certificate responsible
1.3.6.1.4.1.18339.29.7	Department of certificate responsible
1.3.6.1.4.1.18339.29.8	Identity card type of certificate responsible
1.3.6.1.4.1.18339.29.9	Nationality of certificate responsible
1.3.6.1.4.1.18339.29.10	Address of certificate responsible
1.3.6.1.4.1.18339.29.11	Locality of address of certificate responsible
1.3.6.1.4.1.18339.29.12	Province/state/area of certificate responsible
1.3.6.1.4.1.18339.29.13	Postal Code of certificate responsible
1.3.6.1.4.1.18339.29.14	Country where certificate responsible lives
1.3.6.1.4.1.18339.29.15	Phone number of certificate responsible
1.3.6.1.4.1.18339.29.16	Mobile phone number of certificate responsible

1.3.6.1.4.1.18339.29.17	E-mail address of certificate responsible
1.3.6.1.4.1.18339.29.18	Fax number of certificate responsible
1.3.6.1.4.1.18339.30.1	Country to which it corresponds the issuance of the certificate.
1.3.6.1.4.1.18339.40.1	Qualification with which the certificate was issued
1.3.6.1.4.1.18339.41.1	Limit of liability assumed by the CA
1.3.6.1.4.1.18339.41.2	Limitation of use of the certificate by concept
1.3.6.1.4.1.18339.41.3	Limitation of use of the certificate in the amount
1.3.6.1.4.1.18339.41.4	Limitation of use of the certificate coin type
1.3.6.1.4.1.18339.42.1	Registration Authority Identification
1.3.6.1.4.1.18339.42.2	Level 1 RA Identification
1.3.6.1.4.1.18339.42.3	Issuance Reports Manager
1.3.6.1.4.1.18339.42.4	Level 2 RA Identification
1.3.6.1.4.1.18339.42.4.1	It determines whether it is an RA capable of handling short-term valid certificates. "RA authorized in issuing short term"
1.3.6.1.4.1.18339.42.8	PKI security level
1.3.6.1.4.1.18339.42.9	PKI authorized operators
1.3.6.1.4.1.18339.42.11	Name of the holder of the RA office to which the operator RA is linked to
1.3.6.1.4.1.18339.42.13	Department in which the RA operator works inside the RA office.
1.3.6.1.4.1.18339.43	Limitations automation for automatic processes
1.3.6.1.4.1.18339.45.1	VAT number of second attorney (joint powers)
1.3.6.1.4.1.18339.45.2	Name of second attorney (joint powers)
1.3.6.1.4.1.18339.45.3	Surname of second attorney (joint powers)
1.3.6.1.4.1.18339.45.4	Last name of second attorney (joint powers)
1.3.6.1.4.1.18839.45.5	Document supporting power of attorney
1.3.6.1.4.1.18839.46	It determines that it is a short term certificate. Reference value 1.

1.3.6.1.4.1.18339.47.1	UUID of Electronic Signature Device that holds the certificate
1.3.6.1.4.1.18339.47.3	If is active it indicates that signature generation data is contained in a cryptographic device
1.3.6.1.4.1.18339.56.2.1	Black list of persons and entities
1.3.6.1.4.1.18339.60.1	Micropayment system activated
1.3.6.1.4.1.18339.60.4	Signature Limit Amount
1.3.6.1.4.1.18339.85.1	Incoming hash chaining of a Digital Time Stamp
1.3.6.1.4.1.18339.85.2	Outgoing hash chaining of a Digital Time Stamp
1.3.6.1.4.1.18339.90.1	Other aspects related to the quality of the service
1.3.6.1.4.1.18339.90.2	Other aspects related to the quality of the service
1.3.6.1.4.1.18339.90.3	Other aspects related to the quality of the service
1.3.6.1.4.1.18339.91	Company creation date
1.3.6.1.4.1.18339.91.1	Legal form of subscriber
1.3.6.1.4.1.18339.92	Owned trademarks employed
1.3.6.1.4.1.18339.92.1	Distributed trademarks suffix 1
1.3.6.1.4.1.18339.92.2	Distributed trademarks suffix 2
1.3.6.1.4.1.18339.92.3	Distributed trademarks suffix 2
1.3.6.1.4.1.18339.93	Geographical area in which it operates
1.3.6.1.4.1.18339.94	Headquarters address, phone, fax, website location
1.3.6.1.4.1.18339.94.1	Subsidiaries suffix 1
1.3.6.1.4.1.18339.94.2	Subsidiaries suffix 2
1.3.6.1.4.1.18339.94.3	Subsidiaries suffix 3
1.3.6.1.4.1.18339.95	Companies with which it maintains relations
1.3.6.1.4.1.18339.95.1	Related companies suffix 1
1.3.6.1.4.1.18339.95.2	Related companies suffix 2
1.3.6.1.4.1.18339.95.3	Related companies suffix 3
1.3.6.1.4.1.18339.96	Banks with which it maintains relations

1.3.6.1.4.1.18339.96.1	Bank accounts, SWIFT codes
1.3.6.1.4.1.18339.97	Financial information relating to its activity
1.3.6.1.4.1.18339.97.1	Financial information related to its activity suffix 1
1.3.6.1.4.1.18339.97.2	Financial information related to its activity suffix 2
1.3.6.1.4.1.18339.97.3	Financial information related to its activity suffix 3
1.3.6.1.4.1.18339.98	Number of employees
1.3.6.1.4.1.18339.99	Number of distributors
1.3.6.1.4.1.18339.600	It contains the version of the RA Manager application used to process the certificate request.

I. Qualified Certificates

Certificates issued with consideration of qualified additionally incorporate the object identifier (OID) defined by TS 101 862, European Telecommunications Standards Institute on profiles of qualified certificates: 0.4.0.1862.1.1. In addition the value "Qualified Certificate" is included in the proprietary extension of 1.3.6.1.4.1.18339.40.1 OID.

The certificates which are issued with the qualification of qualified are identified in the OID 1.3.6.1.5.5.7.1.3 extension, which indicates the existence of a list of "QcStatements", according to ETSI TS 101 862. Specifically:

- QcCompliance (OID 0.4.0.1862.1.1) establishes the qualification with which the issuance is of "Qualified certificate".
- QcLimitValue (OID 0.4.0.1862.1.2) informs about the monetary value which CA assumes as a responsibility in the attributable loss of transactions. This OID contains the values sequence: coin (encrypted in accordance to the ISO 4217), quantity and exponent.
- QcEuRetention Period (OID 0.4.0.1862.1.3) determines the conservation period of all the relevant information of the certificate after its expiration. In the case of ANF AC, it is 15 years.
- QcSSCD (OID 0.4.0.1862.1.4) reports whether the certificate and keys are contained in a cryptographic token device.

II. Subject Alternative Name

Specification RFC 5280 of the IETF provides for the use of the following types of data:

- Email-based Identity.
- Identity based on Distinguished Name (DN), which is often used to construct a proprietary attribute-based alternative name, 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).

All of them can contain more than one instance (e.g., multiple e-mail addresses).

All names are verified by the issuer when they are included in the certificate.

7.2 Certificate Revocation List (CRL) Profile

7.2.1 Version number

Version 2.

7.2.2 CRL and CRL entry extensions

Fields and extensions used are as follows:

Field	Values	Mandatory	Critical
Version	V2 (version of X.509 standard)	YES	NO
CRL serial number	Unique code with respect to issuer hierarchy	YES	NO
Signature algorithm	Sha1WithRSAEncryption	YES	NO
Hash algorithm	Sha1	YES	NO
Issuer	CN= of the issuing CA SERIALNUMBER = issuing CA's VAT number OU = Issuing CA organizational unit O= Issuing CA name L= Issuing CA address S= Issuing CA city C= Issuing CA country	YES	NO
Effective issuance date	CRL issuance date	YES	NO
Date of next update	CRL effective issuance date	YES	NO
Authority key identifier	Key ID of the issuing CA	NO	NO
Distribution point	Distribution point URL and type of certificates contained	YES	NO
CRL entries	Certificate serial number Date of revocation Reason code	YES	NO

7.3 OCSP profile

7.3.1 Version number

The profile is defined in the RFC 6960 standard.

7.3.2 OCSP extensions

The Validation Authority supports signed requests*[1] and the NONCE*[2]extension.

7.3.2.1. Certification Path Validation

The OCSP consultation verifies the Certification Path and determines the status of each one of the certificates in the chain up to and including the highest Root Certificate level.

The sequence of verified elements in the construction of the Certification Path consists of at least:

1. Name of issuer of verified certificate. This must be the same as the Subject names in the issuer's certificate.
2. The format of the certificate must be X.509 v3 with DER encoding.
3. The certificate signature must be verified with the issuing certificate's public key.
4. The "AuthorityKeyIdentifier" field of the verified certificate must be the same as the "SubjectkeyIdentifier" in the issuer's certificate. Each certificate must include the field "SubjectKeyIdentifier".
5. If the certificate contains "authorityCertIssuer" verified in "AuthorityKeyIdentifier", the name must be equal to the issuer's name on the issuer's certificate.
6. If the certificate contains "authorityCertSerialNumber" verified in "AuthorityKeyIdentifier", "authorityCertSerialNumber" must be equal to "serialNumber" in the issuer's certificate.
7. It determines if the "issuing entity" CA's certificates in the certification routes include the "basicConstraints" field with the value as TRUE.
8. If "basicConstraints" is TRUE, the certificate may contain the field "pathLengthConstant" which specifies the maximum number of CA certificates which can be chained to the verified certificate. If the value is 0, it indicates that the CA may only issue end entity certificates.

   If the CA certificate doesn't contain the field "pathLengthConstraint", it means that there is no restriction in the Certification Route, unless there are restrictions in higher-level certificates. The CA Intermediate parameter must be a lower value that the one that appears in higher-level CAs.

   As such, the length of the Certification Route affects the number of CA certificates that are used during certificate validation. The chain begins with the end entity certificate which is validated and moved upwards.
9. The time check needs to be within the interval "notBefore, notAfter". The certificate must not have expired at the time of control.

10. The time check needs to be within the interval "notBefore, notAfter"–None of the lower-level certificates must have been issued before a higher-level certificate is issued.

11. It will be checked that the "keyUsage" key matches with the type of certificate.

12. If the certificate was issued as qualified, the extension "QcStatements" matches with the profile defined in the corresponding policy which is identified by the OID included in the extension "PolicyIdentifier".

*[1] The signing of the request is optional and depends on what is decided by the OCSP Validation Authority. ANF AC does not required signed requests in OCSP consultations made over the WEB service. But it may be required, depending on the OSCP service consulted, that the applicant be an authorized, subscribed user of the service. ANF AC signs OCSP answers with the OCSP certificate issued by the same issuing organization as the end entity certificates.

*[2] In concordance with RFC 6960, NONCE joins a request and an answer cryptographically to prevent spamming attacks. NONCE is included in the requests as one of the request Extensions and in the responses as one of the response Extensions. In both the request and the response, NONCE is identified by the object identifier id-pkix-ocsp-nonce while the extnValue is the value of NONCE.

8 Compliance audit

The verification of compliance with safety requirements, is defined in the document published by ANF AC "Standards and audit criteria Certification Services"(OID 1.3.6.1.4.1.18339.11.1.1)

Checks are made on-site to determine if the operating staff follows established procedures.

ANF AC carries out security management through the implementation of an Information Security Management System in agreement with the principles established by ISO/IEC 27001 which include the following measures, among others:

1. Carrying out period security checks to ensure conformity with established standards.
2. Ensuring complete management of security events in order to guarantee their detection, resolution and optimization.
3. Maintaining appropriate contact and relationships with special interest security groups, such as specialists, security forums and professional associations related to information security.
4. Suitably planning the maintenance and evolution of systems with the aim of guaranteeing good performance at all times and a service which complies with all users' and customers' expectations.

8.1 Frequency of approval controls for each entity

ANF AC subjects its PKI to an annual auditing process besides other audits which may be carried out under their own criteria whenever there is a suspicion of non-compliance of a security measure or when a key is compromised.

8.2 Identification of the personnel in charge of the audit

The PKI Governing Board determines the staff in charge of each control according to the area subject to revision, making sure that they have the necessary experience and are experts in digital certification systems.

8.3 Auditor relationship to audited entity

The PKI Governing Board can entrust this work to either internal or external auditors, but it is not able to supervise or otherwise control the team.

8.4 Topics covered by audit

The auditing object elements are as follows:

- Public key certification processes.
- Information systems.
- Process center protection.

- Service documentation.
- Conformity of the CPS with the published Policies.

8.5 Actions taken as a result of deficiency

Once an auditor's compliance report has been completed and received, ANF AC analyses it together with the auditing entity, looking for any possible deficiencies found, and designs and carries out a corrective plan to resolve these deficiencies.

Once these deficiencies have been resolved, a new audit will be completed to confirm that the solutions have been implemented and are effective.

8.6 Treatment of audit reports

The audit reports are handed to the PKI Board to be analyzed. The board will take the necessary measures according to incidents detected.

9 Other business and legal matters

9.1 Fees

ANF AC charges subscribers and the persons or entities that hire certification services regulated by this Certification Practice Statement, the fees in force at each moment.

9.1.1 Certificate issuance or renewal fees

Issuing and renewal fees for each certificate are published on the website www.anfacmalta.com.

9.1.2 Certificate access fees

Free service.

9.1.3 Status information access fees

- Free of charge:

  Access to information on the status of the certificates (OCSP publishing service revoked certificates from a date and time)that do not exceed 50 consultations a day.

- Rates applicable:

  Where it is expected a volume greater than 50 consultations per day, an agreement must be established in order to specify the estimated volume of inquiries; ANF AC resources allocated to adequately address this workload, and the price applicable to the service.

9.1.4 Timestamp request fees

Rates found at websitewww.anfacmalta.com.

9.1.5 Re-stamping request fees

Rates found at website www.anfacmalta.com.

9.1.6 Signature verification certificate request fees

Rates found at website www.anfacmalta.com.

9.1.7 Signature device fees

Rates found at website www.anfacmalta.com.

9.1.8 Fees for other services

Rates found at website www.anfacmalta.com.

9.1.9 Refund policy

Rates found at website www.anfacmalta.com.

9.2 Information confidentiality

ANF AC has a Privacy Policy. In general, it covers the following points:

9.2.1 Scope of confidential information

Confidential information is expressly declared as such and may not be shared with third parties except when demanded by law:

- The identity of the certificate's owner has been given as a pseudonym.
- Any information provided to the certification authority or registry authority by the user which doesn't appear in the digital certificate.
- All information relative to security parameters.
- Information or documents which ANF AC has classified as confidential.
- Transaction logs, including full records and the audit records of transactions.
- Records of internal and external audit created and /or maintained by ANF AC or the Registration Authorities and their auditors.

9.2.2 Information not within the scope of confidential information

The following information is considered confidential, and so is recognized by those affected, in binding agreements with ANF AC:

- Certificates issued or pending issuance.
- Binding a subscriber to a certificate issued by ANF AC.
- The identity of the signer of the certificate, the applicant in the event of third party representation, or responsibility for where the license key and any other circumstance or personal data of the holder, in the event that is significant in terms of the purpose the certificate, and is recorded in it.
- The economic uses and limits outlined in the certificate as well as any other information contained herein.
- The different states or conditions of the certificate and the date of the beginning of each of them, specifically: pending generation and / or delivery, valid, revoked, suspended or expired, and the

reason that caused the change of state.

- The Certificate Revocation Lists(CRL) and the remaining revocation status information.
- The information contained in the Service Publication of ANF AC classified as Public.

9.2.3 Disclosure of suspension and revocation

ANF AC issues Certificate Revocation Lists(CRL) that are of free public access.

ANF AC has other means of consultation of state, as outlined in section 2.5 "Publication issued Certificate Status".

9.2.4 Legal disclosure of information

As a general rule any document or record belonging to ANF AC is sent to law enforcement agencies, unless:

- The law enforcement officer is properly identified.
- It provides a subpoena duly drafted.
- The Certification Authority or Registration aware that certificates issued, or any of the instruments belonging to this PKI are being used for the commission of a crime.

ANF AC discloses confidential information only in cases provided for by law.

Specifically, records that support the reliability of the data contained in the certificate will be disclosed if required to provide evidence of certification in case of legal proceedings, even without the consent of the certificate subscriber.

9.2.5 Disclosure on request of the owner

The certificates must be published

Also the owner of the information may require ANF AC issuing a report of the details, it is stored or deposited in the Certification Authority or Registration Authority Recognized. ANF AC notifies the rate budget for that service, and upon acceptance, issues the above report.

9.2.6 Other information disclosure circumstances

Not applicable.

9.3 Intellectual property rights

ANF AC is the exclusive owner of all rights relative to electronic certificates issued by its PKI, regardless of the type, including CRL and ARL certificate revocation lists.

The object identifiers (OID) used are property of ANF AC and have been registered in the Internet Assigned Number Authority (IANA) under the branch iso.org.dod.internet.private.enterprise 1.3.6.1.4.1-IANA-Registered Private Enterprises, having been assigned the numbers:

- 1.3.6.1.4.1.18339

http://www.iana.org/assignments/enterprise-numbers

The total or partial use of any OID assigned to ANF AC or its affiliates outside of the ANF AC PKI environment is prohibited.

9.3.1 Property of certificates and information revocation

Issuing and delivery of certificates issued by ANF AC does not presuppose any change in their intellectual property rights.

ANF AC prohibits the storage of information on their certificates in repositories external to ANF AC's PKI unless express authorization is given, and especially when the aim is provision of information services on the validity or revocation status of a certificate.

Certificates and status information can only be used for objectives stated in this document.

9.3.2 Property of PKI related documents

ANF AC is the owner of all documents published within its PKI field.

9.3.3 Property of information relating to names

The subscriber retains all rights relative to the brand, product or commercial name contained in the certificate.

The subscriber is the owner of the certificate's Distinguished Name.

9.3.4 Property of keys

The pairs of keys are property of the certificates' subscribers. When a key is divided into parts, all parts of the key are property of the subscriber.

9.4 Classification of documents created by ANF AC

The full relation of documents employed by ANF AC is available at

http://www.anfacmalta.com/en/documents

9.5 Obligations

9.5.1 Of the Certification Services Provider

ANF AC MALTA, LTD., in its capacity as Certification Service Provider issuing certificates under this CPS, assumes the following obligations:

9.5.1.1 On the service provision

ANF AC certification provides services in accordance with this Certification Practice Statement, taking responsibility for compliance with all obligations in its capacity as Certification Service Provider. These obligations of the Certification Entity are the following:

- Not storing or copying signature-creation data of the person who has rendered service.
- Maintaining a system which indicates the license and if they are valid or if their application has been suspended or expired.
- Keeping, at least 15years from the date of issue of the certificate, all information and documentation relating to qualified certificates and certification practice statements applicable at all times, and on the other certificates, for 5 years.
- Check that the signer is in possession of the signature creation data corresponding to the verification in the certificate.

9.5.1.2 Of reliable operation

ANF AC guarantees:

- That the identity contained in the certificate uniquely corresponds to the public key it contains.
- The allowance of a fast and reliable service query validity of certificates in accordance with this CPS. This service is permanently available24/7/365.
- Compliance with the technical and personnel requirements required by the current legislation on electronic signature:

    1. To demonstrate the reliability necessary for providing certification services.
    2. To ensure that it can be accurately determined the date and time the certificate was issued or became extinct or suspended.
    3. Employing staff with the skills, knowledge and experience required for certification services and the safety procedures and proper management of electronic signatures.
    4. Use trustworthy systems and products which are protected against modification and ensure the technical and, where appropriate, cryptographic security for the certification processes they support, according to the Security Policy.

5. Take measures against forgery of certificates, and ensure confidentiality in the generation processes described in section 6 of this CPS and its safe delivery to the signer.

6. Use trustworthy storage systems for qualified certificates that allow verifiable authentication and prevent unauthorized alteration of the data; restrict their accessibility on the circumstances or to the persons that the signer has indicated; and allow to detect any change affecting these safety conditions.

- The correct management of safety, thanks to the implementation of a Management System of Information Security according to the principles established by the ISO/IEC27001, which includes, among others, the following measures:

  1. Perform regularly scheduled safety checks, to verify compliance with the standards set.

  2. Conduct a complete management of security events, in order to ensure their detection, resolution and optimization.

  3. Maintain appropriate contacts and relationships with special interest groups on security, as specialists, security forums and professional associations related to information security.

  4. Properly plan maintenance and evolution of systems, in order to always ensure adequate performance and a service compliant with users and customers' expectations.

9.5.1.3 Of identification

ANF AC identifies the signer of the certificate, in accordance with the present Certification Practice Statement.

9.5.1.4 Of information to users

Prior to the issuance and delivery of the certificate to the subscriber, ANF AC, or the Registration Authority on behalf of ANF AC, informs the user of the terms and conditions relating to the use of the certificate, its price, its limitations on usage, and provides documentation regarding the rights and obligations inherent in the use of services of ANF AC's certification, especially regarding escrow and privacy of electronic signature tools and electronic signature activation data.

This requirement is met by formalizing the contract for license applications and services.

ANF AC assumes the obligation to notify the signatories the cease of certification services with two months' notice in and report, if any, the characteristics of the provider to which it is proposed to transfer the management of certificates. Communications to the signatories are carried as provided herein.

ANFAC has a plan for completing the cessation of its activity, which details the conditions in which it would be performed.

All the public information on the licenses is available in the ANF AC repositories listed in this CPS.

9.5.1.5 Concerning verification programs

ANF AC provides mechanisms to verify the validity of certificates and electronic signatures in systems described herein.

9.5.1.6 Concerning the legal regulation of the certification service

ANF AC assumes all obligations incorporated directly in the certificate or incorporated by reference. The incorporation by reference is achieved by including in the certificate object identifier or other form of link to a document.

The legal instrument that binds ANF AC and the applicant or holder of key subscriber and relying party certificate and written language is understandable, given the following minimum contents:

- Indication that allows the subscriber to know and enable compliance with their obligations and rights.
- Indication Certification Practice Statement applicable, specifying, where appropriate, that the certificates are issued with the need to use secure devices of signature creation or decryption approved by ANF AC.
- Provisions relating to the issuance, revocation, and renewal of certificates.
- Statement that the information in the certificate is correct, unless otherwise notified by the subscriber.
- Consent for the storage of the information used for subscriber registration, for the provision of a cryptographic device and for the transfer of such information to third parties in the event of termination of ANF AC operations without valid certificate revocation.
- Certificate usage limits.
- Information on how to validate a certificate, including the requirement to check the status of the certificate, and the conditions under which it can reasonably rely on the certificate.
- Limitations of liability applicable, including uses by which ANF AC accepts or excludes its liability.
- Retention period for certificate application information.
- Procedures for resolving disputes.
- Applicable law and jurisdiction.
- Way that ensures the patrimonial liability of ANF AC.

9.5.2 Responsibility of the Recognized Registration Authority

The issuers can collaborate with others in the provision of their services, but nevertheless the sole responsibility of the certification services rests entirely with the Certification Service Provider. Recognized Registration Authorities are responsible to ANF AC for damage caused in the exercise of their functions, in accordance with the obligations under the relevant agreement, and must also:

- Transcribe with accuracy in the application forms of the RA Device Manager, the information collected from the source documents provided by the applicants.
- Admit only original documentation in the process of identifying, obtaining a copy of the documentation submitted by users. Such documentation shall be forwarded to the certification

authority for escrow.

- Not provide to third parties copies of the applicant's documentation, or any information thereof.
- Safeguard the RA Manager device, not allowing the use or revision thereof by unauthorized parties and incase of loss, immediately report to ANF AC.
- Notify the Data Protection Agency of the existence and activation of the RA Manager, which contains computerized personal data, using the form generated by the system automatically.
- Apply the official rates without making increase or charge for any other item other than those stipulated by ANF AC.
- In case of cessation of activity as RA, return the RA Device Manager, as well as any documentation or materials in its possession derived from the activity as a Recognized Registration Authority.
- Communicate any judicial or extrajudicial claim to occur in the course of his activity as RA.
- In relation to the information contained in the certificate or to the personal characteristics that enabled him to be a Recognized Registration Authority, report any relevant occurring changes.
- Protect and personally safeguard the RA Private Keys and the activation password, against danger of usurpation or abuse. Any suspected breach of security, must be immediately communicated and then proceed to revocation.
- Be diligent in serving the requesting users, facilitating, where possible, information of the original documents that will be required and avoiding unnecessary waiting.
- Do not use the copies accompanying the original documentation of the applicant. Any hard copy or digitized will be obtained directly by the Registration Authority.
- Diligently communicate to ANF AC the existence of applications of emission of certificates, especially those rejected.
- Not intervene in the generation of the signature creation data of users, nor to allow to be informed of the activation PIN chosen by the applicant.
- Store in a secure and permanent way, copies of the documentation provided by the user to perform the request and the documents generated by the RA Manager, during the petition, registration, or revocation process.
- Collaborate with the audits conducted by ANF AC to validate the renewal of their own keys.
- Respect the privacy of applicants and certificate holders.

9.5.3 Responsibility of subscribers and certificate responsible

The responsibilities of the holders of the certificates are set out in the corresponding Certification Policies. Furthermore, in general it is established that:

- Subscribers of ANF AC certificates are responsible to comply with all obligations under this document, its attachments, Electronic Signature Policy and Certification Policy, limiting and adapting the use of the certificate and electronic signature systems under the scope of this PKI for lawful purposes and in accordance with an honest and loyal conduct with the community: ANF AC, RAs, users and relying parties. The following list is merely illustrative and not restrictive.

The subscriber agrees to:

- Ensure that all information contained in the Certificates is true.
- Ensure that the documentation provided in the certificate application is true and authentic.
- At the time of receiving the electronic certificate urgently, will check its correspondence with the request. To do so, it will use the certificate verification option which includes generating device signature creation data. If the check is negative, notify the carrier immediately to ANF AC.
- Use the certificate within the constraints that are imposed by the Policy Certification and the Electronic Signature Policy.
- In case the certificate outlines "Issuer Statement, Attributes and Limitations of use", shall comply with the specified.
- Diligently safeguard the container of signature creation data and the secret activation key, as well as the username and password to access the General Registry.
- Exclusively use ANF AC's devices for the storage of signature generation and for the creation of electronic signatures, as well as for their further verification.
- Keep ANF AC's cryptographic devices updated, following installation and maintenance instructions for this purpose, and ensuring that the devices have not been neglected in ANF AC's protection.
- Maintain ANF AC'S cryptographic devices updated, following installation and maintenance instructions given for this purpose, and ensuring that the devices have not been neglected the protection provided by ANF AC.
- Verify the attributes to be included in a signature, before creating an electronic signature using a cryptographic device of ANF AC, and only activate the signing process after agreeing with them all.
- Accept all electronic signatures related to owned certificates, provided they have been created using current certificate.

The essential activation of signature creation data, by the signatory by using his secret key, implies:

- The full consent of electronic signature creation and acceptance of the Electronic Signature Policy associated with this signature.
- The request for revocation of the certificate when safety of the signature creation data, or the secret activation data is compromised, or the personal information has undergone any modification.

- Upon revocation of the certificate, the subscriber's obligation to cease their use.

Users guarantee that the names and domain names outlined in the application form, and contract services, do not infringe the rights of third parties in any jurisdiction with respect to industrial property rights and brand, and will not use the domain and distinguished name for illegal purposes, including unfair competition, theft and acts of general confusion.

Applicants and in general, users of certificates, will indemnify ANF AC for damages that may result in the realization of these activities. They also commit to:

- Provide the RA original documentation and information considered accurate and complete, and to notify any modifications that occur on the same.
- Pay the fees for services rendered to him by the CA, or by the RA.
- Do not manage applications in case of any conflict of interest with ANF AC or members of the PKI Governing Board.
- Perform the certificate application under the principle of good faith, and with the sole aim of using it for commonly accepted purposes.

9.5.4 Responsibility of trustworthy third parties

The third party considered as receiver, trusts in good faith in the electronic file which is digitally signed by a user of ANF AC, and that besides relying in that signature, comply with the following obligations:

- Verify the signature using electronic signature verification devices of ANF AC.
- Check the condition of validity of the certificate using one of the methods permitted under this CPS.
- Act diligently.
- Assess the adequacy of the certificate associated with the digital signature, according to: the type of certificate, the statement of the issuer, use limitations that are outlined therein, and stated in this CPS and its corresponding Certification Policy.
- Seek advice from the ANF AC "Customer Service Office", in case of doubt.

ANF AC makes available to relying third parties the certificate revocation lists. The third party can access this information for the sole personal use of validating the status of a certificate of interest, and in no case for the provision of services to third parties.

Recipients who do not meet the requirements may not be considered in good faith.

9.5.5 Of the publication service

Not applicable because of the Publication Service not being an independent entity.

9.6 Civil Liability

9.6.1 Of the Certification Service Provider

ANF AC is liable for those damages that derivate, **in general**:

- Of a breach of the obligations contained in this CPS, the corresponding Certification Policies and Chapter 426 Electronic Commerce Act.

And specifically:

- ANF AC will respond for damages caused to any person for failure or delaying including the validity of the certificates in consultation service, or in the termination or suspension of the certificate validity.

- ANF AC assumes all liability to third parties for the performance of the people it has delegated tasks necessary for the provision of certification services.

In any case, the following cases are generally excluded:

- ANF AC will not be liable for any direct, indirect, special, incidental, consequential, from any lost profits, loss of data, punitive damages were foreseeable or not, arising in connection with the use, delivery, license, performance or non-performance certificates, digital signatures, or any other transaction or service offered or referred to in the Certification Practice Statement in case of misuse, or when used in transactions involving a higher than stated in the compensation limit expressed by the CA.

- ANF AC assumes no liability or responsibility other than those detailed in this Certification Practice Statement.

Specifically with the **subscribers and the managers of the certificates**:

- In case of breach of obligations in this CPS, the corresponding Certification Policy and Chapter 426 Electronic Commerce Act.

- In particular the obligations outlined in this CPS.

And **specifically with relying third parties**:

- In case of breach of obligations included in this CPS, in the corresponding Certification Policy and Chapter 426 Electronic Commerce Act.

- In particular the obligations outlined in this CPS.

9.6.2 Of the Registration Authority

In case of breach of obligations in the present CPS, in the corresponding Certification Policies, in Chapter 426 Electronic Commerce Act, in the certificate applications they manage, and in the terms established in the agreement that formalizes their activity, the Recognized Registration Authorities (RA) will be responsible for damage caused in the exercise of the assumed functions.

9.6.3 Of the subscriber

The subscriber is responsible for all authenticated electronic communications and authenticated documents, which have used a digital signature created with private key, and in which the certificate has been validly confirmed through ANF AC verification services.

Within the period of validity of the certificate, or as long as there is no record of the certificate revocation in ANF AC registry, the liability that arises from the unauthorized use and /or misuse of the Certificates, shall in any case be of the subscriber.

With the acceptance of the Certificate, the Subscriber agrees to indemnify and, if necessary, to compensate ANF AC, Registration Authorities and Third Party Recognized Relying any action omission which causes damages, losses, liabilities, litigation costs or of any kind, including professional fees, which may be incurred. Especially when it comes:

- from breach of the terms set in the certificate application and in the certification service contract linking him to ANF AC;
- from the use of Certificates in operations that have not respected the usage limit or that are prohibited, as expressed in this CPS and corresponding Certification Policies:
- from intentional falsehood or mistake committed by the subscriber;
- of any omission of a fundamental fact in the certificates, made negligently or with intent to deceive;
- from breach of the duty of care of private keys, and taking reasonable precautions to prevent the loss, disclosure, alteration or unauthorized use of the private keys;
- from breach of the duty to maintain the confidentiality of the signature creation data and protect all accessor disclosure;
- from breach of the duty of requesting the suspension or revocation of the certificate in the event of doubt as to the maintenance of the confidentiality of their signature creation data;
- from breach of the duty to refrain from using the signature creation data from the time expiry of the period of validity of the certificate or from the moment the service provider notifies the loss of validity;
- from reach of the duty to report promptly any change in circumstances reflected in the certificate;

9.6.4 Of trustworthy third parties

The third party trusting a non-valid certificate or a digital signature that has not been verified with ANF AC devices developed and approved for that purpose, assumes all risks related and will not be able to demand responsibility to ANF AC, the RAs, or the subscribers for any concept derived reliance on such certificates and signatures.

As such, ANF AC will not be liable for damages caused to subscribers of third parties, if the recipient of electronically signed documents breaches any of its obligations under the present CPS, the corresponding

Certification Policies, Chapter 426 Electronic Commerce Act and specially for breach of obligations described in this document.

9.6.5 Of the publication services

This does not apply since the publication service is not a separate entity.

9.7 Financial responsibility

9.7.1 Indemnity clauses

ANF AC in this document, in the Certification Policies and in agreements linking to the Subscriber, to the Registration Authorities and to relying third parties, includes indemnity clauses for violations of duties or applicable law.

9.7.2 Limits of damage compensation

ANF AC notes that:

- Certificates issued as not qualified, cannot be used for operations involving financial risk, and therefore the compensation limit is zero Euros.

- Certificates issued as qualified include the authorized limit assumed by the CA, remains established by the same certificate, specifically in the extension "QcStatements" in the "QcLimitValue" field OID 0.4.0.1862.1.2.

  If no amount is fixed, it should be interpreted that the certificate cannot be used in operations involving financial risk, and therefore the compensation limit is zero Euros.

9.7.3 Financial capacity

ANF AC, bears the risk of liability for damages that may result from use of issued certificates, thus has signed the relevant liability insurance and in accordance with the CA/Browser Forum emission guidelines and management of Extended Validation SSL, has the extent of FIVE MILLION EURO (5.000.000. €).

The information relating to the insurance policy is as follows:

- Insurer: CFC Underwriting Limited. Registered in England and Wales, Nº 3302887. VAT number 135541330. Authorized and regulated by the Financial Services Authority. FRN: 312848.

- Policy number: BA 059760 A.

The coverage of this policy reaches Registration Authorities Recognized by ANF AC.

9.7.4 Fiduciary relationships

ANF AC employs no fiduciary agent, neither as a representative of users or of trusted third parties in the issued certificates.

9.7.5 Administrative processes

ANF AC and Registration Authorities have sufficient resources to maintain operations and perform their tasks. The registration authorities are reasonably able to bear the risk of liability to subscribers and relying third parties.

9.7.6 Exemption from liability to the Subscriber

ANF AC assumes no responsibilities derived from denials of service, apart from those cases in which the service provision contract specifies a penalty.

ANF AC assumes no responsibility for transactions carried out by subscribers through their use of certificates.

ANF AC assumes no responsibility when the owner makes use of the certificates using instruments which are not produced by ANF AC.

ANF AC makes use of other extensions established in the Certification Policy corresponding to the type of certificate in question.

With the exception of what is written in this document, ANF AC assumes no other compromise and makes no other guarantee, and also assumes no other responsibilities with regard to certificate owners, their legal representatives or certificate managers.

9.7.7 Exemption from liability to the relying third party

ANF AC assumes no responsibility when the trusted third party does not assume the obligation to verify the certificate's status, using verification instruments provided by ANF AC.

ANF AC makes use of other extensions established in the Certification Policy corresponding to the type of certificate in question.

With the exception of what is written in this document, ANF AC assumes no other compromise and makes no other guarantee, and also assumes no other responsibilities with regard to trusted third parties.

9.8 Interpretation and enforcement

9.8.1 Applicable law

Legislation applicable to this document and underlying legal relationships is that of the Republic of Malta.

This CPS must be interpreted in accordance with legislation in force, its resolutions in development, and specific legislation which affects its services, especially as regards personal data protection and legislation on user and consumer protection.

9.8.2 Jurisdiction clause

All parties are expressly submitted to the Courts and Tribunals of Malta renouncing their own jurisdiction, if different.

9.8.3 Dispute resolution procedures

9.8.3.1 Application procedure for extra-legal resolution of conflicts

ANF AC voluntarily submits to the institutional arbitration of TACED which takes charge of arbitration and the administration of arbitration for any legal problem which may arise while carrying out their activities. This arbitration will be made in accordance with the Regulations, and ANF AC is obliged to comply with the decision taken.

In the case that one of the opposition parties do not accept this procedure, the information in the following section will be followed.

9.8.3.2 Legal procedure

All parties are expressly submitted to the Courts and Tribunals of Malta renouncing their own jurisdiction, if different.

9.8.4 Notifications

Every notification, demand, request or other communication required under the practices described in this CPS shall be made by document or digitally signed message.

Electronic communications shall be effective once received by the addressee to whom they are addressed.

9.9 CPS and Certification Policies administration

The evolution of ANF AC's certification services requires that this CPS, its Annexes and the Certification Policies are subject to modifications. A numbered version system has been established to correctly differentiate of successive editions produced by these documents.

Any necessary modification must be justified from a technical, environmental, legal or commercial point of view. All technical and legal implications of the new version's specifications must be considered.

Change control will be established to guarantee, in any case, that the resulting specifications comply with the requirements and give cause for the change.

9.9.1 Validity period

This Certification Practice Statement comes into force on the date written in the "Issue date" field in section 1.2 of this document. It expires on the date that a new version of ANF AC's CPS comes into force.

The same validity period applies to ANF AC's Signature and Certification Policies.

9.9.2 Effect of termination

All obligations, rights and restrictions established in this Certification Practice Statement and its respective Electronic Signature and Certification Polices created during its validity period remain after its expiry.

9.9.3 Approval procedure

The Head of the Legal Department and the head of the Technical Department, will discuss the proposed changes in the CPS and policies, are aligned with the latest versions of the "Baseline requirements for the Issuance and Management of Publicly-Trusted Certificates" prepared by the CA / B Forum, and that they serve the requirements that gave rise to the proposed modification. Also assume the realization of an annual update control of the CPS, Certification Policies and other related documents, issuing the corresponding version maintenance report or proposals for change.

All reports are submitted for approval by the Governing Board of the PKI, which assumes responsibility for verifying compliance and, where appropriate, issuing order of application thereof.

9.9.3.1 Modifications that do not require a new document or version change

ANF AC may make changes to this document without publishing a new document and therefore, applying a version change as long as they are no material changes, such as:

- Corrections of typos
- Modifications in URLs
- Changes in contact information

In these cases, ANF AC will publish an annex attached to the document concerned. This Annex shall be signed electronically and contained in the ANF AC Publication Services.

9.9.3.2 Modifications that require a new document or version change

Any changes not covered in the previous section, involves the publication of a new document and a version change.

9.9.4 Notification of the publication of a new CPS and Policies

This follows the provisions of the “Publication and notification policy” section of this document.

9.9.5 Severability and survival

If any section of this document or policies is considered legally invalid or unenforceable, it shall be deemed as not existing, lasting the rest of obligations, rights and restrictions set forth herein.

The invalid or incomplete clause may be replaced by an equivalent and valid agreement of the parties.

The rules contained in sections: Obligations, Liability and Confidentiality, shall survive the termination of the life of this Certification Practice Statement.

9.9.6 Entire agreement and notification

None of the terms of this Certification Practice Statement directly affecting the rights and obligations of ANF AC and not affecting the rest of the parties, may be amended, waived, supplemented, modified or removed except by written document authenticated by ANF AC. This shall not suppose an extinctive renovation, but a mere modification, and shall not affect other rights and obligations of the other parties.

The reports should be directed to:

ANF AC MALTA, Ltd.

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

Reports may be made personally or by written notice. In any case there must be a reliable way to ensure the identity of the person involved in the communication. In case of representing a third party, there must be sufficient proof of its ability to represent.

9.10 Customer service office

ANF AC promises to provide free customer service to users and recipients.

9.10.1 Office purpose

This service will answer all commercial, legal and technical consultations relating to:

- Current electronic signature legislation in force.
- This CPS, Annexes, Certification Policies and certificate requests.
- Installation and use of devices related to electronic signatures.
- Installation and use of provided software.
- Generation and use of provided containers and, in general, anything related to the provision of certification services carried out by this AC.
- General consultations on basic Public Key Infrastructure, digital certificate and electronic signature concepts.

They also carry out various operations that this CPS, its Annexes and its Certification Policies specify, in the name of the user of the person they represent.

9.10.2 Consultation procedure

Consultations are carried out through an e-mail sent to: info@anfacmalta.com

They must include the username of consulting party or, if a recipient, of the receiving signature. Consultations made in this way are answered in the same manner.

There is also a personal customer service via telephone at (+356) 2299 3100 (Malta).

9.10.3 Claim procedure

Every notification, demand, request or other communication required under the practices described in this CPS shall be made by document or digitally signed message.

It is also possible to visit the Customer Service Office in person.

ANF AC will answer the claim form in writing in a period of no more than 15 working days. If the answer is not satisfactory, that specified under the "Dispute Resolution Procedures" section will be followed.

9.10.4 Identification procedure

Persons who go to the Customer Service Office must be reliably identified through an original passport or national ID card. Those persons acting on behalf of third parties must show that they have sufficient legal power to do so.

10 Personal data protection

10.1 Introduction

ANF AC requires certain personal details from applicants in order to carry out its actions as a Certification Services Provider. It is also necessary to provide public access to information contained within certificates and determine their status in order to provide a suitable public PKI service. As such, ANF AC has the corresponding authorization from the owner of the information.

Personal data used in ANF AC's certification system are held at basic and medium security levels and ANF AC, is the Data Controller, which must adopt suitable security measures for all data held.

ANF AC promises not to give or loan information to third parties to which they would have access due to their certification service provision without the express consent of the affected user. This data is exclusively used to provide the services required.

ANF AC promises to protect the data received from certificate applicants or the Registry Authorities, enforcing the appropriate security measures at the Security Level required according to its corresponding characteristics and in agreement with legislation in force.

ANF AC employees and any other person who handles the information are advised on the confidentiality obligations written in this section, subscribing to corresponding confidentiality compromises before accessing them, and being informed about the security measures which must be adopted. ANF AC provides a copy of this CPS, training and legal assistance to every operator to answer any question or doubt they may have.

This CPS and its addendum are obligatory for all staff with access to personal data and systems which deal with this information. The objective is to provide efficient checks which ensure that business data is not subject to unauthorized loss, dissemination or modification.

For this reason, security measures, procedures, rules and regulations have been defined which achieve and maintain a high information security level related to how critical the data and processes are which are stored and managed by the Entity.

The Recognized Registration Authorities and all ANF AC staff in charge of taking information from certificate applicants, legal representatives, certificate owners, trusted third parties or any other natural person attended in the name of ANF AC will verify that the owner of information gives their consent that their data be processed, and is informed about what they will be used for and if they are included in an automated file by ANF AC, as well as their rights to access, correction, cancellation and opposition, and how to exercise these rights.

If the information was not taken directly from the interested parties, ANF AC will expressly, precisely and unmistakably inform these parties within the three months following the registration of the information.

The owner of the information may exercise their access, correction, cancellation or opposition rights by going to the Customer Service Office specified in section 9.8.

10.2 Legal framework

Certification Service Providers' Certification Practice Statement is considered as a security document in terms of other personal data protection legislation in force. The CPS shall also be compliant with the applicable data protection legislation.

10.3 Creation of files and official registration

ANF AC must process its subscribers' information to fulfill its obligations as a PSC.

ANF AC is the Data Controller and acts as the Security Manager in its area of Jurisdiction, formally assuming the role of coordinating and controlling appropriate security measures.

In summary, below is a list of files subject to security measures established in this document, together with their corresponding security level:

File name	CLIENTS(basic security level)
Description	Data on name, address, national ID card number, method of payment for electronic signature service provision.
Purpose	Commercial relationship management in all aspects and electronic signature services.

File name	USERS (basic security level)
Description	Digital certificate subscribers' personal details.
Purpose	Management and maintenance of persons who have requested digital certificates.

File name	ELECTRONIC CERTIFICATES (basic security level)
Description	Information on electronic certificates issued by the company.
Purpose	Management of issuing, administration and public consultations of certificates issued by the company.

File name	EXTERNAL COLLABORATORS (basic security level)
Description	Files containing personal data of collaborators external to the company.
Purpose	Management and control of professional relationships with collaborators external to the company.

File name	SUPPLIERS (basic security level)
Description	File containing company providers.
Purpose	Management and control of commercial relationships with providers to the company.

File name	HUMAN RESOURCES (medium security level)

Description	File containing data of staff internal to the company.
Purpose	Company human resources management.

File name	CALLS RECORDING (medium security level)
Description	Recording file of calls of customers and suppliers.
Purpose	Compliance of obligations for provision of electronic signature certification and quality management.

File name	BLACK LIST (medium security level)
Description	List of natural and legal persons that cannot obtain an electronic certificate.
Purpose	Compliance of obligations for provision of electronic signature certification services.

File name	VIDEO SURVEILLANCE (high security level)
Description	Video surveillance systems installation in the organization because of security reasons.
Purpose	Security control in the organization facilities.

File name	FINGER PRINT (high security level)
Description	Electronic certificate applicant or legal representative finger print, as a part of the identification process.
Purpose	Electronic signature certification services provision.

More information can be found in document OID 1.3.6.1.4.1.18339.39.8.1 "File registration and authorization regulations".

10.4 Scope of application

This CPS is the Security Document relating to personal data protection.

When creating this CPS, it has followed the specification RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" of the Internet Engineering Task Force (IETF), and considering multiple ANF AC organizational and security aspects and Chapter 440 Data Protection Act.

This Security Document is obligatory for all staff internal or external to the entity that has access to personal data which is the responsibility of the entity.

Documents listed in section "Classification of documents created by ANF AC" which are classified as "not public" and which establish procedures and rules to be followed with regard to data protection have been made available to all staff with access to personal data, and are included in documentation given to staff when hired, with the objective of having staff comply with legislation in force.

10.4.1 Staff functions and obligations

This Certification Practice Statement is known by all ANF AC and is obligatory.

An organizational model has been created which establishes the functions assumed by each department in terms of data processing and security, specifically:

ANF AC: the Manager of the Files. Assumes legal responsibility for the security of data contained in the files and notifies the General Register of Data Protection of any files created.

PKI Governing Board: this is the organ which assumes Security Commission functions which maintain the CPS. Adopts and implements security measures necessary so that staff involved in processing information know and assume their responsibilities and have the necessary preparation to carry out their work correctly. Coordinates the various operational areas, both internal and external with third parties.

Security Manager: the director of the Legal Department formally assumes the role of Security Manager. Coordinates and controls security measures applicable to all legal aspects. Collaborates with the Data Controller and the Security Commission in the distribution of the security document, ensuring it is complied with.

Technical File Manager: the Director of the Technical Department. They are in charge of deciding the various IT Systems operational aspects from a functional point of view, as well as controlling and applying IT security measures.
Collaborates with the Data Controller and the Security Commission in the distribution of the security document, ensuring it is complied with.

Administrative File Manager: the Director of the Administrative Department. They are in charge of all administrative process which deal with documentation containing personal data, data entry processes and attending the requirements that information owners carry out. Collaborates with the Data Controller and the Security Commission in the distribution of the security document, ensuring it is complied with.

Processing staff: these are the people that process personal data when carrying out their duties.

All above-mentioned staff are obliged to respect the regulations and procedures specified in this CPS in its capacity as Security Document, as well as all obligations established in legislation in force.

More information can be found in document OID 1.3.6.1.4.1.18339.39.10.1 "Staff Functions and Obligations"."

10.4.2 File storage systems

Within the structure of IT systems which makes up ANF AC, there are three subsystems which process data. Specifically:

- Certificate management subsystem. Receives the identification documents, the requested certificates and is responsible for issuing them.

- Administration subsystem. Assumes the internal management of the organization, providers, human resources, customers and invoicing.
- Analysis and information checking subsystem. In charge of verifying the identification of the applicant, a legal representative's capacity to act in that role, and the veracity of the attributes requested for inclusion in the certificate. Issues decision on approval or denial of service.
- Publication subsystem. In charge of publishing the certificate revocation lists (CRL) and the certificate repositories.

More information can be found in document OID 1.3.6.1.4.1.18339.37.5.1 "Information Systems Descriptions".

10.4.3 Backup and recovery copies

Incremental back-up copies are made daily, and a full system image is taken every month.

Data recovery is made with the authorization of the Data Controller.

If the restoration is caused by a system attack, the Technical Data Controller must obtain authorization from the data owners before restoring the information.

If the incident is a random IT system issue, the back-up procedure established by the Technical Department will be followed.

More information can be found in document OID 1.3.6.1.4.1.18339.37.3.1 "Technical documentation on back-up copy and data recovery procedures".

10.4.4 Access control

The Administrative Manager and the Data Controller, together with the Security Manager, will determine the persons authorized to make use of the personal data processing equipment, always based on the need to correctly manage ANF AC's services in their job role. The employee will be informed of the functions they are expected to perform and how best to achieve this.

Only the Security Manager is authorized to concede, alter or annul access authorized to information and resources.

All equipment which has access to personal data is considered as under restricted access.

All information stored on ANF AC's corporate network, whether statically, in e-mail messages, or any other physical medium is property of the company and is confidential.

Persons working in security are in charge of determining, implementing, managing, authorizing, inspecting or revalidating, according to the situation, the combination of media and security measures, as well as regulations and procedures which ensure physical access control.

More information can be found in document OID 1.3.6.1.4.1.18339.39.2.1 "Physical access control".

10.4.5 Use of real data in tests

The use of real personal data to carry out tests is prohibited, and the test environment is completely separated from the real one.

10.4.6 Regulations associated with the security document

ANF AC has a collection of regulations which guarantee the protection of Personal Data processed while carrying out its duties and answering the obligations established in the legislation in force.

Said regulations are applied to all areas of work, staff, external collaborators and IT systems, regardless of the medium (IT, paper, video, etc.)

The relationship of documents published by ANF AC is detailed in section 9.4 "Classification of documents created by ANF AC" of this document. ANF AC promises to keep these documents maintained at all times, revising them whenever any relevant changes are produced in the IT system or the entity's organization. ANF AC must also be familiar with all personal data security legislation in force.

Staff affected by this Security Document know and must comply with any part which affects their duties. Non-compliance of obligations and security measures established in this document by staff will be sanctioned using the various disciplinary measures considered in working regulations in force at the time, while protected from repeated damage generated by the company, either for loss of earnings or for other damages caused.

The security Manager is in charge of keeping the Security Document up to date and is in charge of communicating any changes to staff that may be affected.

10.5 Material scope

The following security regulations are applied to protected resources. A resource is any component part of an IT system. The following components can be identified as protected resources:

- Automated files.
- IT applications, databases and operating systems.
- Platforms, equipment, and data processing and support systems.
- Communications systems and equipment.
- Buildings.
- Information files and repositories on paper.

The scope of applications consists of systems and/or media which are somehow related to the storage or processing of files containing the entity's personal data.

Security measures are classified into three levels depending on the nature of the information in relation to the greater or lesser need to guaranteeing the confidentiality and integrity of the information:

- Basic Level: Applied to files which hold personal data.
- Medium Level: Files which contain data relating to the commission of administrative or criminal infractions, the Ministry of Finance (in these two cases, they must be public sector), financial

services and those which fall under article 29 of the LOPD (provision of solvency and credit services).

- High Level: Files which contain data on ideology, religion, beliefs, racial or ethnic origin, health, sex life, or information taken for legal reasons without consent (in this last case, must also be public sector).

10.6 Identification and authentication

General principles:

1. ANF AC identifies and authenticates users who access its Information System.
2. The Security Manager supervises logging into and out of any system and application, and modifications to user access rights.
3. Given the importance of users' access to the Information System, the Security Manager must always have up-to-date knowledge of who is authorized to access the Information Systems.

ANF AC employees have devices which have incorporated biometric identification and system authentication systems through electronic signatures. In some processes, authentication can come through the introduction of a username and password. If this is the case, the Access Key Policy is followed.

More information can be found in document OID 1.3.6.1.4.1.18339.45.3.1 "Access Keys Policy".

10.7 Modification of information system data

Modification of data means the changing of any application information, either directly or indirectly, using any software tool which is not the correct application for data processing by users, using permissions or tools which are not used in daily working.

These procedures are described in OID 1.3.6.1.4.1.18339.37.3.1 "Technical documentation on back-up copy and data recovery procedures".

10.8 Temporary files processing

In document OID 1.3.6.1.4.1.18339.39.6.1 "Temporary files processing regulations", the method that ANF AC uses to process temporary files which hold personal data is described.

10.9 Opposition, access, correction and cancellation of data

In the document of OID 1.3.6.1.4.1.18339.39.9.1 "Procedure for information owners exercising their rights", the procedures for how to exercise rights to opposition, access, correction and cancellation of personal data is described.

10.10 Access to data through communication networks

The security measures required to access personal data through networks and communications ports, as well as security servers (firewalls, routers, anti-spam), guarantee a level of security equivalent to that of local access.

10.11 Method of working outside of the premises in which the file is stored

Carrying out processing on personal data outside of the premises in which the file is stored must be expressly authorized by the Data Controller and the same level of security as the file requires must be guaranteed.

The Manager of the working area must create a plan which specifies, point by point, the steps taken to guarantee the security of the files outside of the organization.

Processing time and date
User name
Processing operator
Duration of processing outside of the organization
Files
Finish time and date
Authorization

10.12 Staff functions and obligations

With the aim of complying with legislation in force, ANF AC has established a series of obligations which must be read, accepted, complied with and respected by all staff.

To ensure that all staff knows the security regulations which affect their duties, as well as the consequences of non-compliance, they must acknowledge receipt of security documents given to them.

ANF AC, as the Security Manager, will also periodically information staff on security updates as regards personal data.

In document OID 1.3.6.1.4.1.18339.39.10.1 "Staff Functions and Obligations", all staff functions and obligations relating to LOPD are described and identified to those responsible.

10.13 File structure and systems which process them

With the aim of complying with legislation in force, ANF AC publishes its file structure and describes the IT Systems which process them.

In document OID 1.3.6.1.4.1.18339.39.7.1 "Data File Structure", the file structure and the description of the personal data included in the files at basic, medium and high levels are published.

The description of the IT Systems which process said files is published in document OID 1.3.6.1.4.1.18339.37.5.1 "Description of the IT systems".

10.14 Notification, management and incident response regulation

With the aim of complying with legislation in force, ANF AC makes the following notification, management and incident response regulations available, understanding by "incident" any anomaly which affects or may affect the security or integrity of data. The procedure is detailed in document OID 1.3.6.1.4.1.18339.37.5.1 "Incident Management Regulations".

10.14.1 Notification

Any person that forms part of the ANF AC staff or who temporarily provides their services there must notify the Security Manager of any anomaly which they detect which affects or may affect the security of the data. Any delay in notifying incidents constitutes a breach of the contractual good faith, among other possible infractions, which is punishable according to working laws and/or relevant business practices.

10.14.2 Management

The Security Manager must register the incident in the corresponding application and send it to be resolved.

10.14.3 Response

Those responsible for resolving the incident must provide an answer in the least time possible, guaranteeing at all times that the security and integrity of the data is not compromised. Once the incident is rectified, the File Controller will be informed.

10.14.4 Record

A record must be created in which the following is stated:

- Type of incident and when it was produced.
- Person who made and received the notification.
- Effects derived from said notification.

The File Controller is responsible for ensuring incident records are kept up-to-date.

10.15 Internal control and audit

1. Internal Control. The Security Manager is responsible for regularly checking that this Security Document is kept up to date, with a frequency of at least once a year.

2. Auditing. Every two years, an audit (internal or external) of IT systems and data processing installations will be carried out to ensure they comply with legislation in force.

The audit report will judge whether the measures and checks are suitable, identifying any deficiencies and proposing corrective measures and any necessary complements.

Auditing reports will be analyzed by the Security Manager who will pass on conclusions to the File Controller to adopt necessary corrective measures, and will be made available to the Data Protection Agency.

10.16 Notification, management and incident response procedure

In order to carry out recovery procedures, the written authorization of the File Controller is necessary.

10.17 Additional high level measures

Measures listed below are applied to files with a high level of security as indicated in document OID 1.3.6.1.4.1.18339.39.7.1 "Data File Structure", in the case that the Entity has files with this classification.

10.17.1 Access control and digital information confidentiality

For every access made, the username, date and time of the access, the file accessed, the type of access and if it was authorized or denied.

If the access was authorized, this record remains in the access registry. The access registry is saved for two years.

It is prohibited to deactivate the access registry mechanisms which are controlled by the Security Manager.

The security manager is in charge of revising, monthly, the control information recorded, preparing a report of all revisions made and any problems detected.

10.17.2 Media management

The distribution of media containing high-level security data is done by enciphering the data, or using any other mechanism which guarantees that said information is neither legible nor able to be manipulated during transport.

These media are identified using a legible labelling system with a specific meaning, which allows users with authorization to access the media and documents to identify their contents, and that make identification difficult for any other persons.

Processing of personal data on portable devices which don't allow enciphering is to be avoided. If strictly necessary, it will be recorded in this Security Document and measures will be adopted which take into account the risks of carrying out processes in unprotected environments.

10.17.3 Physical access control

Only staff authorized in the security document may have access to places where physical equipment is installed which support the IT systems.

If the media is not digital, access to documentation will be limited exclusively to authorized staff.

Mechanisms will be established which allow identification users who access files when multiple users have the access to do so. Unauthorized access attempts at high security level must remain clearly registered in the Security Document.

10.17.4 Telecommunications

Transmission of high security personal data and remote connections through telecommunications networks are made by enciphering said data or using any other mechanism which guarantees that the data is neither readable nor able to be manipulated by third parties.

10.17.5 Registry model of high level personal recorded data

Data transmitted
Encryption method
Date and time of the transmission

10.17.6 Procedure to conduct backup and data recovery

A back-up copy of the data recovery procedures is stored in a place different to that where the IT equipment they deal with is stored, complying with all required security measures.

10.17.7 "Access log" monthly record model

Access to high security personal data, once verified, will be recorded in a monthly report which must include the following information:

File name
Date and time in which the access was made
File accessed
Type of access and if authorization was given
Record accessed
Management made on the file
Security Manager authorization