Validation Policy

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

Security Level

Public Document

Important Notice

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

Telephone: (+356) 2299 3100

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

Index

1 Introduction

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

This document aims to describe the functioning of ANF's Electronic Certificate Validation Services and to establish the conditions of use, obligations and responsibilities of the different entities involved.

This Certificate Validation Policy is subject to the Certification Practice Statement of ANF Certification Authority.

A Validation Authority is a Certification Services Provider that provides certainty about the validity of electronic certificates and electronically signed documents at any given time.

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

1.1 Presentation

The Certificate Validation Service is one of the essential elements that, together with the "Electronic Time Stamping" service, allow long-term validation of electronic signatures. Through OCSP Responder, the validity of the electronic certificate is guaranteed at the exact moment when the signature of a document was produced, validation is extended to the entire certification route.

In this way, Certificate Validation becomes a high added value service, fundamental in electronic transactions that require long-term legal evidence.

1.2 Identification

Document name	Validation Policy
Version	1.0
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.55.1.1
Publication date	November 15th, 2016
Expiration date	Not applicable
Related CPS	Certification Practice Statement (CPS) of ANF AC
Location	www.anfacmalta.com

1.3 Community and applicability

1.3.1 Intervening entity and persons

- Validation Authority
- Subscribers
- Relying Parties

1.3.1.1 Validation Authority

A Validating Authority is a Qualified Trust Service Provider which, pursuant to Regulation (EU) 910/2014 of the European Parliament and of the Council, and the Spanish Law 59/2003, of electronic signature, provides certainty about the validity of the electronic certificates.

ANF AC as Validation Authority, offers various computer systems to determine the validity of electronic certificates, all described in the corresponding section of this document.

1.3.1.2 Subjects

As defined in the CPS of ANF AC.

1.3.1.3 Relying Parties

As defined in the CPS of ANF AC.

1.4 Uses of the validation service

1.4.1 Allowed usage

ANF AC validation services can only be used to address validation needs as subject or trusted third parties.

1.4.2 Prohibited usage

It is expressly prohibited to use the validation services of ANF AC to provide validation services to third parties. This prohibition extends specially to processes in which a multivalidation platform of a third entity outside the transactional, that is to say that does not meet the requirements of being considered a subject or relying party, operates as a mere intermediary in the formulation of the query.

It is established as a penalty for the unauthorized use of these services, the cost of 1 euro per query made to any of the ANF AC validation services, either to the OCSP Responder servers, or by any other

validation service, present or future, which ANF AC puts into operation. The minimum penalty is set at 10,000 €.

The use of validation services presupposes an explicit knowledge of this document, and therefore an acceptance of the penalty that will be applicable.

1.5 Definitions and acronyms

As defined in the CPS of ANF AC.

2 Description of the Validation Services

The Validation Services of ANF AC allow to know the validity of the electronic certificates, in addition, the computer application that allows to determine the integrity and authenticity of the electronic certificates issued by ANF AC is available.

ANF AC offers different validation services:

- **OCSP Service**

  It is a distributed infrastructure of OCSP Responders that perform real-time queries directly on the repositories of the issuing entity. OCSP responses are electronically signed and comply with the IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP) standard.

  Optional fields per the RFC6960 specification:

Field	Definition
CertID.hashAlgorithm	Identifier of the hash algorithm
CertID. issuerNameHash	Hash of the issuer's DN (OCTET STRING)
CertID.serialNumber	Serial number of the certificate to be validated
CertID. issuerKeyHash	Public key hash of the issuer (OCTET STRING)
nonce	Optional
certReq	All responses contain the ANF AC's certification chain up to the root. Their presence and value is ignored.

The following is an example of an OpenSSL query:

OpenSSL ocsp -CAfile <certificado_ca>
-issuer <certificado_ia> -cert <certificate_to_verify>
-url <url_of_verification>
The field <url_of_verification > shall be indicated in the field "Authority Information Access" of the certificate.

Example for GET type queries with open SSL:

The request is generated:
openssl ocsp
-noverify
-no_nonce

-respout ocsp.resp
-reqout ocsp.req
-issuer AssuredID64.cer
-cert rev64.cer
-url"http://ocsp.anf.es/spain/AV"
-header "HOST" "ocsp.anf.es"
-text
It is converted into B64
openssl enc
-in ocsp.req
-out ocsp.req.b64 -a

Clarification: It has been found that OpenSSL can issue the following error responses:

1/ If the root CA has directly signed the end-entity certificate, OpenSSL returns:

Response Verify Failure
Verify error: self signed certificate in certificate chain

2/ If the response of the OCSP responder is a CRL type, OpenSSL returns:

Response Verify
Failure signer certificate not found

3/ ANF AC OCSP Responder servers support GET and POST queries.

The corporate website of ANF AC offers technical information for making OCSP queries, and certificates used by the OCSP responders.

www.anfacmalta.com

The validation process includes the certificate submitted for consultation and the entire Certification Hierarchy chain up to the first level (excluding CA Root). They are public and accessible in the URLs specified in the "CRLDistributionPoints" field on the ANF ACS OCSP server.

- **LDAP Service**

The Lightweight Directory Access Protocol (LDAP) provides a standardized method for storing certificates and CRLs for revoked certificates. The current version, LDAP v.3., is detailed in the RFC 4510 of the Internet Engineering Task Force (IETF) standard. They are public and accessible in the URLs specified in the "CRLDistributionPoints" field on the ANF AC LDAP server.

- **CRL – ARL Service**

Certificate Revocation Lists (CRLs) collect the serial numbers of those end-entity electronic certificates that have been revoked prior to the expiration of their validity period. For each certificate, date, time, and cause of revocation are specified.

Certification Authority Revocation Lists (ARLs) collect the serial numbers of those Certificates of Intermediate Certification Authorities that have been revoked prior to the expiration of their validity period. For each certificate, date, time, and cause of revocation are specified. They are public and accessible in the URLs specified in the "CRLDistributionPoints" field of the ANF AC web server.

Certificates of Root Certification Authorities that have been revoked prior to the expiration of their term are published on the ANF AC corporate website:

www.anfacmalta.com

During the provision of ANF CA's certification services, as of the date of publication of this Validation Policy, no CA Root certificates have been revoked.

- **Certificate Verification Device**

  It is an application developed by ANF AC, free and of free distribution. It is available in end user mode, and in API mode for developers. This device allows to:

  - Verify the validity of the certificate.
  - Verify the integrity and authenticity of the certificate.

- **Certificate Search Service**

  Available on ANF AC's website

  www.anfacmalta.com

  It is possible to do searches that allow the determination of the validity of the certificates issued, or even obtain a copy of it.

3 Validation Procedure

To validate an electronic certificate issued by ANF AC, it is necessary to follow the procedures described in the **RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" standard**.

Following the RFC 5280 standard we will be able to validate technically any electronic certificate, although for this we will need:

- Have the root certificate of the issuing CA. Published on the corporate website of ANF AC

  https://www.anfacmalta.com

- Have a copy of the electronic certificate of interest, the serial number, or the name of the subject.

3.1 Authenticity and validity of root certificate

The authenticity and validity of the root certificate is a critical issue in the validation of certificates. ANF AC guarantees the authenticity and validity of the root certificates obtained by any of the following methods:

- Downloaded from ANF AC's website through SSL protocol:

  https://www.anfacmalta.com

- Integrated into ANF Cryptographic Devices whose source is trusted. They are sources of confidence:
  - ANF AC's Website using SSL protocol:

    https://www.anfacmalta.com

  - The devices approved by ANF AC, published in:

    https://www.anfacmalta.com

All ANF AC's Cryptographic Devices maintain versioning control, and online update.

4 Validation Services

4.1 Certificate revocation list (CRL) (ARL)

The generation of Revoked Certificate Lists is defined in the document "Certification Practice Statement of ANF AC".

Each CA of the ANF AC's Certification Hierarchy issues its own CRL:

- Root CAs issue a list of revoked intermediate CAs (ARLs), at least within the term established in the ARL itself, or extraordinarily, when a revocation of a certificate of authority occurs.

- End-entity electronic certificates that have been revoked prior to their expiration date are included in the Revoked Certificates List (CRL), at least within the period established in the CRL itself, or whenever a certificate is revoked.

In the extraordinary case of revocation of a CA Root certificate, the revocation is published on the corporate website of ANF AC.

https://www.anfacmalta.com

It is recalled that ANF AC does not contemplate the temporary suspension of certificates.

4.2 Web certificate status query service

The query is made through a selective location of certificates using a form published on the Web www.anfacmalta.com.

Thus, the current valid status (valid, or revoked) of the certificate that matches the search criteria is obtained. In case their status is "revoked", the date of loss of validity is specified. It is recalled that ANF AC does not contemplate the temporary suspension of certificates.

4.3 OCSP query

The answers on the validation of a certificate are signed by ANF AC, which allows obtaining electronic evidence of the generated response. Per the RFC 6960 "Online Certificate Status Protocol - OCSP " standard.

4.3.1 Validation petition

The basic format for sending the requests follows the following scheme:

Content type ***: application/ocsp-request***

Method ***: POST***

Content-length ***: required***

It contains the OCSP response in ASN.1 (RFC2459), encoded in DER (X.690)

Optional fields per RFC6960 specification:

Field	Definition
CertID.hashAlgorithm	The hash algorithm used.
CertID. issuerNameHash	Issuer DN Hash (OCTET STRING)
CertID.serialNumber	Serial number of the certificate to be validated
CertID. issuerKeyHash	Issuer's Public Key Hash (OCTET STRING)
nonce	Optional
certReq	All responses contain ANF AC's certification chain, except for the root CA, whose presence and value is ignored (it must be verified by consulting the corporate website)

4.3.2 Response to validation petition

4.3.2.1 Definitive responses

All definitive response messages are electronically signed. The certificate used to sign the response, is a specially issued one for the OCSP responder that signs the validation, and has been issued by ANF AC.

The indicators defined for the final response are:

- Good.
- Revoked *[1]
- Unknown

*[1] Per RFC 6960 standard section. 2.2 the definition of revoked includes revoked certificates and non-issued certificates.

4.3.2.2 Exception cases

In case of errors, the OCSP response may return an error message. These messages are unsigned. Errors can be of the following types:

Cause	Definition
MalformedRequest (1)	Error caused because the received request is not in accordance to the OCSP syntax
InternalError (2)	Indicates that the OCSP responder has reached an internal inconsistency state
TryLater (3)	The OCSP responder is temporarily unable to respond
SigRequired (5)	The OCSP responder requires the client to sign the request.
Unauthorized (6)	It is returned in case the client is not authorized to query this server

(4) in accordance with the RFC 6960 standard it is not used

Optional fields per the RFC6960 specification:

Field	Definition
certReq	All responses contain the ANF AC's certification chain up to the root. Their presence and value is ignored.
Nonce *[1]	Optional. If the request contains it, it is present and with the same value.

* 1 Nonce: cryptographically a request and a response to prevent repetitive attacks.

5 Obligations and Responsibilities

5.1 Validation Authority

5.1.1 Obligations

ANF AC as a Validation Authority (VA) is required to:

- Maintain and publish this Certificate Validation Policy in accordance with its Certification Practice Statement and other associated policies.
- Respect the provisions of the Certification Practice Statement and this Certificate Validation Policy.
- Generate validation responses in accordance with this Policy and the standards in this area.
- Generate validation responses per the information sent by the client and free of data entry errors.
- Safeguard generated responses by protecting them from loss, destruction, or falsification.
- Immediately update ANF AC's CRLs every time a certificate is revoked or suspended
- Maintain a public access service to CRLs with high availability 24x7

ANF AC, in its activity of providing certification services, shall be liable for non-compliance with the provisions of this Certificate Validation Policy and, where applicable, pursuant to Law 59/2003 of December 19, Electronic signature, or its development regulations.

6 Operational Requirements

6.1 Obtaining reliable information

ANF AC only responds to requests made on certificates that have been issued by one of its certification hierarchies.

The Validation Authority has direct access to the own repository of the issuing CA, and is an authorized source for deciding on the validity of a certificate.

6.2 Certificate for the provision of the validation services

The generation of certificates necessary for the provision of services as a Validation Authority is regulated by the Certification Practice Statement and specific Policies.