Qualified Validation Policy

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 establishes the validation rules for Qualified and Advanced Electronic Signatures (QES/AES), and for Qualified and Advanced Electronic Seals (QEseal/ AESeal) through the trust service of qualified validation of ANF AC, pursuant to the requirements set by 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 pursuant to the respective European standards of ETSI (Technical Committee Electronic Signatures and Infrastructures).

This Qualified Validation Policy is subject to the Certification Practice Statement of ANF Certification Authority. The rules indicated in this document impact both the business and the legal relations and the security policy in the electronic transactions.

Pursuant to i.6 of COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 (pursuant to Art. 27, paragraph 5 and Art. 37, paragraph 5 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council):

> *"Advanced electronic signatures and advanced electronic seals are similar from the technical point of view. Therefore, the standards for formats of advanced electronic signatures should apply mutatis mutandis to formats for advanced electronic seals.* "

ANF AC provides the service qualified validation in accordance with the requirements set in the Regulation and guarantees that this service:

- Uses operational procedures and security management procedures which exclude any probability of manipulation of data and of the status of the validated certificates.
- Checks the validity of QES/AES and QEseal/ AESeal in accordance with the requirements of the Regulation.
- Checks the status of the certificates in accordance with recommendation RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Validates qualified certificates (QC) and QES/AES and QESeals/ AESeals;
- Performs the technical procedures for signature validation in accordance with the requirements of ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

Regarding the legal status of the e-signature, in accordance with the Regulation and with this Policy the general result of the validation does not change regardless if an advanced signature/seal accompanied by QC or a QES/ QEseal is involved.

1.1 Compliance

This document has been elaborated in accordance with the current legislation of Spain and the pan European recommendations, specifications and standards for provisioning qualified trust services pursuant to:

[1] Regulation (EU) No. 910/2014: "on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC"

[2] COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 (pursuant to Art. 27, paragraph 5 and Art. 37, paragraph 5 of Regulation (EU) No. 910/2014)

[3] ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

[4] RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP

[5] [ETSI-119-101] ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

[6] ETSI TS 119 172-1 V1.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents

1.2 Identification

Document name	Qualified Validation Policy
Version	2.4
Policy status	APPROVED
Document reference / OID	1.3.6.1.4.1.18339.55.1.1
Publication date	April 3rd, 2017
Expiration date	Not applicable
Related CPS	Certification Practice Statement (CPS) of ANF AC
Location	www.anfacmalta.com

1.3 Community and applicability

This Policy is valid by default for all Relying Parties using the Service.

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.

The "validation" service means the process of checking and confirming the validity of a QES / AES y QEseal / AESeal.

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 QES / AES y QEseal / AESeal.

1.4.2 Prohibited usage

It is expressly prohibited for third parties to use the validation services of ANF AC to provide validation services to other third parties. This prohibition extends specially to processes of 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, and 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. Nonetheless, regardless of the number of queries, the minimum penalty is set at 10,000 €, and after the 10.000 query, the cost of 1 euro per query shall be applicable.

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

2.1. Validation of signatures and electronics seal

The Qualified Validation Services of ANF AC allow to confirm the validity provided that:

- The certificate supporting the signature/seal at the moment of signing has been qualified (QC) in accordance with Annex I of the Regulation.
- QC has been issued by a Qualified Trust Services Provider and has been valid at the moment of signature.
- The signature validation data corresponds to the data provided by the Relying Party.
- The unique set of data representing the Signatory of the electronic signature in the certificate has been dully handed to the Relying Party.
- If at the moment of signing a pseudonym has been used, then this has been clearly indicated to the Relying Party.
- The electronic signature/seal has been created by a device for qualified electronic signature/seal creation.
- The electronic signature/seal has been created by using cryptographic components classified as security.
- If the signature / electronic seal upon creation has been subject to a particular electronic signature policy not authorized by this policy.
- The integrity of the signed data has not been compromised.
- The requirements for an advanced electronic signature (Art. 26 of the Regulation) have been complied with at the moment of signing.
- Provides to the Relying Party the correct result of the validation process (status-indication and report) and enables it to find any security related issues.
- The service gives to the Relying Parties the opportunity to receive the result of the validation
- process in an automated way which is trustworthy and effective and which leads to a qualified signature (or seal) for QTSP ANF AC.

The technical validity of the QES/QESeal is checked in accordance with the process described in the document ETSI EN 319 102 and is confirmed through the issuance of qualified electronic status attestations.

The next sections describe the Service – concept model, selection of validation process and attestation (status and report) of the validated qualified certificate for QES/QESeal.

In case there is no specific requirement indicated about the Service in this document, the requirements under i.5 of ETSI EN 319 102 shall apply.

In case this document indicates specific requirements and rules they shall prevail over the relevant ones of ETSI EN 319 102-1.

In case there is a discrepancy between the requirements and the rules in this document and those in ETSI EN 319 102, the ones in this document shall prevail.

2.2. Validation of Certificate

ANF AC offers the following status validation services for electronic certificates:

- **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.

https://www.anf.es/en/show/section/ocsp_service

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.anf.es

  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 a certificate issued by an ANF hierarchy.

- **Certificate Search Service**

  Available on ANF AC's website

  https://www.anf.es/en/show/section/certificate_search

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

2.3. Model Service Validation Signature and electronics seal

In accordance with the concept model of the validation process of advanced signature/seal in ETSI EN 319 102-1, the software with validation functions for QES/QESeal includes two components:

- SVA/Signature Validation Application;
- DA/Driving Application.

The service of QTSP ANF AC is positioned as the Signature Validation Application (SVA) component of the model. SVA is activated through the Driving Application (DA) component which has to receive the result of the validation process in the form of qualified attestation (status and report).

Driving Application (DA) of QTSP ANF AC can be:

- A web client with graphic interface (GUI).
- An API (software library) which allows integration into desktop applications.

These two forms of DA are realized in accordance with the principles described in this document.

2.4. Selection of validation process

The service supports validation processes of electronic signatures and stamps in different formats:

- Validation process for basic signature/seal format - Baseline;
- Validation Process for Signatures with Time Seal;
- Validation Process for Signatures with Time Seal and OCSP Certificate Certificate Status Check.

When validating a signature/seal, the Service performs consecutively the following actions:

1. Performs validation process of QES/QESeal with extended format.
2. Performs validation process of the baseline format of QES/QESeal.
3. If the selected validation process results in status-indication OK, SVA provides to the DA a status-indication TOTAL- CONFIRMED.

4. If the selected validation process results in status-indication KO, SVA provides to the DA a status-indication TOTAL-FAILED.
5. Otherwise SVA provides to the DA a status-indication INDETERMINATE.

2.5. Status-indication of the validation process and validation report

The service provides a detailed report on the validation of the signature/seal, enabling the DA to check in detail the decisions taken during the validation and to establish/examine in detail the causes for the provided status-indication.

The web client provided with the Service when it is used by a person provides the validation report in PDF-format.

The validation process result includes:

- A status-indication of the QES/QESeal validation process results.
- An indication of the policy under which the QES/QESeal is validated.
- Date and time of the validation status, including the data used for validation.
- The used validation process.
- Additional reporting data for validation in accordance with the below tables.

2.6. Status-indication for the QES/QESeal validation process

Status-indication	Semantics	Data to the validation report
TOTAL- CONFIRMED	The QES/QESeal validation process has a TOTAL-CONFIRMED result due to: • successful cryptographic checks of QES/QESeal (including checks of hashes of the different data objects, signed indirectly); • positively validated constraints regarding the certification of the signatory identity (i.e. the signing certificate is valid); and • successfully validated QES/QESeal	The validation process leads to the validated certifying chain including the certificate for QES/QESeal, used in the validation process together with a specific signed/sealed attribute (if any), which is considered as a proof of validation.

TOTAL-FAILED	The QES/QESeal validation process has a TOTAL-FAILED result because the cryptographic checks of the ES/QESeal are unsuccessful (including the checks of hashes of the different data objects, signed/sealed indirectly) or it has been proven that the generation of the signature/seal has happened after a revocation/ suspension of the QC.	The validation process leads to additional information explaining the status-indication TOTAL-FAILED for each of the validation constraints taken into account and for which negative results have been obtained.
INDETERMINATE	The available information is not sufficient for the validation process in order to establish the TOTAL-PASSED or TOTALFAILED status-indication of QES/QESeal.	The validation process leads to additional information in order to explain the indeterminate indication and to help the checkers determine the missing data in order to complete the validation process.

The validation report corresponding to the TOTAL-FAILEQ and INDETERMINATED status-indications in QES validation has a structure that is presented in the table below and consists of main and auxiliary codes which the validation process returns/provides.

Structure and semantics of the Validation report

Main code/statusindication	Auxiliary code	Semantics	Data to the validation report
TOTAL-FAILED	HASH_FAILURE	The QES/QESeal validation process leads to TOTAL-FAILED, because at least one hash of an object participating in the signatory process does not correspond to the respective hash in QES/QESeal.	The validation process provides an identifier which explicitly identifies an element in the signature/seal object causing the error in the form of QES/QESeal certificate.
	FORMAT_FAILURE	QES/QESeal is not compatible with the supported standards indicated in this document to a degree not enabling the cryptographic block check toprocess it.	The validation process provides any available information about the unsuccessful processing of the QES/QESeal

	SIG-CRYPTO- FAILURE	The QES/QESeal validation process leads to TOTAL-FAILED, because the digital value of the signature cannot be checked with the help of the public key from the QES/QESeal certificate	The validation process provides the QES/QESeal certificate used in the validation process
	POLICY- FAILURE	The validation process determines that the QES / QESeal is subject to a Signing Policy not authorized by this Validation Policy.	The validation process is negative because the Signing Policy is not authorized.
	REVOKED	The QES/QESeal validation process leads to TOTAL-FAILED, because: . the QES/QESeal certificate has been revoked; and · there is a proof (PoE) that the time-stamp of the signature/seal is after the time of the certificate revocation.	The validation process provides: ·The certifying chain used in the validation process. · The time and the reason, if any, for revocation/suspension of the QES/QESeal certificate. · CRL, if any, in which the revocation/suspension has been established. · electronic time-stamp seal to the signature/seal, if any, which show the earliest known time of existence of QES/QESeal
INDETERMINADO	SIG_CONSTR AINTS_FAILURE	The QES/QESeal validation process leads to INDETERMINATE, because one or more attributes of QES/QESeal do not correspond to the validation constraints.	The validation process provides: •The certifying chain used in the validation process. •Additional information about the cause.
	CHAIN_CONSTRAINTS_ FAILURE	The QES/QESeal validation process leads to INDETERMINATE, because the certifying chain used in	The validation process provides: •The certifying chain used in the validation process. •Additional information about the

		the validation process does not correspond to the constraints related to the validating certificate	cause.
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The QES/QESeal validation process leads to INDETERMINATE, because the check of the certifying chain shows an error due to an unestablished reason.	The validation process provides: Additional information about the cause.
	CRYPTO_CONSTRAINTS_FAILURE	The QES/QESeal validation process leads to INDETERMINATE, because at least one of the used algorithms (for QES/QESeal or corresponding certificates), participating in the QES/QESeal validation or the size of the keys using these algorithms is under the required level of cryptographic security and also: • QES/QESeal and/or corresponding certificates are generated after a moment until which these algorithms/keys are considered as secure (if such time is known); and • QES/QESeal is not protected by a sufficiently reliable time-stamp seal put before the time until which the algorithms/keys are	The validation process provides: An identification/designation of QES/QESeal or of a certificate generated with an algorithm or a key size under the required level of cryptographic security.

		considered as secure (if such time is known).	
	EXPIRED	The QES/QESeal validation process leads to INDETERMINATE, because the time-stamp of the signature is after the expiration date (notAfter) of the certificate	The validation process provides: The validated certifying chain
	NO_SIGNING_CERTIFICATE_FOUND	The QES/QESeal validation process leads to INDETERMINATE, because the QES/QESeal certificate cannot be identified.	
	NO_CERTIFICATE_CHAIN_FOUND	A certifying chain for identifying the QES/QESeal certificate has not been found.	
	REVOKED_NO_POE	The corresponding certificate has been revoked/suspended during the validation. The SVA however cannot establish if the time-stamp of the signature is before or after the time of revocation/suspension	
	OUT_OF_BOUNDS_NO_POE	The certificate has expired or is not valid yet at the date/hour of validation and SVA cannot determine if the time-stamp of signature is within the interval of validity of the certificate.	
	CRYPTO_CONSTRAINT_FAILURE_NO_POE	At least one of the algorithms used in the QES/QESeal or in the corresponding certificates participating in their validation or the size of the key used with such algorithm is under the required level of cryptographic security and also there is no proof that the signatures/seals or these certificates have been generated before the	The validation process provides: Identification of QES/QESeal or of the corresponding certificate generated with unacceptable key length or with an algorithm not corresponding to the cryptographic requirements for the security level.

		time until which this algorithm/key has been considered as secure.	
	NO_POE	An evidence (PoE) is missing proving that the signature/seal has been generated before the acknowledgement of a compromising event (i.e. crushed algorithm).	
	TRY_LATER	Not all constraints can be fulfilled with the available information. Despite of that the process is possible if the validation uses additional information about the revocation/suspension which will be available at a later stage.	
	SIGNED_DATA_NOT_FOUND	The data for signature/seal canno be received	The validation process provides: The identifier (for example URI) of the data for signature/seal which has caused the error.
	GENERIC	due to other reasons.	The validation process provides: Additional information which shows why the validation status is INDETERMINATE

3 Policy

QTSP ANF AC, operates the Service within this Policy

QTSP ANF AC, is responsible for keeping updated and managing this document in consistency with the Certification Practice Statement.

3.1 Validation constraints

The validation process/Service is managed through a set of validation constraints. These constraints of Service operation are explicitly defined through a system of specific management data as well as through the application.

All validation constraints which are not part of the Service result directly from the very content of the QES/QESeal (included in the signed attributes) or indirectly from it, that is through referring to an external

document intended for machine (automated) processing. Additional constraints can be provided by the DA to the SVA through parameters selected by the application or by the user.

Any additional constraint is provided after a mutual agreement between QTSP ANF AC and the Relying Party.

The following specific constraints are supported:

- Constraints of certificate validation (the chain of certificates);
- Cryptographic constraints;
- Constraints related to elements of the signature.
- Restrictions related to the signature policy.

3.1.1 General constraints

The Service of QTSP ANF AC supports the following general validation constraints:

Constraints	Constraint value in validation of QES/QESeal (SVA or DA)
Electronic Certificates	ANF AC
TSA service used for time-stamp certification of (qualified electronic time-stamp seal)	ANF AC TSA
OCSP Responder service, for checking the certificate's valid status.	ANF AC VA
Maximum file size	100 Mb.

Supported Signing Policy	Signing Policy of ANF AC: OID 1.3.6.1.4.1.18332.27.1.1

3.1.2. Constraints of certificate validation

The Service of QTSP ANF AC supports the following constraints for validation of X.509 certificates in the validation process of the certifying chain pursuant to ETSI TS 119 172-1, clause A.4.2.1., Table A.2. Row (m):

Constraints	**Constraint value in validation of QES/QESeal (SVA or DA)**
(m) 1. X509 CertificateValidationConstraints: This set of constraints refers to the requirements in the validation process of the certifying chain pursuant to IETF RFC 5280. The constraints can be different for the different types of certificates (for example signature certificates, for Certifying Authorities, for OCSP-responses, for CRLlists, electronic time-stamp seals/TST). The semantics of a possible set of required values which is used to present these requirements is determined in the following way:	
(m) 1.1 SetOfTrustAnchors: This constraint indicates a set of acceptable trusted Certifying Authorities (TAs) with a view to limit the validation process.	EU (TSL) ECUADOR (TSL) PERU (TSL) REPUBLICA DOMINICANA (TSL) MEXICO (TSL) ARGENTINA (TSL)
has "n" length from the beginning/the Trusting Authority (VA) towards the QES/QESeal certificates used when validating the signature. The constraint can include the path or to indicate the necessity to include the path provided through the QES/QESeal, if any.	
(m) 1.3. *user-initial-policy-set:* Pursuant to IETF RFC 5280 clause 6.1.1 (c) (m) 1.4. *initial-policy-mapping-inhibit*: Pursuant to IETF RFC 5280 clause 6.1.1 (e) (m) 1.5. *initial-explicit-policy*: Pursuant to IETF RFC 5280 clause 6.1.1 (f) (m) 1.6. *initial-any-policy-inhibit*: Pursuant to IETF RFC 5280 clause 6.1.1 (g) (m) 1.7. *initial-permitted-subtrees*: Pursuant to IETF RFC 5280 clause 6.1.1 (h) (m) 1.8. *initial-excluded-subtrees*: Pursuant to IETF RFC 5280 clause 6.1.1 (i) (m) 1.9. *path-length-constraints*: This constraint refers to the number of certificates of the Certifying Authority (CA) within the certifying chain. (m) 1.10. *policy-constraints*: This constraint refers to the policy(ies) in the QES/QESeal certificate.	100 Mb.

(m) 2. **RevocationConstraints:** This set of constraints refers to the QES/QESeal certificates status check during the validation process. These constraints can be different for the different types of QES/QESeal certificates.	
(m) 2. RevocationConstraints: This set of constraints refers to the QES/QESeal (m) 2.1. RevocationCheckingConstraints: This constraint refers to the requirements for checking the QES/QESeal certificate for revocation/suspension. Such constraints specify whether the check for revocation/suspension is necessary or not and whether OCSPresponses or issued CRL should be used. The semantics for a possible set of required values used to present these requirements is defined in the following way: - ClrCheck: The checks are performed against the current CRL; - OcspCheck: The revocation/suspension status is checked through OCSP IETF RFC 6960; - BothCheck: Both checks are performed through OCSP and CRL; - EitherCheck: Checks are performed either through OCSP or through CRL; - NoCheck: No checks	eitherCheck
(m) 2.2. RevocationFreshnessConstraints: This constraint indicates the time requirements of the revocation/suspension information. The constraints can indicate the maximum acceptable difference between the date of issuance of information on the revocation/suspension status of the QES/QESeal certificate and the validation time, or to require SVA to accept only information for revocation/suspension issued in a specified time after the creation/generation of QES/QESeal.	NONE
(m) 2.3. *RevocationInfoOnExpiredCerts*: This constraint imposes that the QES certificate used in its validating be issued by a Certifying Authority (CA), which supports the updates of revoked/suspended certificates even after they have expired for a period longer than a given low limit.	NONE
(m) 3. LoAOnTSPPractices: This constraint indicates the level of agreement (LoA) regarding the practices of TSP (s), which issue the QES/QESeal certificate in order to be confirmed during the validation process on the path of the certificates.	NONE
EUQualifiedCertificateRequired	YES
EUQualifiedCertificateSigRequired	YES
EUQualifiedCertificateSealRequired 1	YES

3.1.3. Cryptographic constraints

The Service of QTSP ANF AC supports the following cryptographic constraints which indicate requirements on the algorithms and parameters used in the creation of QES/QESeal or used in validating a certain object as indicated in ETSI TS 119 172-1, clause A.4.2.1, Table A2, row (p).

Constraints	Constraint value in validation of QES/QESeal
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements for the algorithms and parameters used in the creation of QES/QESeal or used in validating signatures/seals of objects included in the validation process (for example QES/QESeal, certificates, CRLs, OCSP-responses, time-stamp seals/TSTs).	In accordance with the document ETSI TS 119 312

3.1.4. Constraints of the signature elements

The Service of QTSP ANF AC supports the following constraints regarding the elements of QES/QESeal which indicate requirements to DTBS (Data To Be Signed), in accordance with ETSI TS 119 172-1, clause A.4.2.1., table A.2, row (b).

Constraints	Constraint value in validation of QES/QESeal
b) 1. ConstraintOnDTBS: This constraint indicates the requirements about the type of data to be signed/sealed by the signatory/sealing person.	NONE
(b) 2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints shows the necessary information elements related to the content, in the form of signed or not signed qualified requisites present in the QES/QESeal. The set includes: (b) 2.1 MandatedSignedQProperties-DataObjectFormat requires specific format of the content to be signed/sealed by the signatory/sealing person. (b) 2.2 MandatedSignedQProperties-content-hints requires specific information which describes the most inner signed/sealed content of multilayered messages where one content is capsulated into another in order to be signed the whole content by the signatory. (b) 2.3 MandatedSignedQProperties-content-reference requires the inclusion of information on the way in which to connect a request and a response of the message within an exchange between both parties or the way in which the connection should be made etc.	NONE

(b) 2.4 MandatedSignedQProperties-content-identifier requires presence and eventually a specific value of an identifier to be used later in the signed attribute qualifying "content-reference".	
(b)3. DOTBSAsAWholeOrInParts: This constraint shows if the data or just a specific part/s of it should be signed. The semantics of a possible set of required values used to indicate these requirements is defined, as follows: • Whole: all data must be signed; • Parts: only certain part/s of the data must be signed. In this case, additional information is used to indicate which parts should be signed/sealed.	NONE

3.2. Supported formats and security levels for QES/QESeal

The Service of QTSP ANF AC supports the following formats and levels of QES/QESeal pursuant to COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 on defining specifications referring to the format of advanced electronic signatures and seals:

Formats with baseline profile of QES/QESeal:

- ETSI TS 103 171 V2.1.1 Electronic Signatures and Infrastructures (ESI) - XAdES Baseline Profile
- ETSI TS 103 173 V2.2.1 Electronic Signatures and Infrastructures (ESI) - CAdES Baseline Profile
- ETSI TS 103 172 V2.2.2 Electronic Signatures and Infrastructures (ESI) – PAdES Baseline Profile

In addition, the Service validates the above cited formats, but with an advanced profile in accordance with the security level of QES/QESeal:

- ETSI TS 103 171 V2.1.1 Electronic Signatures and Infrastructures (ESI) – XAdES-T/TL Level
- ETSI TS 103 173 V2.2.1 Electronic Signatures and Infrastructures (ESI) – CAdES T/TL Level
- ETSI TS 103 172 V2.2.2 Electronic Signatures and Infrastructures (ESI) PAdES T/TL Level

3.3. Supported QES / QESeal Restrictions

Position of the signature/seal and the signed data object	Value
Covering QES/QESeal – the signature/seal covers the data object	yes
Covered (type "letter") QES/QESeal – the signed data object covers the signature/seal	yes
Separate QES/QESeal – the signature/seal and the data object are separated (independent)	yes

Simultaneously repeatedly compared positions	yes
One document has more than one QES/QESeal	yes

4 Compliance with Regulation (EU) 910/2014

4.1 Validation of qualified electronic signatures in accordance with eIDAS: Art. 26, 28 and 32

Requirements in Art. 26, 28 and 32 of Regulation (EU) No. 910/2014	**Execution of the Service**
Art. 32 *Requirements to the validation of qualified electronic signatures* *1. In the validation process of a qualified electronic signature the validity of the qualified electronic signature is confirmed, provide that:*	
A) the signature supporting certificate at the moment of signing was a qualified certificate for an electronic signature, corresponding to Annex I.	The certificates validation process complies with the requirements described in EU 2015/1505 and ETSI 319 412-5 Annex A.1 for QTSP issuing qualified certificates for electronic signature.
B) the qualified certificate has been issued by a qualified trust services provider and has been valid at the moment of signing.	The certificates validation process complies with the requirements described in EU 2015/1505 and ETSI 319 412-5 Annex A.1 for QTSP issuing qualified certificates for electronic signature.
C) the signature validation data Corresponds to the data provided by the relying party.	It is guaranteed through the supported formats for QES/QESeal.
D) the unique set of data, representing the signatory of the electronic signature in the certificate is dully handed to the relying party.	The signing certificate for QES/QESeal is included in the response by the validations for each supported protocol pursuant to this document.
E) if at the moment of signing a pseudonym has been used, this has been clearly indicated to the relying party.	As the pseudonym indication in the Subject field is used only at the express request of the client and after a preliminary agreement between them and the QTSP, the requirements of ETSI EN 319 412-2 shall apply pursuant to this document.
F) the electronic signature has been created by a device for qualified electronic signature creation.	The certificates validation process complies with the requirements described in EU 2015/1505 for QTSP issuing qualified certificates. A check for the required type of SSCD (QSCD) is performed.
G) the integrity of the signed data is not Compromised.	It is guaranteed through the supported validation model indicated in this document.
H) the requirements cited in Art. 26 have been complied with at the moment of signing.	It is guaranteed through the supported validation model indicated in this document.
2. The system used for qualified electronic signature validation provides to the relying party the correct result from the validation process and enables it to find eventual security related problems.	The validation process for QES/QESeal and the statusindication after the check are described in this document.
Art. 28 *Qualified certificates for electronic signatures*	
1. The qualified certificates for electronic	Corresponds to the requirements of ETSI 119 412-5, Annex

signatures correspond to the requirements provisioned in Annex I.	A.1.
2. The qualified certificates for electronic signatures are not subject to any mandatory requirement exceeding the requirements provisioned in Annex I.	The certificates validation process complies with the requirements described in EU 2015/1505 for trusted lists. No additional checks are needed except those indicated in Annex I of the Regulation.
3. The qualified certificates for electronic signatures can include additional non-mandatory specific data. This data does not impact the operational compatibility and the acknowledgement of the qualified electronic signatures.	No additional checks are needed except those indicated in Annex I of the Regulation.
4. If a qualified certificate for electronic signature is revoked after its initial activation it loses its validity from the moment of revocation and its status cannot be restored in any circumstances.	In accordance with the Policy and Practice for qualified trust services for QES/QESeal.
5. The Member States can determine national rules regarding the temporary suspension of the validity of the qualified certificate for electronic signature by complying with the following conditions:	Pursuant to ETSI TS 110 102-1 if in the certificate validation process a wrong validation result/response is received due to suspended QES/QESeal certificate, the Service will terminate the validation process. The status-indication is INDETERMINATE and the additional code TRY_LATER with the time of the suspension and, if any, the nextUpdate field of CRL or OCSP-response is used to determine the following validation.
A) if the qualified certificate for electronic signature is temporary suspended, it loses its validity for the term of the suspension	
B) The term of the suspension is clearly indicated in the database of the certificates and the status of the suspended certificate is visible for the term of the suspension within the service providing information about the status of the certificate	
Art. 26 *Requirements to the advanced electronic signatures*	
The advanced electronic signature corresponds to the following requirements:	It is guaranteed through the supported formats for QES/QESeal.
A) it is related in a unique way to the signatory of the signature	It is guaranteed through the supported formats for QES/QESeal.
B) can identify the signatory of the signature	It is guaranteed through the supported formats for QES/QESeal.
C) has been created through data for electronic signature creation which the signatory of the electronic signature can use with high reliability and solely under their control; and	It is guaranteed through the supported formats for QES/QESeal.
D) it is related to the data signed with it in a way it enables finding any consecutive modification in them	It is guaranteed through the supported formats for QES/QESeal.