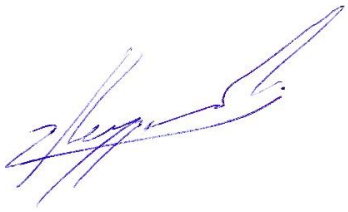
QUALIFIED VALIDATION

POLICY

Version: 1.0

	Position	Forename, surname	Date	Signature
Approved by	Executive Director	Konstantin Bezuhanov	*13.04.2017*	
Coordinated by	Representative of the management for ISMS	Stefan Hadzhistoychev	*13.04.2017*	
Elaborated by	Consultant for ISMS	Mariya Vladimirova	*13.04.2017*	

Registration date of the document:	*13.04.2017*
The original is kept at:	*with Representative of the management for ISMS*

Type of copy and consecutive No.

Original	X	**Controlled copy**		**Informational**	

Distribution of the document:	**Subscriber:**
Internally:	
Externally:	

TABLE OF CONTENTS

1. Introduction and scope

This document establishes the validation rules for Qualified and Advanced Electronic Signatures (QES/AES), for Qualified and Advanced Electronic Seals (QEseal/ AESeal) and for issuance of qualified electronic statutory attestations of qualified certificates (QC) through the trust service of qualified validation “Evrotrust RSA QS Validation” (referred herein as “the Service”). The document has been elaborated by “EVROTRUST TECHNOLOGIES” AD, Qualified Trust Service Provider (referred herein as “QTSP EVROTRUST”) 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).

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. “

EVROTRUST provides the Service 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, or.
- 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 RFC2560 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 TS 119 102.

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.

Each of the policies in accordance to which the qualified certificates issued by EVROTRUST are validated received an object identifier (OID). The values of the object identifiers are:

Validating authority	Object identifier (OID)
Evrotrust RSA Validation Policy of the validating authority servicing the qualified certificates of the basic certifying authority "**Evrotrust RSA Root CA**"	1.3.6.1.4.1.47272.1.1
Evrotrust RSA QS Validation Policy of the validating authority servicing the qualified certificates of the operational certifying authority "**Evrotrust RSA Operational CA**"	1.3.6.1.4.1.47272.2.1

2. Compliance

This document has been elaborated in accordance with the current legislation of the Republic of Bulgaria and the pan European recommendations, specifications and standards for provisioning qualified trust services pursuant to Regulation (EU) No. 910/2014.

[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] EN 319 132-1 v1.1.1 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

[4] EN 319 132-2 v1.1.1 XAdES digital signatures; Part 2: Extended XAdES signatures

[5] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CadES Base Profile

[6] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PadES Base Profile

[7] ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

[8] [ETSI-119-102] ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures

for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

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

[10] 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

[11] ETSI TS 119 312 V1.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[12] ETSI TS 119 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[13] ETSI TS 119 412-5 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[14] ETSI TS 101 733 V.1.7.4 (2008-07) Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

[15] ETSI TS 101 903 V.1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES).

[16] ETSI TS 102 778 (2009-07) Electronic Signature and Infrastructure (ESI) – PDF Advanced Electronic Signature (PAdES).

[17] R.Housley. Cryptographic Message Syntax (CMS). RFC5652. 2009.

[18] D.Eastlake, J.Reagle, D.Solo, (Extensible Markup Language) XML-Signature Syntax and Processing, RFC3275. 2002.

[19] ETSI TS 119 612 V2.1.1 (2015-07) Electronic Signatures and Infrastructures
(ESI); Trusted Lists

[20] S.Drees et al., Digital Signature Service Core Protocols and Elements OASIS. 2007.

[21] OASIS Digital Signature Service Signature Gateway Profile. 2007.

[22] OASIS Digital Signature Service eXtended

[23] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version 1.6. 004

[24] M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC6960.

3. Abbreviations

CA - Certificate Authority
CAdES - CMS Advanced Electronic Signatures
CRL - Certificate Revocation List
DSS - Digital Signature Standard
eIDAS - Regulation (EU) No 910/2014 of the European Parliament
ETSI - European Telecommunications Standards Institute
GUI - Graphical User Interface
OASIS - Organization for the Advancement of Structured Information Standards
OCSP - Online Certificate Status Protocol
PDF - Portable Document Format
PAdES - PDF Advanced Electronic Signatures
PoE - Proof of Evidence
SOAP - Simple Object Access Protocol
TLS - Transport Layer Security
TSA – Time Stamping Authority
TSL - Trust Status List
VA - Validation Authority
VS - Validation Service
XAdES - XML Advanced Electronic Signatures
XML - eXtended Markup Language
XML - DSIG XML Digital Signature

4. Service

4.1. General principles

The “validation” service means the process of checking and confirming the validity of a QES/QEseal. The Service confirms the validity of a QES/QEseal, 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 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 EVROTRUST.

The technical validity of the QES/QESeal is checked in accordance with the process described in the document ETSI TS 119 102 and is confirmed through the issuance of qualified electronic status attestations.

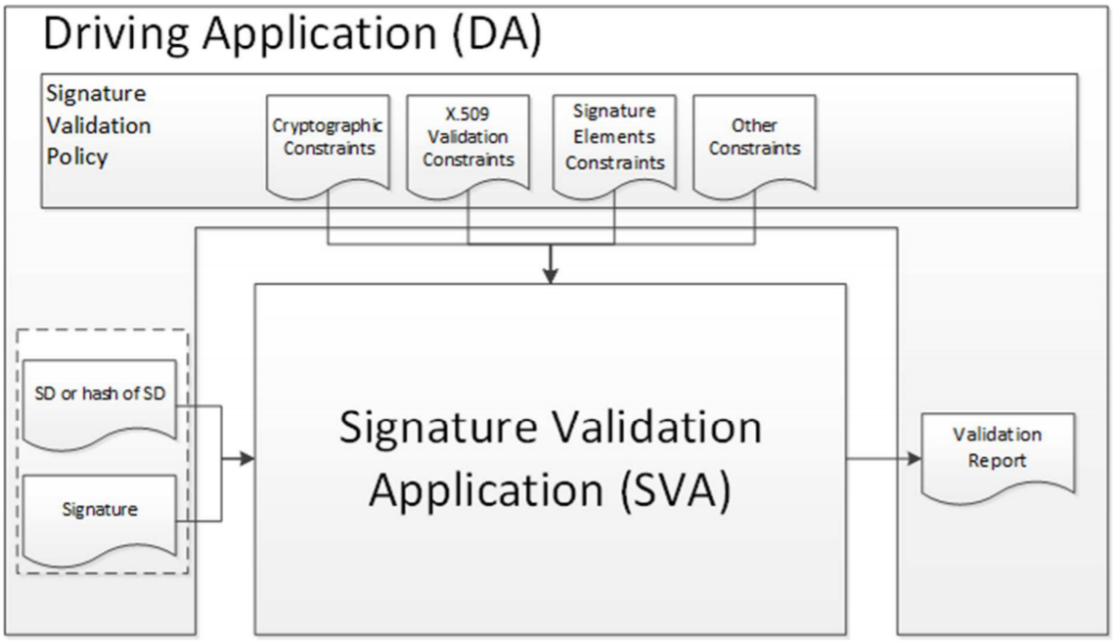
The next sections describe the Service – concept model, selection of validation process and attestation (status and report) of the validated qualified certificate for QES/QESeal.

In case there is no specific requirement indicated about the Service in this document, the requirements under i.5 of ETSI TS 119 102 shall apply.

In case this document indicates specific requirements and rules they shall prevail over the relevant ones of ETSI TS 119 102-1.

In case there is a discrepancy between the requirements and the rules in this document and those in ETSI TS 119 102, the ones in this document shall prevail.

4.2. Service model



In accordance with the concept model of the validation process of advanced signature/seal in ETSI TS 119 102-1 (fig. 1), the software with validation functions for QES/QESeal includes two components:

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

The service of QTSP EVROTRUST 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 EVROTRUST can be:

- A web client with graphic interface (GUI).
- An application-client (or a software library) using OASIS-DSS specifications.

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

4.3. Selection of validation process

Depending on the classes (formats) of QES, the Service supports validation processes (that is validates) of Baseline formats of signature/seal and of Advanced formats (with added electronic time-stamp seal (T) or with long-term validation data (TL)) as follows:

- Validation process for basic signature/seal format - Baseline;
- Validation Process for Signatures with Time – Baseline + T;
- Validation Process for Signatures with Long-Term validation data – Baseline + LT.

DA cannot define the validation process. The format of QES and the security level (Level T/TL) of the format determine the validation process.

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

4.4. 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.

➢ An attribute showing the reason to create the QES/QESeal, if such is available to the provided data for signature/seal.

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

Status-indication	Semantics	Data to the validation report
TOTAL-PASSED	The QES/QESeal validation process has a TOTAL-PASSED 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 against the validating constraints and thus it is accepted against these constraints.	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 QES/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 TOTAL-FAILED 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/status-indication	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 to process 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.
	REVOKED	The QES/QESeal validation process leads to TOTAL-FAILED, because: . the QES/QESeal certificate	The validation process provides: ·The certifying chain used in the validation process. · The time and the reason, if any, for

		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.	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.
INDETERMINATE	SIG_CONSTRAINTS_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 does not correspond to the constraints related to the validating certificate	The validation process provides: • The certifying chain used in the validation process. • Additional information about the 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	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

		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 considered as secure (if such time is known).	cryptographic security.
	NOT_YET_VALID	The QES/QESeal validation process leads to INDETERMINATE, because the time-stamp of the signature/seal is before the expiration date (notBefore) of the certificate.	
	EXPIRED	The QES/QESeal validation process leads to INDETERMINATE, because the time-stamp of the signature is after the expiration date (notAfter) of	The validation process provides: The validated certifying chain

		the certificate.	
	NO_SIGNING_CERTIFICATE_FOUND	The QES/QESeal validation process leads to INDETERMINATE, because the QES/QESeal certificate cannot be identified.	
	NO_CERTIFICATE_CHAIN_FOUND	The QES/QESeal validation process leads to INDETERMINATE, because a certifying chain for identifying the QES/QESeal certificate has not been found.	
	REVOKED_NO_POE	The QES/QESeal validation process leads to INDETERMINATE, because 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	The validation process provides: • The certifying chain used in the validation process. • The time and the reason for revocation/suspension of the QES/QESeal certificate.
	OUT_OF_BOUNDS_NO_POE	The QES/QESeal validation process leads to INDETERMINATE, because 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	The QES/QESeal validation process leads to INDETERMINATE, because 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 time until which this algorithm/key has been considered as secure.	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
	NO_POE	The QES/QESeal validation process leads to INDETERMINATE, because an evidence (PoE) is missing proving that the signature/seal has been generated before the acknowledgement of a compromising event (i.e. crushed algorithm).	The validation process identifies only signatures/seals for which there is no evidence (POEs). The validation process should provide additional information for the issue.
	TRY_LATER	The QES/QESeal validation process leads to INDETERMINATE, because 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 QES/QESeal validation process leads to INDETERMINATE, because the data for signature/seal cannot be received	The validation process provides: The identifier (for example URI) of the data for signature/seal which has caused the error.
	GENERIC	The QES/QESeal validation process leads to INDETERMINATE, due to other reasons.	The validation process provides: Additional information which shows why the validation status is INDETERMINATE.

5. Policy

QTSP EVROTRUST operates the Service within this Policy. This Policy is valid by default for all Relying Parties using the Service. The introduction of specific constraints for the Relying Party is forbidden.

5.1. 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 EVROTRUST 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.

5.1.1. General constraints

The Service of QTSP EVROTRUST supports the following general validation constraints:

Constraints	Constraint value in validation of QES/QESeal (SVA or DA)
TSA service used for time-stamp certification of (qualified electronic time-stamp seal)	Evrotrust TSA
Maximum file size	10MB

5.1.2. Constraints of certificate validation

The Service of QTSP EVROTRUST 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 CRL-lists, 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)
(m) 1.2 *CertificationPath*: This constraint shows the certification path	

used by the SVA for QES/QESeal validation. The certification path has "n" length from the beginning/the Trusting Authority (TA) 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.	None
(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. The semantics for a possible/acceptable set of required values used to present these requirements is defined in the following way:	
(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 OCSP-responses 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:	eitherCheck

- 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	
(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

5.1.3. Cryptographic constraints

The Service of QTSP EVROTRUST 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

5.1.4. Constraints of the signature elements

The Service of QTSP EVROTRUST 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 multi-layered 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. (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".	None

(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

5.2. Supported formats and security levels for QES/QESeal

The Service of QTSP EVROTRUST supports/validates 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
- ETSI TS 103 174 V2.2.1 Electronic Signatures and Infrastructures (ESI) – AsiC 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;
- ETSI TS 103 174 V2.2.1 Electronic Signatures and Infrastructures (ESI) AsiC T/TL Level.

5.2.1. Constraints of the supported QES/QESeal

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

6. Scope of the Certifying Authorities

Pursuant to the Regulation on eIDAS an immediate and priority task is to create a common European system of trusted lists (TSL) covering the qualified certifying authorities in the Member States.

7. Service interfaces for users and Relying parties

The Service of QTSP EVROTRUST is offered as web services which are accessible and used through:

- OASIS DSS Interface.
- GUI interface.

In both interfaces the Service is authenticated (though a certificate for a server/ a certificate for authenticity of a website) to the application or the client/browser.

The Service does not require authentication of the user (application or client/browser).

8. OASIS DSS Interface

The Service of QTSP EVROTRUST is accessible and used through OASIS DSS interface. The interface defines XML-commands Request/Response for both protocols:

- Protocol for signing/sealing documents with QES/QESeal.
- Protocol for validation of signed/sealed documents (validation of QES/QESeal).

Both protocols of the OASIS DSS interface use transport protocol SOAP for exchange of XML-commands in signing/sealing and in validation of the signature/seal.

The specifications of the DSS-interface are regulated and supported by the OASIS-consortium.

8.1. Graphic user interface (GUI)

The Service of QTSP EVROTRUST is accessible and used through GUI (graphic user interface). In this interface, the XML-commands of the DSS-interface use HTTP POST for exchange/transport.

Using GUI, a certain client accesses the Service and can indicate and upload a signed document with QES/QESeal, to select the parameters of the request and those of the response and afterwards to send the formed XML-request to the Service through the HTTP POST protocol.

9. Compliance with Regulation (EU) N 910/2014

9.1. 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 119 412-5 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 119 412-5 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 119 412-2 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.	See below (about Art. 26)
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 status-indication after the check are described in this document.
Art. 28 *Qualified certificates for electronic signatures*	
1. The qualified certificates for electronic signatures correspond to the requirements provisioned in Annex I.	Corresponds to the requirements of ETSI 119 412-5, Annex 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.

Registration of modifications																					
Page																					
Valid modification																					