Validation Policy of CERTUM's QESValidationQ Qualified Validation Service for qualified electronic signatures and qualified electronic seals

Version 1.0
Effective date: 1st of July, 2016
Status: valid

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia„Certum - Powszechne Centrum Certyfikacji"
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl

Trademark and Copyright notices

Table of Contents

1 Introduction, scope and assumptions

The Validation Policy of CERTUM's QESValidationQ Qualified Validation Service for qualified electronic signatures and qualified electronic seals describes a set of rules applied to issue qualified validation tokens (formerly known as data validation and certification server tokens), according to the requirements specified in the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, together with attached Implementing and Delegated Acts, and in European Standards produced by ETSI Technical Committee Electronic Signatures and Infrastructures.

The set of rules described in this document reflects business, legal and security policy requirements.

Based on Recital 6 of Commision Implementing Decision [EU 2015/1506]

"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" all rules described in this document for electronic signatures also aplly for electronic seals.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

[1] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

[2] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

[3] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

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

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

[eIDAS] the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[EU 2015/1505] COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[EU 2015/1506] COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015
laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[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

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

[ETSI 119 172-1] 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

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

[ETSI 119 412-2] 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

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

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

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

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

[RFC2315] B.Kaliski, PKCS#7: Cryptographic Message Syntax Standard - Version 1.5. RFC2315. 1998. http://datatracker.ietf.org/doc/rfc2315

[RFC5652] R.Housley. Cryptographic Message Syntax (CMS). RFC5652. 2009. http://datatracker.ietf.org/doc/rfc5652

[RFC3275] D.Eastlake, J.Reagle, D.Solo, (Extensible Markup Language) XML-Signature Syntax and Processing, RFC3275. 2002. http://datatracker.ietf.org/doc/rfc3275

[ETSI-11-612] ETSI TS 119 612 V2.1.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Trusted Lists

[OASIS-DSS-Core] S.Drees et al., Digital Signature Service Core Protocols and Elements OASIS. 2007. http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html

[OASIS-DSS-Gateway] OASIS Digital Signature Service Signature Gateway Profile. 2007. http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-SignatureGateway-spec-v1.0-os.html

[OASIS-DSS-X] OASIS Digital Signature Service eXtended Technical Committee draft documents. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x

[PDF] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version 1.6. 2004. http://partners.adobe.com/public/developer/en/pdf/PDFReference16.pdf

[PEPPOL-DSS] dsffsd

[RFC 3029] Internet X.509 Public Key Infrastructure; Data Validation and Certification Server Protocols https://tools.ietf.org/html/rfc3029

[RFC2560] M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC2560. 1999. http://datatracker.ietf.org/doc/rfc5055

[RFC3377] J.Hodges, R.Morgan. Lightweight Directory Access Protocol (v3): Technical Specification. RFC3377. 2002. http://datatracker.ietf.org/doc/rfc3377

[RFC4346] T.Dierks, E.Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC4346. 2006. http://datatracker.ietf.org/doc/rfc4346

[SOAP] Simple Object Access Protocol v1.2 (second edition), parts 0-3. W3C Recommendations. 2007. http://www.w3.org/TR/2007/REC-soap12-part0-20070427 http://www.w3.org/TR/2007/REC-soap12-part1-20070427 http://www.w3.org/TR/2007/REC-soap12-part2-20070427

[TSL-HR] EU Trust Status List of national TSL issuer, human readable (PDF) format. 2010. https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

[TSL-MP] EU Trust Status List of national TSL issuer, machine processable (XML) format. 2010. https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

[XKMS] XML Key Management Specification (XKMS 2.0) Version 2.0, W3C Recommendation. 2005. http://www.w3.org/TR/2005/REC-xkms2-20050628 http://www.w3.org/TR/2005/REC-xkms2-bindings-20050628

[Validation model] How to avoid the Breakdown of Public Key Infrastructures Forward Secure Signatures for Certificate Authorities, J. Braun, A. Hulsing, A. Wiesmaier, M. Vigil, J. Buchmann

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

API	Application Program Interface
CA	Certificate Authority
CAdES	CMS Advanced Electronic Signatures [ETSI-101-733]
CMS	Cryptographic Message Syntax [RFC5652]
CRL	Certificate Revocation List
DSS	Digital Signature Standard (OASIS) [OASIS-DSS-Core]
eID	Electronic Identity
eIDAS	the Regulation (EU) No 910/2014 of the European Parliament
EU	European Union
EUPL	European Union Public License
ETSI	European Telecommunications Standards Institute
ESI	ETSI Technical Committee Electronic Signatures and Infrastructures
GUI	Graphical User Interface
LDAP	Lightweight Directory Access Protocol [RFC3377]
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol [RFC2560]
PDF	Portable Document Format [PDF]
PAdES	PDF Advanced Electronic Signatures [ETSI-102-778]
PEPPOL	Pan European Public Procurement On-Line [PEPPOL]
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PoE	Proof of Evidence
RFC	Request For Comments (Internet publication)
SDO	Signed Data Object
SOAP	Simple Object Access Protocol [SOAP]
TC ESI	Technical Committee Electronic Signatures and Infrastructures
TLS	Transport Layer Security [RFC4346]
TSA	Time Stamping Authority [RFC3628]
TSL	Trust Status List [ETSI-102-231]
VA	Validation Authority
VS	Validation Service
XAdES	XML Advanced Electronic Signatures [ETSI-101-933]
XKMS	XML Key Management Specification [XKMS]
XML	eXtended Markup Language
XML DSIG	XML Digital Signature [RFC3275]

4 Signature Validation

CERTUM's QESValidationQ service procedures for estabilishing wheter an electronic signature or electronic seal is technically valid relay on the process described in ETSI TS 119 102 [ETSI-119-102].

The following sections explains the way CERTUM QESValidationQ Service performs individual components of validation procedures, indicated the processes occurring and constraints.

When no specific requirement is set in the present document, requirements and rules from ETSI TS 119 102 clauses 5 shall apply in their entirely. When specific requirements and rules are set in the present specification, they shall prevail over the corresponding requirements from ETSI TS 119 102. In case of discrepancies between the present specifications and specifications from ETSI TS 119 102, the present specifications shall prevail.

4.1 Signature Validation model

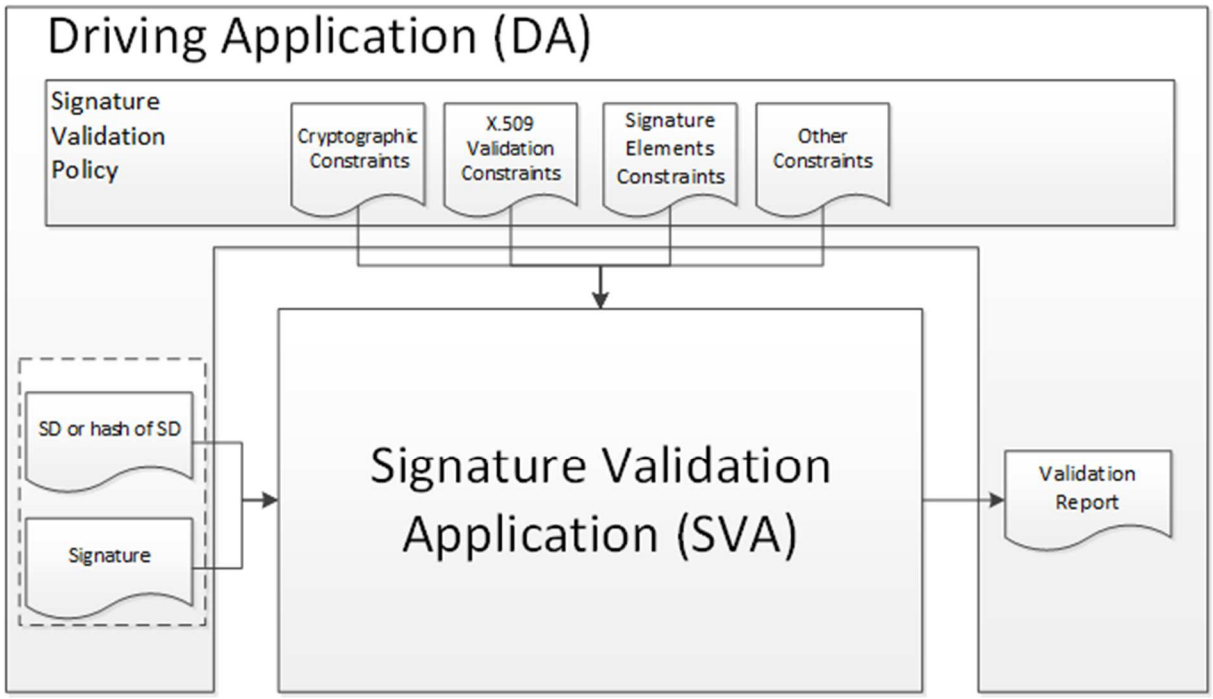

Figure 1 Signature Validation Conceptual Model

According to conceptual model of Signature Validation define in reffered specification CERTUM's QESValidationQ acts as a SVA. The SVA is called by the Driving Application (DA), to which it has to return the results of the validation process, in the form of a validation report. Driving Application (DA) for CERTUM QESValidationQ Service could be:

- Web based client with graphical interface,
- Client under protocol DVCS,
- Client under protocol OASIS-DSS,

- Client under protocol XKMS,
- Validation Gateway,
- Email Validation Interface,

These possible Driving Applications are generaly described in chapter 8 and 11.

4.1.1 Selecting validation processes

CERTUM QESValidationQ service supports the Validation Process for Basic Signatures and the Validation Process for Signatures with Time and Signatures with Long-Term Validation Data.

There's no possibility to specifies the process to be used by the DA.

When validating an instance of a signature or a seal, CERTUM QESValidationQ service proceed as follows:

1) SVA performs the Validation Process for Signatures with Time and Signatures with Long-Term Validation Material and it goes to step 2.
2) The SVA performs the Validation Process for Basic Signatures.
3) When the validation status returned by the selected validation process returned the status indication PASSED, the SVA provides the status indication TOTAL-PASSED to the DA.
4) When the validation status returned by the selected validation process returned the status indication FAILED, the SVA provides the status indication TOTAL-FAILED to the DA.
5) Otherwise, the SVA provides the status indication INDETERMINATE to the DA.

4.1.2 Status indication of the signature validation process and signature validation report

CERTUM QESValidationQ service provides a comprehensive report of the validation, allowing the DA to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the service.

The web client delivered together with CERTUM QESValidationQ service, when a human user is involved, presents the report in a way meaningful to the user – human readable form – PDF.

The signature validation process output contains:
a status indication of the results of the signature validation process

an indication of the policy which the signature has been validated

the date and time for which the validation status was determined together with the validation data used for the determination; and

the validation process that has been used in validation;

additional validation report data as specified in tables below;

signature creation reason attribute when attached to the provided signature

Table 1 Status indication of the signature validation process

Status indication	Semantics	Associated Validation report data
TOTAL-PASSED	The signature validation process results into TOTALPASSED based on the following considerations: • the cryptographic checks of the signature succeeded (including checks of hashes of individual data objects that have been signed indirectly); • any constraints applicable to the signer's identity certification have been positively validated (i.e. the signing certificate consequently has been found trustworthy); and • the signature has been positively validated against the validation constraints and hence is considered conformant to these constraints.	The validation process outputs the validated certificate chain, including the signing certificate, used in the validation process, together with specific signed attribute if present and considered validation evidences.
TOTAL-FAILED	The signature validation process results into TOTALFAILED because the cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly) or it has been proven that the generation of the signature took place after the revocation of the signing certificate.	The validation process outputs additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.
INDETERMINATE	The available information is insufficient to ascertain the signature to be TOTAL-PASSED or TOTAL-FAILED	The validation process outputs additional information to explain the INDETERMINATE indication and to help the verifier to identify what data is missing to complete the validation process.

Table 2 Validation Report Structure and Semantics

Main indication	Sub indication	Semantics	Associated Validation report data
TOTAL-FAILED	HASH_FAILURE	The signature validation process results into TOTAL-FAILED because at least one hash of a signed data	The validation process provides an identifier uniquely identifying the element within the signed data object that

		object(s) that has been included in the signing process does not match the corresponding hash value in the signature.	caused the failure in form of signing certificate
	FORMAT_FAILURE	The signature is not conformant to one of the supported standards 5.2 to the extent that the cryptographic verification building block is unable to process it.	The validation process provide any information available why parsing of the signature failed.
	SIG_CRYPTO_FAILURE	The signature validation process results into TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the signing certificate.	The validation process outputs the signing certificate used in the validation process.
	REVOKED	The signature validation process results into • TOTAL-FAILED because: the signing certificate has been revoked; and • there is PoE available that the signing time lies after the revocation time.	The validation process provides the following: • The certificate chain used in the validation process. • The time and, if available, the reason of revocation of the signing certificate. • The CRL, if available, on which revocation status was found • TheTimeStampover Signature, from unsigned attributes, if available, which indicates the earliest known time when signature existed
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	The signature validation process results into INDETERMINATE because one or more attributes of the signature do not match the validation constraints.	The validation process outputs: • The certificate chain used in the validation process. • Additional information regarding the reason
	CHAIN_CONSTRAINTS_FAILURE	The signature validation process results into INDETERMINATE because the certificate chain used in the validation process does not match the	The validation process outputs: • The certificate chain used in the validation process. • Additional information regarding the reason.

		validation constraints related to the certificate.	
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The signature validation process results into INDETERMINATE because he set of certificates available for chain validation produced an error for an unspecified reason.	The process outputs: • Additional information regarding the reason.
	CRYPTO_CONSTRAINTS_FAILURE	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and: • this material was produced after the time up to which this algorithm/key was considered secure (if such a time is known); and • the material is not protected by a sufficiently strong timestamp applied before the time up to which the algorithm/key was considered secure (if such a time is known).	The process outputs: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level.
	EXPIRED	The signature validation process results into INDETERMINATE because the signing time lies after the expiration date (notAfter) of the signing certificate.	The process outputs: • The validated certificate chain.
	NOT_YET_VALID	The signature validation process results into INDETERMINATE because the signing time lies before the issuance	

		date (notBefore) of the signing certificate.	
	NO_SIGNING_CERTIFICATE_FOUND	The signature validation process results into INDETERMINATE because the signing certificate cannot be identified.	
	NO_CERTIFICATE_CHAIN_FOUND	The signature validation process results into INDETERMINATE because no certificate chain has been found for the identified signing certificate.	
	REVOKED_NO_POE	The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the signing time lies before or after the revocation time.	The validation process shall provide the following: • The certificate chain used in the validation process. • The time and the reason of revocation of the signing certificate.
	OUT_OF_BOUNDS_NO_POE	The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate.	
	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The signature validation process results into INDETERMINATE because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is	The process outputs: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level.

		no proof that this material was produced before the time up to which this algorithm/key was considered secure.	
	NO_POE	The signature validation process results into INDETERMINATE because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g.broken algorithm).	The validation process identifies at least the signed objects for which the POEs are missing. The validation process should provide additional information on the problem.
	TRY_LATER	The signature validation process results into INDETERMINATE because not all constraints can be fulfilled using available information. However, it may be possible to do so using additional revocation information that will be available at a later point of time.	
	SIGNED_DATA_NOT_FOUND	The signature validation process results into because signed data cannot be obtained.	The process outputs when available: • The identifier (s) (e.g. an URI) of the signed data that caused the failure.
	GENERIC	The signature validation process results into INDETERMINATE because of any other reason.	The validation process outputs: • Additional information why the validation status has been declared INDETERMINATE.

5 Validation Policy

CERTUM QESValidationQ Service operates under default validation policy.
There's no possibility to configure validation constraints for Relaying Parties.

5.1 Validation constraints

CERTUM QESValidationQ service validation constraints are defined explicitly in system specific control data and by the implementation itself.

Any validation constraints not implied by the implementation originate from the signature content itself directly (included in the the signed attributes) or indirectly, i.e. by reference to an external document, provided in a machine processable form
Additional constraints could be provided by the DA to the SVA via parameters selected by the application or the user.

This additional constraint could be provided after mutual agreement between CERTUM QESValidationQ Service Provider and Relaying Party.

5.1.1 General Constraints

CERTUM QESValidationQ service supports following general constraints.

Table 3

Constraint(s)	Constraint value at signature validation (SVA or DA)
TSA service used for timestamping validation responses	CERTUM QTST
Maximum file size of supported documents	10MB

5.1.2 X.509 Validation Constraints

CERTUM QESValidationQ service supports following X.509 validaion constraints which indicate requirements for use in the certificate path validation process as specified in ETSI TS 119 172-1 [ETSI 119 172-1], clause A.4.2.1, table A.2 row m.

Table 4

Constraint (s)	Constraint value at signature validation (SVA or DA)
(m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows:	
(m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process.	EU TSL
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of	

length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any.	
• (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) • (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) • (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) • (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) • (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) • (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) • (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it) • (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path).	None
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows:	
(m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a	eitherCheck

possible set of requirement values used to express such requirements is defined as follows: – clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); – ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; – bothCheck: Both OCSP and CRL checks shall be carried out; – eitherCheck: Either OCSP or CRL checks shall be carried out; – noCheck: No check is mandated.	
(m)2.2. RevocationFreshnessConstraints: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation or require the SVA to only accept revocation information issued a certain time after the signature has been created.	No
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	No
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process, i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chains validated during the signature validation process.	No
EUQualifiedCertificateRequired	true
EUQualifiedCertificateSigRequired	true
EUQualifiedCertificateSealRequired [1]	true

[1] Based on Annex C from [ETSI 119 172-1]:
The following constraints indicates requirements on specific certificate metadata whose semantic applies in the context of the EU legislation:
a) EUQualifiedCertificateRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate as defined in the applicable EU legislation; expressed as a boolean.

PKIX Certification Path Validation Model 2	Chain model
CRLCache enabled If enabled then CRL will be upload for each validation	true
CRLCache time Time for which CRL could be stored in cache	30 seconds
TSLUnavilable In case TSL is unavailable	Last available

5.1.3 Cryptographic Constraints

CERTUM QESValidationQ service supports following cryptographic constraints which indicate requirements on algorithms and parameters used when creating signatures or used when validating signed object as specified in ETSI TS 119 172-1 [ETSI 119 172-1], clause A.4.2.1, table A.2 row p.

Table 5

Constraint(s)	Constraint value at signature validation (SVA or DA)
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). They will be typically be represented by a list of entries as in table A.3.	Based on ETSI TS 119 312 [ETSI 119 312]

5.1.4 Signature Elements Constraints

CERTUM QESValidationQ service supports following signature elements constraints which indicate requirements on the DTBS as specified in ETSI TS 119 172-1 [ETSI 119 172-1], clause A.4.2.1, table A.2 row b.

Table 6

Constraint(s)	Constraint value at signature validation (SVA or DA)
(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of the data to be signed by the signer.	None
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicate the required content related information elements under the form of signed or unsigned	None

b) EUQualifiedCertificateSigRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic signature as defined in [eIDAS]; expressed as a boolean.
c) EUQualifiedCertificateSealRequired: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic seal as defined in [eIDAS]; expressed as a boolean.

[2] [Validation Model]

qualifying properties that are mandated to be present in the signature. This includes: (b)2.1 MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. (b)2.2 MandatedSignedQProperties-content-hints to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. (b)2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. (b)2.4 MandatedSignedQProperties-content-identifier to require the presence of, and optionally a specific value for, an identifier that can be used later on in the signed qualifying property "content-reference" attribute.	
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • whole: the whole data has to be signed; • parts: only certain part(s) of the data have to be signed. In this case additional information should be used to express which parts have to be signed.	None

5.2 Supported electronic signature and electronic seal formats and levels

The following electronic signature and electronic seal formats applies in the context of the EU legislation [EU 2015/1506] and are supported by CERTUM's QESValidationQ Service:

[1] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile

[2] ETSI TS 103 173 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

[3] ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile

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

5.2.1 Restrictions on the supported electronic signatures and electronic seals

Table 7

Signature and signed data object placement; Number of signatures and signed data objects	Value
Enveloped signatures	true
Enveloping signatures	true
Detached signatures	true
Simultaneous multiple relative positions	true
One document is signed by more than one signature	true

6 CA Coverage

6.1 EU's Trust Status List (TSL) System

An immediate and prioritised action point in [eIDAS] is establishment of a European system of Trust Status Lists (TSL) covering qualified CAs.

7 Customer (Relying Party) Interface

CERTUM QESValidationQ Service is available as Web Services, i.e. as defined XML structures exchanged over the SOAP [SOAP] protocol. Only synchronous communication is REQUIRED, although asynchronous calls MAY be supported.

7.1 Signature Validation, OASIS DSS Interface

The OASIS DSS interface profile defined by [PEPPOL-D1.3] part 6 is offered. This specification must be assumed to be subject to changes according to ongoing standardisation work [OASIS-DSS-X]. The specification is governed by the PEPPOL project until the end of this project.

7.2 Signature Validation, DVCS Interface

The DVCS protocol defined by [RFC 3019] is offered.

7.3 Certificate Validation, XKMS v2 Interface

The XKMS v2 interface profile defined by [PEPPOL-D1.3] part 5 is offered. This specification is assumed to be stable. The specification is governed by the PEPPOL project until the end of PEPPOL.
In PEPPOL, bremen online services has developed an XKMS responder component (server side component) according to the specifications of [PEPPOL-D1.3] part 5. The component is

provided as open source software. Software, source code and documentation are available on OSOR3. See Attachment A to [PEPPOL-D1.2] for documentation on the XKMS v2 responder software component.

8 Options

This chapter contains requirements for functionality that CERTUM QESValidationQ trust service provider MAY choose to offer. If an option is offered by CERTUM QESValidationQ trust service provider, the Customer MAY choose to include this in the Agreement from the start or at a later stage.

8.1 Validation Gateway

[PEPPOL-D1.3] part 4 describes use of a Validation Gateway to avoid sending entire documents with potentially confidential content to the VS. As described, the Validation Gateway builds an OASIS DSS request (see also [OASIS-DSS-Gateway]) containing pairs of hash values and signature elements, but no document content, and sends this to the VS over the OASIS DSS interface offered by the VS. This is shown in **Błąd! Nie można odnaleźć źródła odwołania.** below.
The Validation Gateway is installed (software package, possibly dedicated hardware) on the client side. A Validation Gateway installation may be dedicated to one domain (e.g. one public service owner) or it may be reusable across domains (e.g. offered from the Customer to several public service owners).
A Validation Gateway additionally has the following advantages:
The Validation Gateway increases the efficiency of VS operation since potentially large documents do not have to be sent to the VS.
The Validation Gateway provides a single point of policy enforcement since the Validation Gateway may decide policy requirements (request parameters) for all requests passing through the Validation Gateway.
Keys and certificates for TLS client authentication and/or request signing towards the VS may be installed only in the Validation Gateway and not in each end system in need of VS integration.
The two latter bullet points are valid even for eID validation by XKMS, meaning that a Validation Gateway for the XKMS interface is also a possibility.
A Validation Gateway using the VS' XKMS interface can also be an option if the VS offers only the XKMS interface but a signature verification service is still needed. E.g. the Validation Gateway can offer signature verification through a Web GUI, verifying the signatures in the Validation Gateway but forwarding certificates to the VS over the XKMS interface.

8.2 Web GUI Interface

Consequently, a web based GUI (graphical user interface) service MAY be offered by the CERTUM QESValidationQ trust service provider, either directly towards the VS or via a Validation Gateway. By access to the GUI a human user can upload a signed document or an eID certificate, select request parameters and return parameters, and send the resulting request to

[3] Open Source Observatory and Repository for European public administrations, http://www.osor.eu. Results from PEPPOL are available in http://www.osor.eu/projects/peppol.

the VS. The GUI input SHOULD be translated to an XKMS or OASIS DSS request but an alternative interface to the VS MAY be used.

8.3 Email Validation Interface

CERTUM QESValidationQ trust service provider MAY offer an email VS interface. A signed document or an eID certificate may be sent to the VS, or to a Validation Gateway, as an attachment to an email; or the object may actually be a signed email itself. The attachment may be used to form an XKMS or OASIS DSS request according to some default policy (request parameters). The response can be sent back to the user as an email attachment – e.g. an XKMS or OASIS DSS response structure, optionally with style sheet for display included.
If the email interface is to a Validation Gateway, the email may be only internal to the requestor's company. If email is directly to the VS, proper protection of email content and access control to the VS are necessary.

Annex A: Relationship with the Regulation (EU) No 910/2014

A.1 Validation of qualified signatures under eIDAS: Article 28 and 32

Requirements from Article 32 and 28 in the Regulation (EU) No 910/2014 [eIDAS]	Implementation according to the CERTUM's QESValidationQ Service
Requirements for the validation of qualified electronic signatures 1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:	
(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	Certificate validation process fullfils requirements described in [EU 2015/1505] for qualified trust service providers issuing qualified certificates for electronic signatures. Moreover compliance with Annex A.1 ETSI 119 412-5 [ETSI 119 412-5] is assessed
(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	
(c) the signature validation data corresponds to the data provided to the relying party;	Guaranteed by correctnes of supported signature formats 5.2
(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	Signing certificate is included in validation report for each supported protocol as described in Table 2 Validation Report Structure and Semantics
(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	Since indication of pseudonym used is included within Subject field of signing certificate [ETSI 119 412-2] the use of any pseudonym is clearly indicated within provided validation report (Table 2 Validation Report Structure and Semantics)
(f) the electronic signature was created by a qualified electronic signature creation device;	Certificate validation process fullfils requirements described in [EU 2015/1505] for qualified trust service providers issuing qualified certificates for electronic signatures. In particular check for correct indication of the nature of the SSCD support is done.
(g) the integrity of the signed data has not been compromised;	Guaranteed by supported signature validation model as described in 4

(h) the requirements provided for in Article 26 were met at the time of signing.	Provided below.
2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	Signature validation process together with provided status indication is described in 4
Article 28: Qualified certificates for electronic signatures	
1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.	Compliance with Annex A.1 ETSI 119 412-5 [ETSI 119 412-5] is assessed.
2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.	Certificate validation process fullfils requirements described in [EU 2015/1505] for qualified trust service providers issuing qualified certificates for electronic signatures. There's no additional checks performed to this laid down in Annex I.
3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.	There's no additional checks performed to this laid down in Annex I.
4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	Requirement for qualified trusted services issuing qualified certificates for electronic signatures.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature: (a)if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension; (b)the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.	According to [ETSI TS 110 102-1] if the certificate path validation returns a failure indication because the signing certificate has been determined to be on hold, CERTUM's QESValidationQ Service will terminate validation returning the indication INDETERMINATE, the sub-indication TRY_LATER, the suspension time and, if available, the content of the nextUpdate -field of the CRL or OCSP-response used as the suggestion for when to try the validation again.
Article 26: Requirements for advanced electronic signatures An advanced electronic signature shall meet the following requirements:	

(a) it is uniquely linked to the signatory;	Guaranteed by correctnes of supported signature formats 5.2
(b)it is capable of identifying the signatory;	
(c)it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and	
(d)it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.	

A.2 Validation of qualified seals under eIDAS: Article 38 and 40

Requirements from Article 38 and 40 in the Regulation (EU) No 910/2014 [eIDAS]	Implementation according to the CERTUM's QESValidationQ Service
Qualified certificates for electronic seals	
1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.	Compliance with Annex A.2 ETSI 119 412-5 [ETSI 119 412-5] is assessed.
2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.	Certificate validation process fullfils requirements described in [EU 2015/1505] for qualified trust service providers issuing qualified certificates for electronic seals. There's no additional checks performed to this laid down in Annex III.
3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.	There's no additional checks performed to this laid down in Annex III.
4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	Requirement for qualified trusted services issuing qualified certificates for electronic seal.
5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:	According to [ETSI TS 110 102-1] if the certificate path validation returns a failure indication because the signing certificate has been determined to be on hold, CERTUM's QESValidationQ Service will terminate validation returning the indication INDETERMINATE, the sub-indication

(a)if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension; (b)the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.	TRY_LATER, the suspension time and, if available, the content of the nextUpdate -field of the CRL or OCSP-response used as the suggestion for when to try the validation again.
Validation and preservation of qualified electronic seals	
Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	

History

Document history		
1.0	03 czerwca 2016 r.	**Initial draft**