Policy for qualified validation service and qualified preservation service for qualified electronic signatures and electronic seals (Certum QESValidationQ)

Version 1.5

Effective Date: January 28th 2022

Asseco Data Systems S.A.
Jana z Kolna Street 11
80-864 Gdańsk, Poland
www.assecods.pl/en/

Certum
Bajeczna Street 13
71-838 Szczecin, Poland
www.certum.eu

Trademark and Copyright notices

Table of Contents

1 Introduction, scope and assumptions

Policy of qualified validation service and qualified preservation service for qualified electronic signatures and electronic seals (Certum QESValidationQ) presents a set of rules required to issue a qualified validation and preservation tokens (formerly known as data validation and credentials), in accordance with the requirements set out 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, especially in Article 33 and 34, and the accompanying delegated and implementing acts, and in European Standards produced by the ESI ETSI Technical Committee.
Compliance with the requirements set out in Articles 33 and 34 of the Regulation, is described in Annex A.3 and A.4.

The set of policies described in this document reflects business, legal, and security policy requirements. The basis for specific policy and security requirements for signature validation service is [ETSI TS 119 441], and for preservation service [ETSI TS 119 511].

According to the point 6 of the Commission Implementing Decision (EU) [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 policies described in this document regarding electronic signatures also *apply mutatis mutandis* to electronic seals.

1.1 TSP Identification

Certum QESValidationQ service provider is Asseco Data Systems S.A., which description could be found on polish TSL under: https://webgate.ec.europa.eu/tl-browser/#/tl/PL/9

1.2 Document name, its identification and dependencies

The present document is given a proper name of: **Policy of qualified validation service and qualified preservation service for qualified electronic signatures and electronic seals (Certum QESValidationQ)**; this document is available as an electronic version on the website of the qualified trust service provider at: www.certum.eu.

With the present document the following registered object identifier is connected (OID: 1.2.616.1.113527.2.4.1.0.5.1.5):

> **id-cck-kpc-v1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-ESSVP(5) version(1) 5}**

in which the last two numeric values correspond to the current version and subversion of this document.

This document is a document that bases and supplements the "Certification Policy and Certification Practice Statement of Certum Qualified Services", hereinafter referred to as the Main Policy, which defines the general rules applied by Certum during the provision of qualified trust services.

2 References

References can be based on selected versions/editions of documents (with an indicated publication date and/or edition or version number) or on versions incorporating changes that have been made. For the documents listed at the beginning, only the exact version indicated applies. For all other documents, the latest version of the document (including revisions) applies.

2.1 Normative References

[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 Information references

[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 119 441] ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services v1.1.1 (2018-08)

[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 319 401] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[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 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 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

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

[ETSI 119 511] ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

[ETSI 119 512] ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

[ETSI 101 733] ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES)

[ETSI 101 903] ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

[ETSI 319 412-2] ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[ETSI 319 412-5] ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[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

[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

[RFC3029] 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

Certum QESValidationQ - denotes a qualified validation and qualified preservation services for qualified electronic signatures and electronic seals provided by Certum

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	Regulation (EU) No 910/2014 of the European Parliament [eIDAS]
EU	European Union
ETSI	European Telecommunications Standards Institute
ESI	ETSI Technical Committee Electronic Signatures and Infrastructures
GUI	Graphical User Interface
Main Policy	"Certification Policy and Certification Practice Statement of Certum Qualified Services", which defines the general rules applied by Certum during the provision of qualified trust services
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol [RFC2560]
PDF	Portable Document Format [PDF]
PDS	Preservation of Digital Signatures
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 Existence
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]
WST	Preservation Service with storage
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 and Preservation

The set of procedures of the Certum validation and preservation services for verifying whether an electronic signature or electronic seal is technically valid, is based on the process described in ETSI TS 119 102-1 [ETSI 119 102].

In case the following document does not contain a description of specific requirements, it is assumed that the requirements and principles from ETSI TS 119 102 point 5 are fulfilled in their entirety. Where the following document contains a description of requirements and rules, this means that they take precedence over the corresponding requirements in ETSI TS 119 102.

The present document describes preservation mechanisms that can be used to maintain the long-term evidential validity of electronic signatures or to preserve objects using electronic signature techniques. These mechanisms support a qualified preservation service in accordance with Articles 34 and 40 of eIDAS.

4.1 Signature Validation model

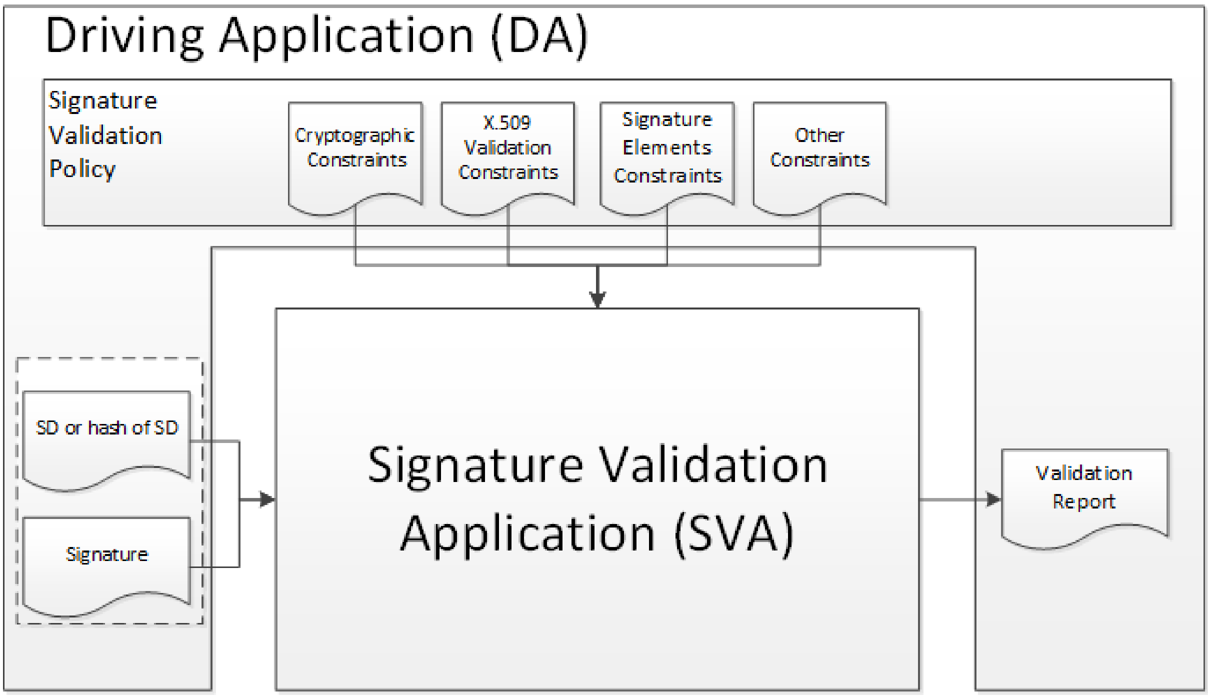
Driving Application (DA)
Signature Validation Policy
Cryptographic Constraints
X.509 Validation Constraints
Signature Elements Constraints
Other Constraints
SD or hash of SD
Signature
Signature Validation Application (SVA)
Validation Report

Figure 1 Signature Validation Conceptual Model

The above diagram of a conceptual model for a signature validation application is proposed in Technical Specification ETSI TS 319 102. The individual elements of the diagram stand for:

- Driving Application (DA) – a driving application; an application that uses a signature validation system to validate signatures;

- Signature Validation Policy – a signature validation policy; a set of rules applicable to one or more electronic signatures that defines technical and procedural requirements for their validation to meet a specific business need under which an electronic signature can be considered valid;
- Cryptographic Constraints – cryptographic rules; a set of applied rules, values, ranges and results of calculations in the field of cryptography, according to which a signature is validated;
- X.509 Validation Constraints – rules regarding X.509 validation;
- Signature Elements Constraints;
- Other Constraints;
- SD or hash of SD – signed data or hash of signed data;
- Signature;
- Signature Validation Application (SVA);
- Validation Report.

According to the conceptual model of the signature validation application, the Certum service is an SVA component. The SVA is invoked by the control application (DA), to which the result of the validation process is then returned in the form of a validation report. The controlling application (DA) for the Certum service is available as:

- A web application with a graphical user interface,
- A client compliant with DVCS protocol,
- OASIS-DSS protocol compliant client,
- Client compliant with XKMS protocol,
- Validation Gateway.

The above mentioned control applications (DA) are implemented in the form of a web interface or a Validation Gateway as described in Chapter 7.

When the Certum service calculates a digest from the signed data (this happens in the Validation Gateway), integrity is ensured for the transmitted signed data.

The communication channel between the client and the Certum service is secured.
The client of the Certum service is authenticated. Requests sent between the control application and the service are signed.

The web application with a graphical user interface where the validation report is presented, is secured with a TLS session. The page is secured through a Trusted SSL certificate issued by Certum.

4.1.1 Selecting validation processes

The Certum QESValidationQ service supports the validation process of qualified signatures in the following cases: standard signatures, time-stamped signatures and signatures with long-term evidential value.

It is not possible to select the case according to which the validation is to be performed by the Driving Application (DA).

4.1.2 Description of the signature validation process results and validation process report

The Certum service provides a full validation process report, allowing the DA to check the individual steps taken in the validation process along with the ability to see why the process returned a different result.

For the same input data, the Certum service should return the same validation status. However, it may happen that for a longer period of time the validation result for the same document will change, as it depends on many components, e.g. trusted signature time, validity period of the signer's certificate, availability of certificate validity information.

If the user uses the web application delivered with the Certum service or the Validation Gateway (described in chapter 7), the validation process report is presented in a user-friendly PDF file.

The Certum service ensures consistency between the validation process report in PDF form, in machine-readable form, and presented in the web application.

The validation report is signed with a certificate which identifies the service. The report signature is in basic form, the time-stamp is not added.

The service certificate with which the validation reports are signed is identified by:

Certificate serial
190776352711112402811911134056768917207409779927

Digest algorithm
SHA512

Issuer
OID.2.5.4.97=VATPL-5250008198, CN=National Certification Centre, O=National Bank of Polan, C=PL

Subject
OID.2.5.4.97=VATPL-5170359458, CN=Certum QESValidationQ 2017, O=Asseco Data Systems S.A., C=PL

Validity
2017-03-15 11:25:12 - 2028-03-16 00:59:59

The validation report doesn’t conform to ETSI TS 119 102-2, as the TS was published when service already supported the validation report defined by OASIS-DSS protocol. Both of them have the same basis OASIS.

The result of the signature validation process consists of:

- the status of the signed document validation process,
- a unique identifier of the issued certificate,
- date together with the time for which the indicated result of the validation process is valid, together with information which date was used in the validation process,
- indication whether the signature or the electronic seal was validated,
- signature validation statuses, for each of the signatures concerning the document, described in Table 1 Statuses of the signature validation process and Table 2 Structure and description of the validation report,
- information about the hash algorithm used in each of the signatures,
- information identifying the signer, for each of the signatures,
- information about the quality of the time-stamp used in the signature, if added, for each signature,
- the reason for the signature, if included in the signature being checked,
- other signature attributes, if included in the signature,
- the identifier indicating the validation process that has been used in validation
- the list of evidence used in the validation process (CRLs, OCSP responses, TSLs, time-stamp tokens).

Table 1. Status of the signature validation process

Status	Description	Associated validation report data
TOTAL-PASSED	A TOTAL-PASSED result in the validation process is returned when: • the cryptographic verification of the signature was successful (including checking the hash values of individual data objects that were indirectly signed); • all requirements concerning the signer's identity certification were positively verified (e.g. the signer's certificate was recognized as trusted); • the signature has been positively assessed against the	As a result of the validation process, the certificate chain of trust used in the document signing process is displayed along with the specific signed attributes, if any, and considered as evidence of validation.

	requirements in the validation process, thus it is considered compliant with those requirements.	
TOTAL-FAILED	A TOTAL-FAILED result in the validation process is obtained if the cryptographic verification of the signature failed (including a check of the hash values of individual data objects that were signed) or it was proven that the signature was created after the revocation date of the associated certificate.	As a result of the validation process, additional information is provided to explain the reason for the TOTALLY NEGATIVE status.
INDETERMINATE	The information available is insufficient to determine whether the certificate should be in a TOTAL-PASSED or TOTAL-FAILED status.	As a result of the validation process, additional information is provided to explain the reason for the UNKNOWN status along with information, for the validating party, what data is missing to correctly pass the full validation process.

Table 2. Validation Report Structure and Semantics

Status	Sub status	Description	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 object that has been included in the signing process does not match the corresponding hash value in the signature.	The signature validation process unambiguously indicates which element of the signed data caused the negative signature validation result.
	FORMAT_FAILURE	The signature does not conform to any of the supported standards to the point that it is impossible to perform cryptographic verification of the signature.	The validation process provides information indicating why the signature analysis 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 returns a result of • TOTAL-FAILED if the signer's certificate has been revoked and • when there is evidence that the time of signing occurred after the revocation of the signer's certificate	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 • The time-stamp over signature, from unsigned attributes, if available, which indicates the earliest known time when signature existed

	EXPIRED	The signature validation process results into INDETERMINATE if 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 if the signing time lies before the beginning of validity date (notBefore) of the signing certificate.	
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	The signature validation process results into INDETERMINATE, if 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, if the certificate chain used in the validation process does not match the validation constraints related to the signer's certificate.	The validation process outputs: • The certificate chain used in the validation process. • Additional information regarding the reason.
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The signature validation process results into INDETERMINATE, if the set of certificates available for chain validation returns an error for an unspecified reason.	The validation process outputs: • Additional information regarding the reason.
	CRYPTO_CONSTRAINTS_FAILURE	The signature validation process results in an INDETERMINATE status if at least one of the algorithms used in the signature elements or the key length of the algorithm are below the required security level, and: • this element was generated after a period of time when the algorithm/key in question was	The process outputs: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level.

		considered secure (for example, when the date of generation is known); • this element is not protected by a sufficiently strong time-stamp applied during the time period in which the algorithm/key was considered secure.	
	NO_SIGNING_CERTIFICATE_FOUND	The signature validation process results into INDETERMINATE if the signing certificate cannot be identified.	
	NO_CERTIFICATE_CHAIN_FOUND	The signature validation process results into INDETERMINATE if no certificate chain has been found for the identified signing certificate.	
	REVOKED_NO_POE	The signature validation process results into INDETERMINATE if the signer's certificate was revoked at the time of signature validation. However, the signature validation algorithm cannot determine whether the signature date is before or after the certificate revocation date.	The validation process returns the following information: • The certificate chain used in the validation process, • The time and, if available, the reason for revocation of the signing certificate.
	OUT_OF_BOUNDS_NO_POE	The signature validation process results into INDETERMINATE, if the signer's certificate is outdated or not yet active at the time of the validation process and the signature validation algorithm cannot determine if the signature date is within the validity period of the signer's certificate.	
	CRYPTO_CONSTRAINTS_FA	The signature validation process results into	The process outputs:

	ILURE_NO_POE	INDETERMINATE, if at least one of the algorithms used in the signature elements or the key length of the algorithm is below the required security level and there is no evidence that the indicated signature elements were generated during the time period when the algorithm/key was considered secure.	• Element identification information (signature, certificate) that is generated using an algorithm or cryptographic key with a length below the required security level.
	NO_POE	The signature validation process results into INDETERMINATE if there is no evidence to unambiguously conclude that the object was signed before the compromising event (e.g., algorithm breakage) occurred.	The validation process identifies at least one object, for which the PoE is missing. The validation process provides additional information about the error that is occurring.
	TRY_LATER	The signature validation process results into INDETERMINATE, if not all constraints can be fulfilled, due to the lack of information.. However, it is possible to redo the validation process using additional certificate revocation information that will be available at a later date.	
	SIGNED_DATA_NOT_ FOUND	The signature validation process results into INDETERMINATE, if signed data cannot be obtained.	The validation process outputs: • The identifier(s) (e.g. an URI) of the data, that caused the failure.
	GENERIC	The signature validation process results into INDETERMINATE if any other error not described in this table has occurred	The validation process outputs: • Additional information why the validation status has been declared INDETERMINATE.

4.2 Signature Preservation Model

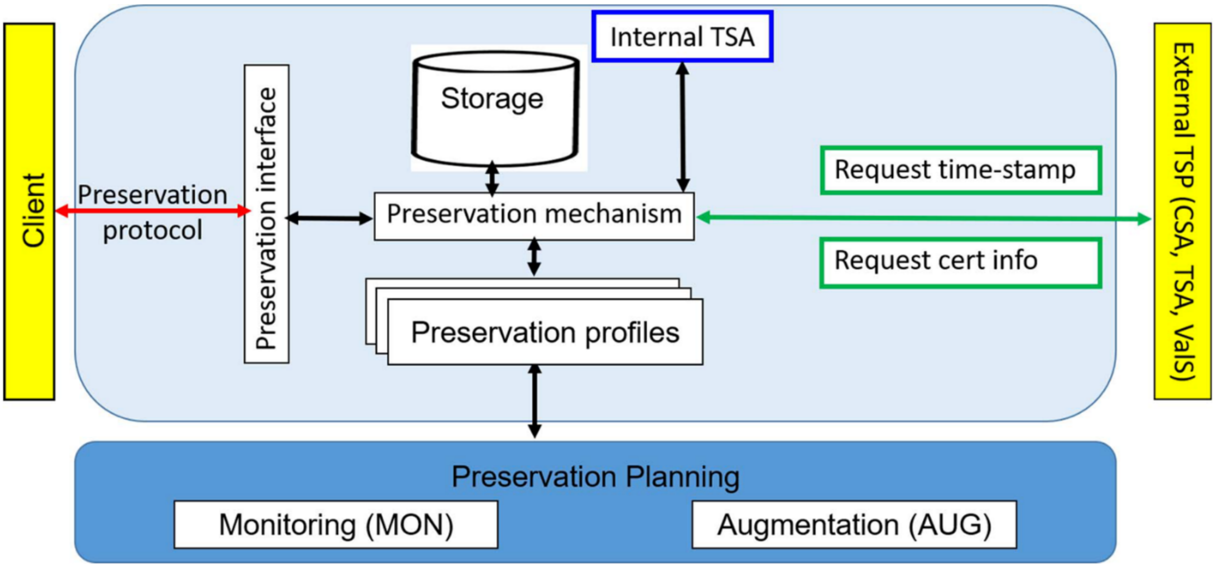

Figure 2. Conceptual Model of preservation service with storage

The above schema for the conceptual model of a preservation service with storage is proposed in the ETSI TS 119 511 technical specification. The individual elements of the schema stand for:

- Client – Subscriber of the service; a legal or physical person providing data to the service for preservation purposes;
- Preservation protocol – protocol for communication between the Subscriber and the service;
- Preservation interface – component that implements the preservation protocol on the service side;
- Storage – data repository;
- Preservation mechanism – a mechanism used to maintain the long-term evidential validity of preserved objects;
- Preservation profiles – preservation profile; a uniquely identified set of implementation details associated with a preservation model that defines, among other things, how preservation evidence is generated and validated;
- Internal TSA – internal time-stamping authority;
- Preservation Planning – the component responsible for monitoring and augmenting maintenance evidence;
- Monitoring (MON) – monitoring of cryptographic algorithms;
- Augumentation (AUG) – augmentation of preservation evidence;
- Request time-stamp;
- Request cert info;

- External TSP (CSA, TSA, ValS) – external trust services: CSA Certificate Status Authorities, TSA Time-Stamp Authorities, ValS Validation Service.

The requirements imposed on the preservation service by the eIDAS regulation closely link this service to the validation service.

Key requirements include:

- The preservation service validates the submitted data according to the signature validation policy and verifies that the submitted data is appropriate.
- The preservation service provides the proof of existence of a signature and the validation data necessary for the signature validation process using electronic signature techniques.
- The Preservation Service provides evidence of the existence of a signature and the validation data necessary for the signature validation process and evidence of the existence of signed data if signed data has been submitted to the service.
- In the case of external signatures or if the Subscriber uses a Validation Gateway, the preservation service allows the Subscriber to provide only a hash of the signed data instead of the full signed data - the QTSP indicates in the preservation profile the hash functions that can be used.

The Certum service, acting as a preservation service, uses the Validation service to validate the submitted signatures. It then collects the maintenance proofs. The proofs are cryptographically secured and stored for the period specified in the maintenance profile. The proofs are secured using a qualified time-stamp provided by Certum QTSA.

The communication channel between the client and the Certum service is secured.
The client of the Certum service is authenticated.

5 Validation and Preservation Policy

Certum QESValidationQ policy is a policy for validating that the signature (or seal) is a qualified signature (or qualified seal) compliant with eIDAS.

The service does not provide the ability for the user to specify a validation and preservation policy or to configure separate requirements for the validation and preservation process for each relying party. The validation process performed always conforms to the default policy.

Supported signature validation service policy

The supported signature validation policy is identified by the following object identifier, defined in [ETSI TS 119 441]:

itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)

Supported preservation service policy

The supported preservation policy is identified by the following object identifier, defined in [ETSI TS 119 511]:

itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2)

5.1 Validation constraints

The requirements for the validation process in the Certum QESValidationQ service are defined in the system control data and by the service implementation itself.

Any validation rules that are not derived from the implementation are derived directly from the signature content itself (contained in the signed attributes) or indirectly, i.e. by reference to an external document provided in machine processable form.

5.1.1 General Constraints

The Certum QESValidationQ service operates according to the following rules:

Table 3

Constraint(s)	Value
TSA service used for time-stamping 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)	Value
(m)1.1. SetOfTrustAnchors: This constraint indicates a set of acceptable trust anchors (TAs) as a constraints for the validation process.	EU TSL

• (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).	None
(m)2.1. RevocationCheckingConstraints: The constraints related to checking the revocation of a verified certificate. Specifies whether a certificate revocation check is required and whether it is checked using the response from the OCSP, or whether a CRL should be used. The following is a description of the requirements: – clrCheck: Verification shall be done against the 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

– eitherCheck: Either OCSP or CRL checks shall be carried out; – noCheck: There is no mandatory check.	
(m)2.2. RevocationFreshnessConstraints: The constraint for certificate revocation information and associated date ranges. Requirements specifying the maximum acceptable difference between the date of issuance of certificate revocation status information and the date the revocation became valid. A requirement that allows the SVA to accept only certificate revocation information created after the date of the electronic signature.	No
(m)2.3. RevocationInfoOnExpiredCerts: The constraint for a signing certificate used in validating a signature issued by a CA that retains information about revoked certificates for longer than the required minimum retention period.	No
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA level for the practices of the certifying TSPs.	No
EUQualifiedCertificateRequired	true
EUQualifiedCertificateSigRequired	true
EUQualifiedCertificateSealRequired [1]	true
PKIX Certification Path Validation Model	Chain model
CRLCache enabled If enabled then CRL will be upload for each validation.	true
CRLCache time The maximum period of time that a CRL can be cached.	30 seconds
TSLUnavilable In case TSL is unavailable	Last available
Impact of time-stamps on the validation results.	Only qualified time-stamps

[1] Based on Annex C from [ETSI 119 172-1]:

5.1.3 Cryptographic Constraints

The Certum QESValidationQ service supports the following cryptographic constraints that apply to the algorithms and parameters used in the creation of signatures or used in the validation of a 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)	Value
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements for algorithms and parameters used during creation of signatures or used during validation of signed objects occuring in the validation process (e.g. signatures, certificates, CRLs, OCSP responses, time-stamps).	According to ETSI TS 119 312 [ETSI 119 312]

5.1.4 Signature Elements Constraints

The 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)	Value
(b)1. ConstraintOnDTBS: This constraint indicates requirements on the type of the data to be signed.	None
(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This constraints set indicates the required content-related information elements, in the form of signed or unsigned attributes, required to be present in the signature. This includes: (b)2.1 MandatedSignedQProperties-DataObjectFormat: requires a specific format for the content being signed by the signer; (b)2.2 MandatedSignedQProperties-content-hints: require specific information describing the innermost signed content of a multilayer message in which one content is encapsulated in another for the content signed by the signer; (b)2.3 MandatedSignedQProperties-content-reference: requires the inclusion of information about how requests and responses should be linked between two parties or how such a link should be established, etc.; (b)2.4 MandatedSignedQProperties-content-identifier:	None

requires the presence, and optionally a value, of an identifier that can be used later in the "content-reference" attribute.	
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether all data, or just some of it, must be signed. The semantics for a possible set of values are: • 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 2015/1506] and are supported by Certum 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

5.3 Qualified electronic signature/seal relying on long-term availability of validation data

Certum QESValidationQ service allows the preservation of advanced electronic signatures or advanced electronic seals based on a qualified certificate as defined in eIDAS, that are time-stamped for a proof of existence.

The validation data is not submitted by the preservation client. The preservation service as a first step of preservation process collects and verifies the validation data according to the signature validation policy supported by the preservation profile. The ability to validate a digital signature and to maintain its validity status is obtained by making sure, that all needed validation data is collected, verified and protected using digital signature techniques.

Accumulated evidence is successively time-stamped before the earlier timestamp certificate expires or when the algorithms are deemed too weak for long-term protection.

Used time-stamp token is provided by qualified provider Certum QTST which follows the requirements of RFC 3161 and updated by RFC 5816 and time-stamp protocol and profiles as defined ETSI EN 319 422.

Recommendation for suitable cryptographic algorithms is based on in ETSI TS 119 312.

For every supported active preservation profile, Certum monitors the strength of every cryptographic algorithm that was used in connection with this profile. In case, one of the used algorithms or parameters is thought to become less secure or the validity of a relevant certificate is going to expire, the related preservation evidence policy will be updated, or a new preservation profile will be created to handle newly submitted POs.

5.3.1 Preservation profile

The preservation service is based on validation service which stores localy validation data for the qualified CAs. Validation data are collected on a day-to-day basis. This approach makes the service independent of the availability of validation data for whole preservation timeframe.

The same preservation policy will be used during the whole preservation period.

After the end of the Subsribers agreement period validity, for 1 month it is possible for the Subscriber to download the complete set of preserved data, after which the data is irreversibly deleted.

Certum QESValidationQ service allows one submission data object (SubDO) to be preserved under the specific preservation profile and receive back immediately (syncronous mode) a preservation evidence with a preservation object identifier included. A preservation evidence has form of validation process report, which includes serial number, which acts as a preservation object identifier.

The preservation service allows to delete stored POs. In case the deletion of the preservation evidence the corresponding SubDO shall be deleted as well. The preservation service assures that stored POs can only be deleted before the end of the preservation period when the delete request is submitted together with a justification. Any submitted justification is logged together with the information of the deletion request.

Certum QESValidationQ service implements one Preservation profile, described below:

a) **Identifier:** http://uri.etsi.org/19512/scheme/pds+wst+ers

b) **Supported operation:**

   i. PreservePO:

      1. Input formats:

         a. According to 5.2

         b. Allowed Hashes: according to 5.1.3

   ii. VerifyRequest

      1. Input formats:

         a. According to 5.2

         b. Allowed Hashes: according to 5.1.3

c) **Policy:**

   i. The preservation evidence policy: according to 5.3.2

   ii. The validation policy: according to chapters 4, 05.2

d) **Profile Validity Period:**

   i. Valid from: the date the service is placed on the TSL list

e) **Preservation storage model:** Preservation services with storage (WST)

f) **Preservation goal:** Preservation of digital signatures (PDS) http://uri.etsi.org/19512/goal/pds

g) **Evidence format:** validation response and time-stamp tokens

5.3.2 Preservation Evidence Policy

Preservation Evidence Policy is described by the following set of rules:

a) **Version:** 1

b) **Algoriths used:** RSA-PKCSv1, SHA-512 (in accordance with the recommendations of ETSI TS 119 312)

c) **Trust Anchors to be used to validate digital signature within preservation evidence:** QEsValidationQ identified by:

   Certificate serial
   190776352711112402811911134056768917207409779927

   Digest algorithm
   SHA512

   Issuer
   OID.2.5.4.97=VATPL-5250008198, CN=Narodowe Centrum Certyfikacji,
   O=Narodowy Bank Polski, C=PL

Subject
OID.2.5.4.97=VATPL-5170359458, CN=Certum QESValidationQ 2017, O=Asseco Data Systems S.A., C=PL

Validity
2017-03-15 11:25:12 - 2028-03-16 00:59:59

The PKI certificate corresponding to en electronic seal that is applied to a receipt returned to the client after submitting data to the preservation service. The certificate is issued by National Root CA.

d) **Trust Anchor to be used to validate time-stamps within preservation evidence:** Certum QTST identified by:

Certificate serial
100341102919473197820118384675833212695201296873

Digest algorithm
SHA512

Issuer
OID.2.5.4.97=VATPL-5250008198, CN=Narodowe Centrum Certyfikacji, O=Narodowy Bank Polski, C=PL

Subject
OID.2.5.4.97=VATPL-5170359458, CN=Certum QTST 2017, O=Asseco Data Systems S.A., C=PL

Validity
2017-03-15 11:23:18 - 2028-03-16 00:59:59

e) **Preservation evidence augmentation technics:** time-stamp renewal according to IETF RFC 4998

f) **Expected evidence duration:** 30 years

The evidence in form of the validation report is signed by certificate issued for QESValidationQ service, so the preservation service could be identified. The evidence don't contain explicit information about preservation evidence policy or preservation profile.

5.3.3 Export-import Packages Policy

Access to preserved electronic signatures is done according to the following rules:

- Available to authenticated Subscribers only;
- The structure of Export Package is based on the RetrievePOResponse, where we find a data validation request (containing signed data, or a hash of signed data), a validation response and a time-stamp chain;
- Preservation service keeps records of all released export packages including:

- The date of the event,
- The criteria that has been used to select the set of preservation objects to be included in the export package.

6 Supported API

Certum QESValidationQ service is available for machine processing through various types of APIs, both based on XML structures and ASN.1. Only synchronous communication is supported. The supported interfaces are listed below:

- OASIS-DSS

The service supports the profile defined by the PEPPOL project [PEPPOL-D1.3], based on XML structures. The protocol allows to send validation and maintenance requests for electronic signatures and seals.

- DVCS

Protocol defined in [RFC3029], based on ASN.1 structures. It allows to validate electronic signatures, seals and X.509 public key certificates.

- XKMS

The service supports the profile defined by the PEPPOL project [PEPPOL-D1.3], based on XML structures. The protocol allows to send verification requests for X.509 public key certificates.

- Preservation protocol

The service supports part of the protocol defined by ETSI TS 119 512. In particular supported operations are: RetrievePO, PreservePO and DeletePO. The protocol is protected against unauthorized usage.

Certum QESValidationQ service doesn't conform to ETSI TS 119 442, as the technical standard was published when service already supported, mentioned above, well-estabilished APIs. Especially OASIS-DSS protocol is comparable with ETSI TS 119 442 since they both re-use constructs of DSS-X core.

Certum QESValidationQ signature validation response doen't bear the OID of the service policy. Because the service supports only one validation policy it's not neccessery to add policy OID to response.

7 Additional options

This chapter describes the functionalities that Certum offers additionally.

7.1 Validation and Preservation Gateway

Validation and preservation Gateway allows to avoid sending entire signed documents with potentially confidential content or be large.
The Gateway is installed (software package) on the Subscriber's IT infrastructure side. It supports the same API for validating electronic signatures and seals as the Validation Service.
The advantages of using a gateway include:

- increased efficiency of the validation and preservation service, as large documents no longer need to be sent;

- provides a single point of policy enforcement because it may specify policy requirements (request parameters) for all requests passing through the gateway;
- TLS keys and certificates intended to authenticate and sign the request sent to the service may be installed in the gateway, instead of being installed in each subscriber's system that use the service;
- the two bullets above also apply to the process using XKMS, which means that it is possible to use the gateway together with the XKMS interface.

7.2 Web GUI Interface

As part of the Certum QESValidationQ service, a web GUI interface is available, directly for the validation service or through the Validation Gateway. Through the GUI, the user can send a document or certificate, select the request and response parameters, and then send the request to the service.

8 Risk analysis

The scope related to this chapter was addressed in the Main Policy in the chapter 5.4.8.

9 TSP (public) documentation applicability

Validation and preservation service policies and procedures are the same as for other qualified services provided by Certum and are described in the Main Policy.

The management of this document follows the same principles as described in the Main Policy.

Certum QESValidationQ validation and preservation service does not use services of external organizations.

9.1 Subscriber agreement

Certum QESValidationQ is provided on basis of the Subscriber agreement which include clause:

“By signing the agreement, the Ordering Party (Subscriber) declares that before signing it, it has read the regulations for the provision of the service and undertakes to apply to them.”

In each agreement, we indicate the representative of the Ordering Party (Subscriber) who is authorized to coordinate the performance of the contract, including access to the SubDO and preservation evidence, and right to request on the action related to the POs.

10 Information Security Policy

The scope related to this chapter is addressed in the Main Policy in the chapters 5.4.8, 6.6.2 and 9.8.1.1.

The applied security policy and personal data protection are included in the Information Security Policy, which is the part of the Integrated Management System implemented in Asseco Data Systems S.A.

The security policy documents the security and privacy controls implemented to protect personal data, in case Certum QESValidationQ has access to signed data, which can contain personal data.

Please be informed that Asseco Data Systems S.A. has the status of the personal data administrator in connection with the provision of the electronic signature validation and preservation service, due to the legal liability of the qualified trust service provider. Personal data is stored for the periods of limitation of claims resulting from generally applicable legal provisions.

11 Service management and operation

11.1 Internal organization

The scope related to this chapter is addressed in the Main Policy.

11.2 Human resource management

The scope related to this chapter is addressed in the Main Policy in the chapters 5.2 and 5.3.

11.3 Resource amangement

The scope related to this chapter is addressed in the Main Policy in the chapters 5.1, 5.4.8 and 9.3.

11.4 Access control

The scope related to this chapter is addressed in the Main Policy.

11.5 Cryptographic security

The scope related to this chapter is addressed in the Main Policy in the chapters 6.1 – 6.3.

The private signing key which is used for reports signing is held within cryptographic module which is a trustworthy system which is assured to EAL4 +.

11.6 Physical security

The scope related to this chapter is addressed in the Main Policy in the chapter 5, in particular in chapters 5.1 and 5.7.

The cryptographic libraries used comply with the requirement: ETSI TS 119 101, chapter 5.2, point GSM 1.4.

11.7 Operational security

The scope related to this chapter is addressed in the Main Policy.

11.8 Network security

The scope related to this chapter is addressed in the Main Policy in the chapters 6.7 and 5.1.2.

Additionally, the preservation service is integrated in the IT environment implemented in such a way that all storage access by the preservation client changing the content of the storage could only be done by the preservation service.

11.9 Security incidents management

The scope related to this chapter is addressed in the Main Policy in the chapters 5.4 and 5.5.

11.10 Event logging

The scope related to this chapter is addressed in the Main Policy.

The service records event logs for evidence purposes. Each validation operation is logged. Logs contain information about the exact time of the event. Event logs include the type of the event, the event success or failure, and an identifier of the component at the origin for such event.

11.11 Business Continuity Plan management

The scope related to this chapter is addressed in the Main Policy in the chapter 5.7.

11.12 Termination of service provision

The scope related to this chapter is addressed in the Main Policy in the chapters 5.8 and 9.2.1.

At the termination of the Certum QESValidationQ service, for 1 month it would be possible for the Subscriber to download the complete set of preserved data, after which the data will be irreversibly deleted.

11.13 Compliance and legal requirements

The scope related to this chapter is addressed in the Main Policy in the chapters 1, 1.3, 2.2, 8, 8.1.

If the validation process is based on the full signed data provided by the Service Subscriber, it is stored for the needs of the preservation service after the validation process is completed.

Annex A: Relationship with eIDAS

A.1 Validation of qualified signatures under eIDAS: Articles 26, 28 and 32

Requirements from Articles 32, 28 and 26 of eIDAS	Implementation according to the Certum QESValidationQ Service
Article 32: 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 EN 319 412-5 [ETSI 319 412-5] 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 described in chapter 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;	Indication of pseudonym used is included within Subject field of signing certificate [ETSI 319 412-2]. The signer certificate data are 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 correctnes of supported signature validation model described in chapter 4.1.
(h) the requirements provided 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 chapter 4.1.
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 EN 319 412-5 [ETSI 319 412-5] 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 is no additional checks beyond the requirements described 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 is no additional checks beyond the requirements described 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 119 102] if the certificate path validation returns a failure indication because the signature certificate has been temporarily suspended, the Certum QESValidationQ Service terminates validation and returns the indication INDETERMINATE, the sub-indication TRY_LATER, the date the signature was suspended and, if available, the content of the field nextUpdate of the CRL or OCSP-response will be 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 described in chapter 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 in such a way that any subsequent change of the data is detectable.	

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

Requirements from Article 38 and 40 of eIDAS	Implementation according to the Certum QESValidationQ Service
Article 38: 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 EN 319 412-5 [ETSI 319 412-5] 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 are no additional checks beyond the requirements described 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 are no additional checks beyond the requirements described 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: (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.	According to [ETSI 119 102] if the certificate path validation returns a failure indication because the seal certificate has been temporarily suspended, the Certum QESValidationQ Service terminates validation and returns the indication INDETERMINATE, with the sub-indication TRY_LATER, the date the seal was suspended and, if available, the content of the field nextUpdate of the CRL or OCSP-response will be used as the suggestion for when to try the validation again.
Article 40: 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.	

A.3 Qualified Preservation Service of qualified signatures and seals under eIDAS: Article 34

Requirements from Article 34 of eIDAS	Implementation according to the Certum QESValidationQ Service
Qualified preservation service for qualified electronic signatures	
A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.	Compliance with ETSI TS 119 511 V1.1.1 (2019-06) is assessed.

A.4 Qualified Validation Service of qualified signatures and seals under eIDAS: Article 33

Requirements from Article 33 of eIDAS	Implementation according to the Certum QESValidationQ Service
Qualified validation service for qualified electronic signatures	
1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:	
(a)provides validation in compliance with Article 32(1); and	Anex A.1
(b)allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	Described in 4.1.2

Annex B: Exceptions regarding validation of electronic signatures/ seals and certificates

B.1 Validation of qualified certificates issued before eIDAS

According to Article 51 of the eIDAS Regulation:

"**2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until they expire.**"

Certum QESValidationQ service assumes the following certificates to be valid.

Exception description	The legal acts allowing to accept an exception
polish qualified certificates issued before 01.07.2016	Directive 1999/93/EC and polish Act on Electronic Signature of 21.09.2001

Annex C: Testing procedures regarding validation of qualified electronic signatures/ seals

Certum QESValidationQ tests its service to demonstrate the correct implementation with regard to check whether the signature or seal is qualified.

The test cases include different use-cases, positive and negative ones.

In addition, we regularly participate in events organized by national and European institutions, which purpose is to create space for testing interoperability and provide test cases from different TSPs.

History

Document history		
1.0	03 of June 2016	Initial draft
1.1	1 August 2018	Change to the address of Asseco Data Systems S.A.
1.2	1 August 2019	Adding the Apendix B Adding information in 5.1.2 Table 4 about acceptance of non-qualified time-stamps
1.3	2020	Qualified Preservation Service added in chapters: 1, 4 and 5 New chapters: 5.3 and A.3
1.4	July 27th 2021	ADS address data update Detailed description of meeting the requirements in accordance with ETSI TS 119 441 and ETSI TS 119 511 New chapters: 1.1, 1.2, 8-11, Annex A.4, B, C
1.5	January 28th 2022	Updating the statuses in Table 2. Addition of information in Chapter 10 on the status of personal data adminitrator.