Public

SIGNATURE VALIDATION POLICY

AND SIGNATURE VALIDATION PRACTICE STATEMENT OF B-TRUST QUALIFIED VALIDATION SERVICE PROVIDED BY BORICA AD

(B-Trust QSVS)

Version 1.0

Effective:
July 1, 2018

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	20.05.2018	Approved	Initial release

CONTENTS

1 SCOPE AND USE

This document:

- Has been developed by "BORICA" AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- Is effective as of 01.07.2018;
- Specifies the policy and the security requirements on the provision of the service for qualified validation of qualified electronic signature and seal (referred to as SERVICE in this document) in accordance with the technical specifications EN 319 102-1 and ETSI TS 119 101 for this service operated by the Qualified Trusted Services Provider (QTSP) BORICA AD;
- Constitutes the General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA);
- Includes a description of the policy and practice in the provision of the SERVICE by the Provider and is a public document for the purpose of establishing compliance of the Provider's activity with the legal framework;
- Defines the practice of operating and managing the SERVICE to allow users and relying parties, who have a B-Trust Qualified Trusted Services Contract or have signed a Service Level Agreement to such a contract, to receive a description and evaluation the security of this qualified service;
- serves to evaluate the activity of the QTSP BORICA AD to provide qualified validation of qualified e-signatures/seals in accordance with Regulation 910/2014;
- defines the basic formats of e-signatures/seals to which the SERVICE is applicable;
- defines the protocols and interfaces of the SERVICE;
- defines the relations to "external" qualified services (e.g., CRL, OCSP, TSA) providing information to the SERVICE;
- addresses only the technical aspects of the validity of the signature/seal, but not the verification of their applicability (i.e. the legal feasibility) for different business purposes;
- May be changed by the QTSP and each new version of the document shall be published on the Provider’s website.

The following are outside the scope of the document:

- The legal feasibility (applicability rules) to different business purposes of the qualified electronic signature/seal; ETSI TS 119 172-1 can serve this purpose;
- Technical aspects of formats, syntax, e-signature/seal coding, and specific formats, profiles and coding of documents for signature/seal;
- The process of signing, i.e. generating a qualified e-signature/e-seal.

2 DEFINITIONS AND ABBREVIATIONS

2.1 Definitions

Validation – a complete process of verifying and confirming the validity of the e-signature/e-seal.

Signature/seal applicability – defining the legal applicability of the signature/seal to certain business purposes.

Driving application – an application/component that uses the signature/seal validation process to validate it.

Signature applicability rules – rules that define the (legal) applicability of the signature/seal for specific business purposes (for example, qualified signature/seal time, Holder/Creator identification, signature/seal qualification, validation report, etc.).

Qualified e-signature/e-seal/QES – according to Regulation 910/2014.

Advanced e-signature/e-seal with qualified certificate/AdES_QC – according to Regulation 910/2014.

Augmentation of e-signature – qualified e-signature/e-seal with data attached to it, allowing the validity of the e-signature/e-seal to be maintained over time (for example, profiles BASELINE_T, BASELINE_LT, and BASELINE_LTA).

Signature class – a set of signatures/seals to achieve a certain functionality (CAdES, XAdES, PAdES, ASiC).

Signature Level – a specific format defining a set of data included in the signature (BASELINE_B, BASELINE_T, BASELINE_LT, BASELINE_LTA), allowing the implementation of a particular class.

Enveloping signature - the signed document contains the signature, i.e. the signature is a sub-element in the signed document.

Enveloped signature – the signature contains the signed document, i.e. the document is a sub-element of the signature.

Detached signature - the signature and the document are in separate files.

Signature scheme – triad of: creation algorithm, verification algorithm, and algorithm for generating a pair of crypto switches.

Signature Validation Application/SVA – an application that validates the e-signature / e-seal in accordance with the Validation Policy that includes a set of constraints and which returns status and report of the validation.

Signature Validation Service/SVS – a system accessible through a network that validates an e-signature/e- seal.

Qualified Validation Service of Qualified e-signature/e-seal/QSVS – qualified validation in accordance with Regulation 910/2014 (Articles 32, 33 and 40).

Signature Validation Service Client/SVS Client – a software component of the SERVICE that implements the validation protocol at the user of the validation service.

Signature Validation Service Server/SVS Server – a component of the SERVICE at the QTSP that implements the validation protocol and performs the validation process.

Signature Validation Service Policy/SVS Policy – a set of e-signature/e-seal validation constraints that manages (is processed by) the validation module (SVA) – a Policy of the SERVICE Provider; a Policy is a technical concept and is limited by a specific set of constraints.

Signature Validation Service Report/SVS Report – report on the e-signature/e-seal validation process submitted to the "external" application or to the user for technical assessment of its applicability.

Signature Validation Service Practice Statement/SVS Practice Statement – the set of procedures for delivery/support of the validation service.

Validation constrain –technical criteria (functional requirement, value, range and result) against which the signature/seal is validated (according to EN 319 102-1).

Signature validation status – one of the following indications of the SERVICE – TOTAL-PASSED, TOTAL-FAILLED or INDETERMINATE.

Trusted List/TL – National Trusted List (or of a Member State)

List of Trusted Lists/LoTL – European List of Trusted Lists.

2.2 Abbreviations

QES/QESeal – Qualified Electronic Signature/Seal
QC – Qualified Certificate
AdES/AdESeal – Advanced Electronic Signature/Seal
AdES_QC - Advanced Electronic Signature with Qualified Certificate
AdESeal– Advanced Electronic Seal with Qualified Certificate
DA – Driving Application
OCSP (status) – Online certificate status
PKI – Public Key Infrastructure
SD – Signature document
SDO – Signed document
SVA – Signature Validation Application
SVI – Signature Validation Interface
SVP – Signature Validation Protocol
SVR – Signature Validation Request
QSVS/SVS – Qualified/ Signature Validation Service („SERVICE“)
SVS_Client – SERVICE Client
SVSP – Signature Validation Service Provider (QTSP BORICA AD)
SVS Policy – Signature Validation Service Policy
SVS Practice – Signature Validation Service Practice
SVS_Report – Signature Validation Service Report
SVS_Server – Signature Validation Service Server
TL – Trust List (national)
LoTL – List of Trusted Lists (European)
CPDP– Commission for Personal Data Protection

3 Concept

3.1 General requirements

The Qualified Signature/Seal Validation Service (the SERVICE) of the Qualified Trusted Services Provider BORICA AD (the Provider) uses the B-Trust® public key infrastructure that it operates.

The requirements and conditions contained in this document address the Provider's Policy and Practice regarding the SERVICE in the use of Qualified Electronic Signature/Seal (QES/QESeal) and/or Advanced Electronic Signature/Seal supported by a Qualified Certificate (AdES_QC/AdESeal_QC).

Regarding the general requirements of the Provider's policy and practice, the structure and content of the document conform to ETSI EN 319 401, including the specific requirements for Qualified Validation of QESQESeal and AdES/AdESeal.

Users (Relying Parties) should use this document to obtain an accurate description and assessment of the security of the SERVICE and the technical validity of the validated QES/QESeal and AdES/AdESeal_QC.

3.2 Policy and Practice

This document defines the common elements of the policy and practice of the Provider of the SERVICE in providing QTST in its capacity as general conditions and has the nature of general terms within the meaning of Art.16 of the Obligations and Contracts Act (OCA). These conditions are part of a written Trusted Services Agreement that is concluded between the Provider and the Users.

The Policy sets out the conditions and rules to which the Provider adheres, to implement the Practice when providing the SERVICE.

The Practice describes how the Provider implements the described Policy, and the procedures it follows when providing the SERVICE.

The Provider, through this SERVICE (B-Trust QSVS) validates a qualified e-signature/seal and/or advanced signature/seal accompanied by a qualified certificate from any interested party, subject to a common Validation Policy.

A rule in the Practice of the Provider of the SERVICE is to validate signature/seal with a format according to its Policy following the terms and procedures included in this document.

The Provider's Practice in the provision of the SERVICE is performed by a B-Trust object (B-Trust QSVS) identified by an object identifier 1.3.6.1.4.1.15862.1.6.6:

SERVICE for qualified validation of e-signature and e-seal (B-Trust QSVS)	**OID**
Practice of the SERVICE Provider	**1.3.6.1.4.1.15862.1.6.6**

In accordance with ETSI EN 319 441 and this document, the Provider's Practice implements a Common Policy on the Service with identifiers as follows:

SERVICE (B-Trust QSVS)	**OID(s)**
SERVICE Policy	**1.3.6.1.4.1.15862.1.6.6.1** **0.4.0.9441.1.1** **0.4.0.9441.1.2**

The identifier 0.4.0.9441.1.1 confirms compliance of the Validation Policy of the Provider in this document with ETSI TS 119 441.

The identifier 0.4.0.9441.1.2 confirms that the SERVICE is qualified.

The SERVICE does not validate to the User/Relying Party the applicability of the validated signature/seal, it only validates the technical validity of the signature/seal.

When a successfully validated signature/seal contains the Signature Policy identifier, the Relying Party can assess the applicability of the validated signature/seal to the specific business purpose after having become familiar with this common policy and the Signing Policy.

When the validation signature/seal does not include a Signature Policy identifier, the User/ Relying Party can assess the applicability of a successfully validated signature/seal following its Applicability Policy or by the indicated Certificate Policy.

In practice, the legal applicability of a validated signature/seal for a particular business purpose is entirely within the prerogatives of the User/Relying Party. The format and profile of the validated signature are indicated in the validation report, i.e. the functionality that is achieved with this signature/seal and, as a consequence, its relevance for a particular business purpose.

The SERVICE is paid by the User/Relying Party under contractual terms with the Provider for its delivery and use.

3.3 Management of the Provider's Policy and Practice

The Provider's Policy and Practice are subject to administrative management and supervision by the Board of Directors of BORICA AD.

Changes, modifications and additions are admissible, which do not affect the rights and obligations arising from this document and the standard contract between the Provider and the Users/Relying parties. They shall be reflected in the new version or revision of the document after approval and validation by the Board of Directors.

Each new version or edition of this document, submitted and approved, shall be immediately published on the Provider's website.

Any comments, inquiries and clarifications regarding this document may be addressed to:

• E-mail address of the Certification Authority: info@b-trust.org

• E-mail address of the Provider: info@borica.bg

• Tel.: 0700 199 10

3.4 Other Documents Related to the SERVICE

The Policy and Practice of the SERVICE Provider are rather technical documents and specify the technical aspects and features of validating e-signatures/e-seals. These documents are the Provider's property and specify:

- The Practice - how the Provider operates the SERVICE;
- Policy - the set of constraints against which the SERVICE determines the technical validity of the signature/seal.

While the SERVICE verifies the technical validity of the signature/seal, the Applicability Rules determine whether the signature/seal corresponds to a particular business purpose. The Service and the Applicability Rules are two independent processes:

- The SERVICE (Signature/Seal Validation Process) may end with a TOTAL-PASSED status but may not meet certain eligibility rules,

As well as

- The signature/seal may conform to certain Rules, but the SERVICE returns the INDETERMINATE or TOTAL-FAILED status indicator.

This requires documenting criteria regarding the business aspects of the e-signature/e-seal applicability and the legal aspects of their applicability.

There should be a Document for e-Signature/e-Seal Applicability Policy that define requirements developed in the context of Business Scoping Parameters (BSP), namely:

- Parameters referring to business applications that require e-signatures / seals;
- Parameters depending on legal/regulatory provisions related to the business objectives;
- Parameters related to participants in the processes of creating and validating e-signatures/e-seals;
- and other.

The rules on the legal applicability of the e-signature/seal for business purposes are outside the scope of this document, they should be prepared by Users/ Relying parties of e-signature/e-seal. These rules may be documented or prepared for automated verification (for example, based on the Validation Report) after using the SERVICE and prior to the final acceptance of the e-signature/e-seal by the Relying Party for the defined business purposes.

4 CONCEPTUAL MODEL OF THE VALIDATION PROCESS

4.1 Participants

The parties involved in the process of signature/seal validation are:

- A Provider as a QTSP that operates the validation process;
- Users (Relying parties);
- Indirect participants in the validation process:
  - Parties that have signed/sealed document(s);
  - External QTSP (their certifying authorities – CA, TSA, CRL/OCSP);
  - Trusted Lists of the Member States;
  - European List of Trusted Lists.

4.2 Formats and levels of compliance of QES/QESeal

THE COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 has defined the technical specifications and standards referring to the formats and levels of qualified or advanced e-signatures/e-seals, which each Member State of the Union should support (sign and validate) and which are accepted by the public authorities of the Member States in view of their cross-border interoperability and the required level of security for specific business purposes:

- XAdES Baseline Profile - ETSI TS 103 171 v.2.1.1 (2012) (or draft ETSI EN 319 132-1, 2015);
- CAdES Baseline Profile – ETSI TS 103 173 v.2.1.1 (20012) (or draft ETSI EN 319 122-1, 2015);
- PAdES Baseline Profile – ETSI TS 103 172 v. 2.1.1 (2012) (or draft ETSI EN 319 142-1, 2015).

The DECISION (art. 1 and , 3), in accordance with the Regulation 910/2014, approves the following advanced signatures/seals in CMS, XML, and PDF formats at B, T and LT levels of compliance, that should be recognized among Member States.

The DECISION (Articles 2 and 4) approves the conditions under which the validity of an advanced electronic signature/seal is confirmed:

(1) the certificate that supports the advanced electronic signature was valid at the time of signing, and when the advanced electronic signature is supported by a qualified certificate, the qualified certificate that supports the advanced electronic signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of Regulation (EU) No 910/2014 and that it was issued by a qualified trust service provider;

(2) the signature validation data corresponds to the data provided to the relying party;

(3) the unique set of data representing the signatory is correctly provided to the relying party;

(4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(5) when the advanced electronic signature is created by a qualified electronic signature creation device, the use of any such device is clearly indicated to the relying party;

(6) the integrity of the signed data has not been compromised;

(7) the requirements provided for in Article 36 of Regulation (EU) No 910/2014 were met at the time of signing;

(8) the system used for validating the advanced electronic signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues.

4.3 Validation model

4.3.1 General requirements

According to ETSI EN 319 102-1, the conceptual model of validation of QES/ QESeal or AdES_QC/AdESeal_QC, is presented in Fig. 1. The division in the model is conditional in order to better position the validation process to the general requirements.

Policy

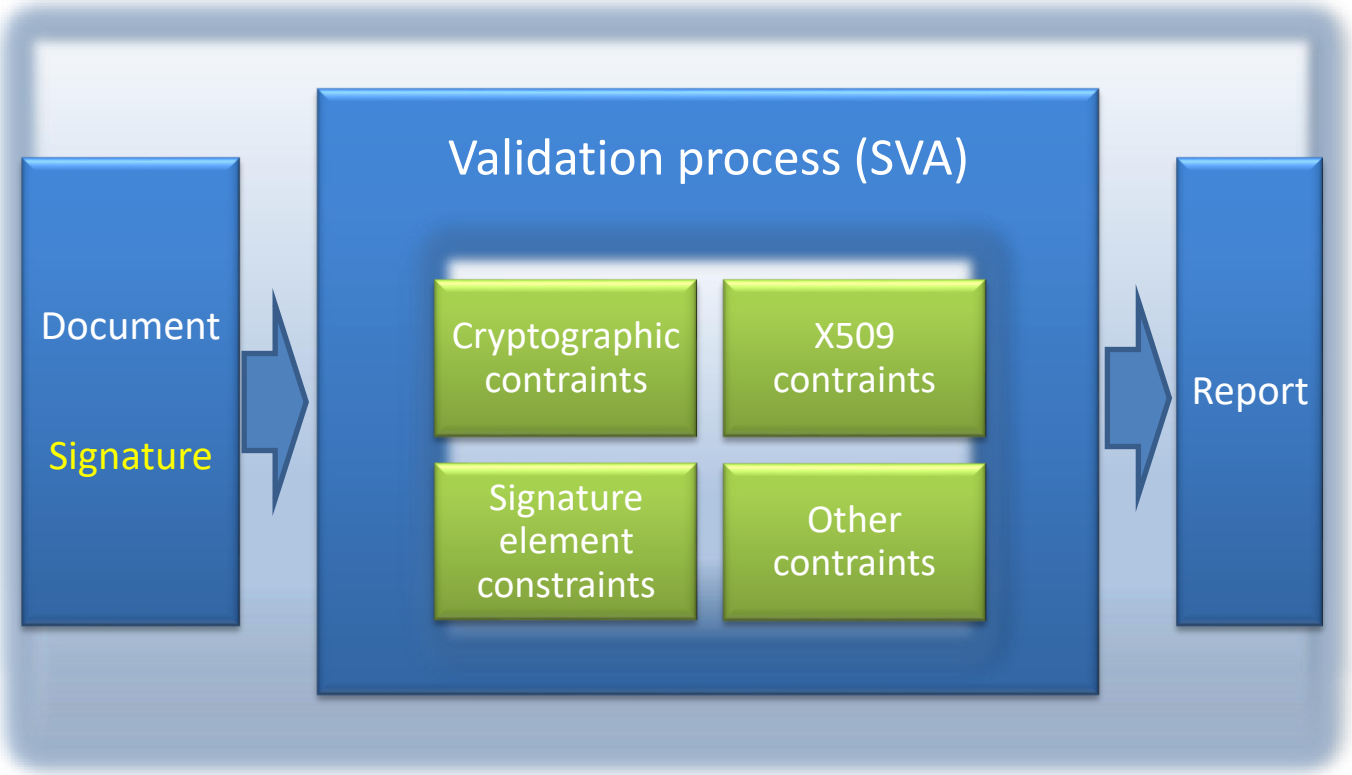


Figure 1 VALIDATION CONCEPTUAL MODEL

The SVA component in the model receives the signature/seal and, in accordance with the Validation Policy (Set of constraints), validates it and generates status-indicator and validation report that is interpreted by a User (Relying party) for the applicability of the signature/seal.

In order to validate a signature/seal format, several sub-processes are being executed within the SVA (validation process for a selected format/level): format checking, QC verification, cryptographic verification, etc. The status-indicator of each such single process is PASSED, FAILED or INDETERMINATE.

The status-indicator that SVA provides after validating the particular format/level according to the Validation Policy is:

- TOTAL-PASSED – the checks of all cryptographic characteristics/parameters of the signature/seal are successful, and those in accordance with the Policy (constraints); The User/Relying party accepts the signature/seal technically valid, but this does not mean that it is applicable to the particular business purpose;
- TOTAL-FAILED – the checks of all cryptographic characteristics/parameters of the signature/seal are unsuccessful or the signature/seal was created after revocation of the QC, or the format did not match one of the baseline formats specified in section 5.2; The User/Relying party accepts the signature/seal technically valid;

- INDETERMINATE – the results of individual/single checks do not allow the signature/seal to be evaluated as TOTAL-VALID or TOTAL-FAILED; the acceptance of the signature/seal is the prerogative of the User/Relying party.

To each level/format of e-signature/e-seal, the SVA performs a logical sequence of sub-processes that comprise the following validation processes:

- Validation Process for basic signature/seal format - BASELINE_B. The SVA performs this process if the time of validation is within the validity period of the QC and it is not revoked, or the time of validation is outside the validity period of the QC and the CA has provided information on its revocation/cancellation;
- Validation Process for basic signature/seal level BASELINE_T and BASELINE_LT – the SVA performs this process of basic signature validation of a signature/seal with certified time (_T) and of signature/seal with certified time and status of a QC (_LT);
- Validation Process for signature/seal level BASELINE_LTA – the SVA performs this process of basic signature validation of a signature/seal with certified time (_T), of signature/seal with certified time and status of a QC (_LT) and of a signature/seal with archival material (_LTA);

4.3.2 Selecting validation process

A User/Relying party cannot determine the validation process. THE SVA implicitly/imperatively follows the sequence of selection of the validation process:

(1) If the signature / seal for validation is:
- with BASELINE_B profile – the SVA shall perform (4)
- with BASELINE_T or BASELINE_LT profile – the SVA shall perform (3)
- with BASELINE_LTA profile – the SVA shall perform (2)

(2) If the SVA does not support signature/seal validation with BASELINE_LTA profile, the SVA shall perform (3); otherwise, the SVA shall perform a signature/seal validation process with BASELINE_LTA profile and shall go to (5);

(3) If the SVA does not support signature/seal validation with BASELINE_LTA, BASELINE_T and BASELINE_LT profiles, the SVA shall perform (4); otherwise, the SVA shall perform a signature/seal validation process with BASELINE_T and BASELINE_LT profile and shall go to (5);

(4) The SVA shall perform a basic format signature/seal validation process (BASELINE_B profile) and shall go to (5);

(5) When the validation status of the selected validation process is PASSED, the SVA shall return a status-indicator TOTAL-PASSED and a validation report;

(6) When the validation status of the selected validation process is FAILED, the SVA shall return a status-indicator TOTAL-FAILED and a validation report;

(7) In another case, the SVA shall return INDETERMINATE status-indicator and a validation report.

4.3.3 Validation status-indicators and validation report

The signature/seal validation process ends with:

- Validation status-indicator (TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE);
- Validation policy identifier (or description of constraints);
- Validation date and time and validation data (signature/seal certificate;
- The validation process selected (according to the signature / seal profile);
- Validation report.

The QTSP BORICA AD implements the conceptual model presented above for the e-signature/e-seal validation process by providing and maintaining a service for qualified validation of QES/QESeal and

AdES_QC AdESeal_QC (the SERVICE) in compliance with Regulation 910/2014, following the Practice and the Policy of the Provider contained in this document.

5 SERVICE (B-Trust QSVS)

5.1 Functional model

The SERVICE (B-Trust Qualified Signature Validation Service/B-Trust QSVS) of the Provider BORICA AD includes the following software components:

- Signature/seal validation client (SVS_Client) – the component is from the User side. It can be a web browser / web client with a graphical user interface (GUI) with the following functionality:
  - validation requests
  - validation protocol
  - provides the generated validation report.
- Validation server (SVS_Server) - Web service by the Provider with the following functionality:
  - validation protocol
  - SVA (signature/seal validation algorithms) according to ETSI EN 319 102-1
  - uses interfaces to internal and external/indirect participants/parties for the SERVICE - CRL/OCSP of Certification Authority(ies), TSA, TL/LTL
  - generates the report (summary or detailed) of the signature/seal validation.

Figure 2 presents the functional model of the SERVICE.

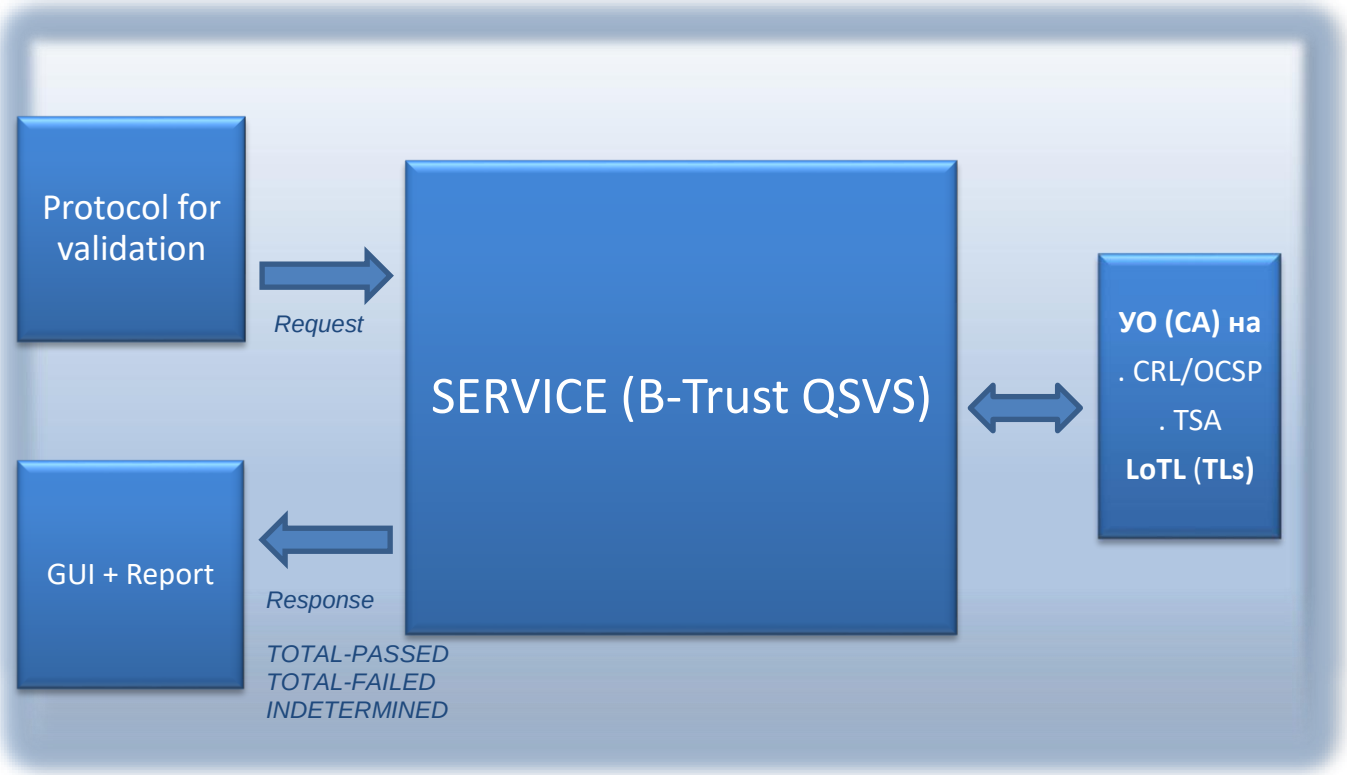


Fig. 2 Functional model of the SERVICE

5.2 Validation process

Signature/seal validation requests and responses to these requests use the communication channel between SVS_Client and SVS_Server. The exchange is protected by supporting server authentication and customer authentication can be maintained. The validation protocol (requests and responses) corresponds to ETSI EN 119 442.

In accordance with ETSI TS 319 172-1, the SERVICE performs the validation process in the following steps:

Step 1: The SVS_Client generates and sends a validation request containing the signed document (if the signature/seal is enveloped or enveloping) or sends the document and the signature (with a detached signature/seal);

The validation constraints are implicitly set by the SERVICE software (in SVS_Server) and the validation process executes them according to the format of the signature/seal delivered in the request.

Step 2: The SVS_Server performs signature/seal validation; the implementation of this step involves the use of additional internal trusted services of the Provider (B-Trust CRL/ OCSP, B-Trust QTSA) or, if necessary, of other external providers.

Step 3: The SVS_Server generates, prepares, and sends a validation report in response to a request for signature/seal validation; the detailed validation report contains the status-indicator (YES / NO) from the validation of each constraint and its effects depending on the selected validation process of the SERVICE, and follows the ETSI TS 119 102-2 technical specification; the validation report is sealed/certified by the SERVICE with a QESeal (BASELINE_LT profile). Validation report is generated for each signature/seal of the document.

Step 4: The validation report is submitted; the web-client visualizes the validation report in the appropriate format (in pdf format) and it can be printed. On the basis of the validation report, the User/Relying party accepts or rejects the technical validity of the signature/seal.

The service performs the following validation processes, depending on the profile of the submitted signature/seal:

- Validation process of signature/seal with a BASELINE_B profile;
- Validation process of time stamp;
- Validation process of signature/seal with BASELINE_T and BASELINE_LT profiles; this process is the same for both profiles;
- Validation process of signature/seal with a BASELINE_LTA profile.

The choice of the validation process of the SERVICE follows the instructions in section 5.3.2 of the conceptual model and the selected process performs the above steps, including basic functional procedures (sub-processes), which build up the logical sequence of checks in the framework of the validation process of the signature/seal.

5.3 Basic procedures (sub-processes)

A brief description of the constituent procedures (sub-processes) within the selected validation process for each format/profile supported by the SERVICE follows below.

5.3.1 Format Checking

If the signature/seal is in compliance with the applicable base format, the result of this verification is PASSED. Otherwise, the result of the verification is FAILED.

5.3.2 Identification of signing certificate

If the certificate is determined successfully, the outcome of this check is the signature/seal certificate. In the event that the signature certificate cannot be identified, the status-indication is INDETERMINATE with a NO_SIGNING_CERTIFICATE_FOUND sub-status.

This sub-process shall end with INDETERMINATE status only if the certificate is not contained in the signature/seal and cannot be retrieved from an external resource specified in the signature/seal reference number.

5.3.3 Validation context initialization

This sub-process initializes the validation constraints (implicitly set in the software) used to validate the signature/seal. In case of failed initialization, the sub-process ends with an INDETERMINATE status indication with a POLICY_PROCESSING_ERROR or SIGNATURE_POLICY_NOT_AVAILABLE sub-indication. Otherwise, the status indicator is PASSED with the set of constraints that are used during signature/seal validation.

5.3.4 Revocation freshness checker

Tis sub-process checks whether a status-indication of cancellation/revocation is current at the time of validation. The process is used by other sub-processes for verifying the revocation of the certificate.

5.3.5 X.509 certificate validation

This sub-process verifies the signature/seal certificate at the time of validation. Verification is performed at the current time for the SERVICE. Upon successful verification, the output of the sub-process is PASSED, otherwise - INDETERMINATE with a specified number of sub-indicators (YES / NO).

5.3.6 Cryptographic verification

Verifying the integrity of the signed data by performing cryptographic checks. Upon successful verification, the output of the sub-process is PASSED, otherwise – FAILED with a HASH_FAILURE or SIG_CRYPTO_FAILURE sub-indicators, or INDETERMINATE with a SIGNED_DATA_NOT_FOUND sub-indicator.

5.3.7 Signature/seal applicability

This sub-process includes an additional check, which is done on the signature/seal itself or on the signature/seal characteristics. Upon successful verification of the signature/seal for compliance with the established constraints, the outcome is PASSED, otherwise - INDETERMINATE with IG_CONSTRAINTS_FAILURE or CRYPTO_CONSTRAINTS_FAILURE_NO_POE sub-indicators.

5.3.8 Signature validation presentation

This sub-process presents to the User (Relying Party) the results of the overall validation process - the status-indication on the signature/seal validation - PASSED, FAILED, INDETERMINATE as well as the Validation Report.

5.4 Status-indications and validation report

The SERVICE ends with a status-indication as follows:

- PASSED – the cryptographic signature/seal checks (including all hash values) are successful, as well as all checks against constraints, implicit (direct) to the SERVICE (under this Policy);
- FAILED – the cryptographic signature/seal checks (including all hash values) failed or the signature/seal generation is after its certificate revocation or the signature/seal does not match one of the acceptable formats/profiles for the SERVICE;
- INDETERMINATE – the result of the check does not allow the SERVICE to certify that the signature/print is PASSED or FAILED.

The status indicator is accompanied by additional information contained in:

- A summary report on the validation process (requested via the "VERIFICATION" option of the SERVICE);
- A detailed report on the validation process (requested via the "DETAILED VERIFICATION" option of the SERVICE);

The summary validation report for each validated signature/seal includes:

- Validation policy (general description);
- Status-indication;
- Signature identifier;
- Date and time of creating the signature/seal;
- the validated signature/seal format/profile (i.e., the validation process selected);
- the Holder/Creator of the signature/seal;
- The scope of the signature/seal;
- Information on the signed/sealed document (name, number of signatures).

The detailed report includes full information to verify all constraints under the Policy on attribute/ characteristics of the objects in the signature/seal structure (according to its format/profile.

Both types of validation reports are provided through a web client in the User/ Relying Party browser in PDF format. Both reports are sealed/certified with a QESeal_QC of the SERVICE certifying their origin, intact data and time of sealing (i.e., validation time).

5.5 Interfaces and validation protocol

The Provider operates and supports the SERVICE as a web-service that is accessed through:

- OASIS DSS interface;
- GUI interface.

Both interfaces use a secure communication / transport channel supporting unilateral authentication of the server component of the SERVICE.

THE SERVICE is authenticated to the User/Relying party by means of a Qualified Certificate for website authentication issued on its server component (SVS_Server) by the CA of B-Trust of the QTSP BORICA AD.

5.5.1 OASIS DSS interface

The SVS_Client application accesses the SERVICE via OASIS DSS Interface that defines a set of XML commands for both protocols of the SERVICE:

- Protocol for document signing/sealing by a QES/QESeal;
- Protocol for validation of signed/sealed document.

Both protocols of the OASIS DSS interface use a SOAP transport protocol that transmits the XML-commands for signing/sealing, respectively for signature/seal validation.

5.5.2 GUI interface

The SERVICE is accessed/used by the User/Relying party by means of a web-based application that works with its browser and uses a graphical interface. Through it, the Relying party loads a file, chooses request parameters, loads a signed/sealed document for signature/seal validation, and then the web application in the browser sends a Request/Response XML to the server component of the SERVICE.

This interface uses a HTTP(S) POST transport protocol.

5.6 External sources of certificates

In certain cases, the SERVICE requires access to external sources of certificates related to the signature/seal validation process to a signed/ sealed document. Such external (indirect) participants in the validation process are:

- Certificate repositories maintained by other QTSPs - public registers, CRL/OCSP sources; time-stamping certifying authorities;
- National Trust List, External (Member States) Trust Lists (TL);
- List of Trusted Lists (LoTL).

THE SERVICE uses standardized software interfaces to access these external sources of qualified certificates, which verifies during the validation process of QES/QESeal and/ or AdES/AdESeal_QC.

The LoTL is published by the European Commission This XML file contains the Member States' Trusted Lists, including the national Trusted List. Information on who signs and publishes LoTL can be found at:
http://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52015XC1224(01)&from=EN.
The signature format of the LoTL and the national TL is XAdES BASELINE_B. The SERVICE relies to LoTL by verifying the signature through the certificate posted at the above address.

6 RISK ASSESSMENT

Taking into account found business and technical problems in the delivery, operation and maintenance of the SERVICE, the Provider shall carry out a risk assessment to identify, analyze and assess the related risks.

Relevant/appropriate measures to avoid identified risks are selected taking into account the results of the risk assessment. The measures adopted ensure a level of security equivalent to the degree of risks.

The Provider shall document through the Practice and Policy included as parts of this document the security requirements and operational procedures required to avoid identified risks for the SERVICE.

Periodic review and risk assessment shall be performed to address identified risk factors. The Provider's management approves the results of the risk assessment, the prescribed measures to overcome identified risk factors and accepts the established residual risk for the SERVICE.

See the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS).

7 PRACTICE STATEMENT

The B-Trust SERVICE procedures, control mechanisms and technical features contained herein are complementary to those parts of the "Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD" (B-Trust CPS-eIDAS) which regulate the general conditions, activities and procedures of BORICA AD as a QCSP for the provision of qualified trusted services.

This Practice is the basis of the Provider's operational work and corresponds to/serves the Policy contained in this document with the following identifiers:

SERVICE (B-Trust QSVS)	OID(s)
SERVICE Policy	**1.3.6.1.4.1.15862.1.6.6.1** **0.4.0.9441.1.1** **0.4.0.9441.1.2**

The Provider maintains this Policy under the following conditions:

- it is applied simultaneously for validation of QES/QESeal and AdES_QC/AdESeal_QC;
- it allows the User/Relying party to assess the applicability of the technically valid signature/seal for the particular business purpose;
- the current version is subject to change and the previous version is discontinued;
- the validation report indicates the policy;
- Previous versions are available to Users /Relying parties.

7.1 Service Certificates of the SERVICE

The SERVICE has two public certificates:

- Qualified certificate for qualified electronic seal;
- Qualified certificate for website authentication.

B-Trust QSVS e-seal certificate is a qualified certificate for e-seal and is electronically sealed with the private key of the B-Trust Operational Qualified CA of the Provider. With the private key of the SERVICE corresponding to the public key in this certificate, the Provider electronically seals the report (PDF format) of the signature/seal validation that is provided to the User/Relying party.

This certificate authenticates the SERVICE as the source of the generated report from the validation of an electronically signed/sealed document and validates the integrity of the data in the report from the validation process.

The B-Trust QSVS Web Site Certificate is an qualified website certificate and is electronically sealed with the private key of the B-Trust Operational Advanced CA of the Provider. This certificate online authenticates the site of the SERVICE to the User and serves a secure SSL / TLS session with the User.

The profile of the qualified certificate for qualified e-seal of the SERVICE is according to the document „Policy on the provision of qualified certificates for qualified electronic signature and qualified electronic seal of BORICA AD (B-Trust QCP-eIDAS QES/CQES/QESeal) and is specified below:

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	67 93 0c 9b 53 f1 2c 8b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256

Issuer	CN =	B-Trust Operational Qualified CA	
	OU =	B-Trust	
	O =	BORICA AD	
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426	
	C =	BG	
Validity from	-	2018-05-11T10:48:56Z	
Validity to	-	2024-05-11T10:48:56Z	
Subject	CN =	B-Trust Qualified Signature Validation Service	
	OU =	B-Trust	
	O =	BORICA AD	
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426	
	C =	BG	
Public key	-	RSA(2048 Bits)	
Subject Key Identifier		fd 1b 8e f2 76 d4 b1 ab b1 c1 94 62 be 84 c6 f7 ea cf a1 7b	
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0	
Issuer Alternative Name	URL=	http://www.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.3	
CRL Distribution Points	-	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCA.cer	
Key Usage(critical)	-	Digital Signature, Key Encipherment	
Enhanced Key Usage	-	Client Authentication, Secure Email	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (QcSSCD) (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en
Thumbprint (Sha1)		b4 f5 00 6c 27 8e fb ec 67 4b 44 b5 d4 3a 82 e6 31 a9 42 a3	
Thumbprint (Sha256)		da 4c 80 0c 0e 21 11 5f 85 e4 5c 51 22 f1 dd 7f b6 a8 40 5b	

		c9 be 48 8c 50 b0 54 c4 4d 47 46 44

The profile of the Qualified Certificate for Website authentication of the SERVICE is in accordance with the document "Policy on the provision of Qualified Certificates of Website authentication (B-Trust QCP-eIDAS Web SSL / TLS) of BORICA AD and is specified below

Field	Attributes	Value/meaning
Version	-	V3
Serial number	-	29 b9 2a 53
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2019-02-27T11:37:27Z
Validity to	-	2021-06-01T12:37:27Z
Subject	CN =	qsvs.b-trust.org
	O =	Borica AD
	2.5.4.97= (organizationIdentifier)	NTRBG-201230426
	OU=	OV SSL
	L=	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
SubjectAlternativeName		DNS Name=qsvs.b-trust.org RFC822 Name=support@borica.bg
Subject Key Identifier	-	b8 09 80 0c 5a 78 5e 48 ff 5a 08 cc ec 7f 87 fa 5d 98 4f 1e
Authority Key Identifier	KeyID =	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [3] Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Enhanced Key Usage	-	Server Authentication, Client Authentication
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalACA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

		Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/qsvs_pds_en.pdf language=en
Thumbprint (Sha1)		d9 0a 02 a2 87 40 87 93 a9 b2 68 38 87 3a d1 b9 0f 80 86 84	
Thumbprint (Sha256)		6b 1d f3 a6 71 5f 69 b2 cc 4f 95 69 c2 03 c9 7c 4f cb d8 07 b5 ae 52 47 62 4b 1f 95 a4 76 3d d2	

B-Trust uses the following algorithms for electronic signature/seal and data protection:

Name	**Algorithm**
Hash-algorithms:	SHA 256
Asymetric algorithms:	RSA

7.2 SERVICE operation and management

7.2.1 Internal organization at the Provider

BORICA AD, a registered QTSP within the meaning of Regulation 910/2014 and the Electronic Document and Electronic Trusted Services Act (EDETSA) is the Provider of the SERVICE. This Qualified Trusted Service operates and is maintained through the B-Trust® public key infrastructure, which is the Organizational Unit of the Provider. (Parts of) the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)“ regarding the internal organization of this infrastructure and the qualified trusted services provided through it are also applicable to the SERVICE.

7.2.2 Staff

The characteristics of the QTSP staff responsible for operating and maintaining the SERVICE and the assigned positions are in accordance with the document "Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)" (see section 5.2 and 5.3).

7.2.3 Asset Management

The asset management of B-Trust® infrastructure of the QTSP BORICA AD as specified the document "Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)", is applicable to the SERVICE.

7.2.4 Access management

All components requiring physical and logical protection against critical data and information (servers, communication equipment, keys, repositories archives, etc.) are segregated in rooms and areas with high security protection. The physical and logical control of access to the environment/infrastructure of B-Trust® of the QTSP is in accordance with the document "Certification Practice Statement for Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)" and is applicable to the SERVICE.

7.2.5 Cryptographic security - Key management

7.2.5.1 Key pair generation

The RSA key pair of the certificate to the SERVICE is generated in a software environment highly secure software environment PKCS # 12) by Provider's staff eligible to perform this role. The generated pair of RSA keys has a length of 2048 bits.

The description and role of this staff are set out in the document "Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)".

The environment for generating a key pair of the SERVICE is described in the same document.

7.2.5.2 Private Key protection

The generated private key for seal of the SERVICE is stored on HSM (QSCD).

The generated OV SSL private key of the SERVICE is stored in a PKCS # 12 cryptographic file protected by a secure password. In a special safe, a copy of the cryptographic file is stored for restoration purposes (server failure, deleting the key, etc.).

7.2.5.3 Public key distribution

The public key of the SERVICE for seal is certified by a qualified seal certificate issued by B-Trust Operational Qualified CA in the PKI hierarchy of B-Trust.

The public key of the SERVICE is certified by a website authentication certificate issued by B-Trust Operational Advanced CA in the PKI hierarchy of B-Trust.

This public keys certificate are loaded into the SERVICE platform and serve to:

- Seal the signature/seal validation report generated by the SERVICE;
- Authenticate the SERVICE (QSVS_Server) to Users/Relying parties who use it.

In addition, the Provider publishes the certificate of the SERVICE on its website. A User/Relying party can freely deliver it to his/her computer if necessary.

In order to authenticate the SERVICE, a User/Relying Party should have loaded on his/her computer/system the B-Trust Operational Qualified CA and B-Trust Operational Advanced CA (part of the B-Trust Trusted Servises, also posted on the Provider's website).

7.2.5.4 Certificate extension and/or renewal

The period of validity of the certificate of the SERVICE is 5 years. Upon expiration of this period, the validity of the certificate is extended for a period of 1 year. After this period, a new key pair is generated, the private key from which is stored in a HSM or respectively in a new cryptographic file PKCS#12, and the public keys are certified by issuing new certificates of the SERVICE. The key pairs with expired validity period are stored as follows:

- private key - stored for 10 years;
- public key - stored for 10 years.

7.2.6 Physical controls

The means and measures applied regarding the physical security of the B-Trust® Infrastructure of the Provider as specified in the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)“ (section 5.1.) are valid and applied for the SERVICE.

7.2.7 Operational Security

The operational security of the platform of the SERVICE complies with the requirements for the security of computer systems in the B-Trust infrastructure as specified in the document "Certification

Practice Statement for Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)" (sections 6.6, 6.7, 6.8).

7.2.8 Network security

Under section 6.9 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)“.

7.2.9 Incident management

According to the common security policy of the QTSP BORICA AD.

Under section 5.4 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)“.

7.2.10 Archiving

Under section 5.5 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS)“ .

7.2.11 Continuity

Under the general measures implemented by the Provider to ensure the continuity of the operation of the B-Trust infrastructure, including qualified certification services based on the reservation of the critical components of the infrastructure.

7.2.12 Termination of service

In the event of termination of the SERVICE, the relevant procedures under section 5.9 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS) “ are performed.

7.3 Information security

BORICA AD shall not publish a separate Information Security Policy for the SERVICE. The Provider operates, maintains and provides the SERVICE by using the common B-Trust® Public Key Infrastructure through which it provides Qualified Trusted Services (Qualified Signature/Seal Certificates and Qualified Time Stamps) under Reg. 910/2014.

The information security of the components of the B-Trust infrastructure is part of the common information security policy of BORICA AD, approved by the management of the company. This policy establishes the organizational measures and procedures for the security management of the systems and information assets through which services are provided. The staff having direct relations to these systems and assets is familiar with and implement this policy. See document „Certification Practice Statement for the Provision of Qualified Certificates and Trusted Services by BORICA AD (B-Trust CPS-eIDAS).

Documents signed/sealed by a QES/QESeal may contain information to be considered personal data In accordance with the legislation on such data, BORICA AD as a QTSP, respectively as Provider of the SERVICE, is registered by CPDP as a data controller.

8 POLICY

The Provider's policy on the SERVICE defines a set of constraints to the selected validation process for QES/QESeal and AdES_QC/AdESeal_QC.

The SERVICE follows Validation Policy by default, i.e. the validation constraints are implicitly defined in its software (configuration file, XML files).

8.1 General principles

(1) The Policy is common to QES/QESeal and AdES_QC/AdESeal_QC and sets the validation rules (constraints) of the formats/profiles admissible for the SERVICE.

(2) These rules apply also to the advanced electronic signatures/seals corresponding to Regulation 910/2014.

(3) The set of validation constraints is a combination of the common constraints for the SERVICE and the implicitly defined constraints by its base components, including:

- validation rules according to the standards/specifications for formats/profiles of supported signatures/seals;
- the validation rules according to the functional characteristics of the software (software libraries) of the SERVICE, i.e. the constraints imposed by the software (libraries) used.

(4) Qualified validation of AdES/AdESeal with a public certificate (unqualified) does not give a positive result of validation (the result is TOTAL-FAILED or INDETERMINATE).

8.2 Supported formats and levels for electronic signature/seal

In accordance with the implementation of Commission Implementing Decision (EU) 2015/1506 the SERVICE validates the following formats and profiles of QES/QESeal and AdES/AdESeal:

Format/Level	**BASELINE_B**	**BASELINE_T**	**BASELINE_LT**	**BASELINE_LTA**	**Comment**
CAdES	Validated	Validated	Validated	Validated	TS 103 173
XAdES	Validated	Validated	Validated	Validated	TS 103 171
PAdES	Validated	Validated	Validated	Validated	TS 103 172
ASiCS/ ASiCE (*)	Validated	Validated	Validated	Validated	TS 103 174

(*) The service validates this format and the compliance levels for it in addition to implementing the DECISION with regard to functional completeness.

Appendix 1 of the document presents the structures of the e-signatures/e-seal formats that the SERVICE validates.

8.3 Types of signatures/seals

For the formats and levels specified above, the SERVICE validates the following types of qualified signatures/seals according to their placement regarding the signed/sealed data:

Type	**CAdES**	**XAdES**	**PAdES**	**ASiCS**	**ASiCE**
Enveloped	NA(*)	Validates .xml format	Validates .pdf format	Validates .asics format	Validates .asice format
Enveloping	Validates .p7m format	Validates .xml format	NA(*)	Validates .asics format	Validates .asice format

Detached	Validates .p7s format	Validates .xml format	NA(*)	Validates .asics format	Validates .asice format

(*) Not applicable (NA)

8.4 Conditions for Validation of Qualified Signatures/Seals

In accordance with Art. 32 of Regulation 910/2014, the SERVICE confirms the validity of QES /QESeal and of AdES_QC/AdES_QC under the following conditions:

- the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature;
- the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- the signature validation data corresponds to the data provided to the relying party;
- the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- when the advanced electronic signature is created by a qualified electronic signature creation device, the use of any such device is clearly indicated to the relying party;
- the integrity of the signed data has not been compromised;
- the requirements provided for in Article 26 of Regulation (EU) No 910/2014 were met at the time of signing;

8.5 Validation constraints

Signature/seal validation constraints address the attributes and characteristics of the objects contained in the validated signature/seal structure that a User/Relying party submits to the SERVICE.

The following general sets of constraints are applicable to the SERVICE:

- On the certificates involved in the validation process;
- On the cryptographic characteristics of the signature/ seal;
- On the signature/ seal elements.

8.5.1 General Constraints

- The validation status-indication returned by the SERVICE determines only whether a signature is technically valid under the Validation Policy in this document. This Policy may not be appropriate for signatures / seals created in other territories (by Member States).
- The result of the SERVICE contains status-indicators from the validation of all signatures in the signature container (with a detached signature) or all signatures in the container of a signed document (with wrapped or wrapping signatures).
- Therefore, in the case of multiple segregated / packaged / packing signatures, the final result of the validation of a signed/sealed document with multiple signatures is not defined;
- Maximum size of signed/sealed data file - 10 Mbytes.

8.5.2 Constraints to formats

The SERVICE validates QES /QESeal and of AdES/AdES in the formats: XML (XAdES), CMS (CAdES) or PDF (PAdES), _B, _T or _LT profiles, which are supported by qualified certificates according to EC Decision 2015/1506. In addition, the SERVICE validates a versatile zip-format signature/seal container (ASiCS / E).

8.5.3 Constraints to profile and compatibility levels

Under section 4.2. of this document.

8.5.4 Constraints to the type of signature/seal

Under section 4.3. of this document.

8.5.5 Constraints to software (software library)

The service unconditionally fulfills the restrictions imposed by the underlying software library it uses:

- OASIS DSS.

8.5.6 X.509 Validation Constraints

THE SERVICE unconditionally supports the constraints implied by the X.509 v.3 qualified certificates for QES/QESeal and AES/AESeal in accordance with the technical standards of ETSI EN 319 412-1/5, and as follows:

- For qualified certificates for QES/QESeal:

Attribute in X.509 v.3 certificate	**Attribute value**
QES/QESeal – Natural/Legal Person	
Key Usage (critical)	*Non-Repudiation*
Qualified Statement:	
id-qcs-pkixQCSyntax- v2	*oid=1.3.6.1.5.5.7.11.2*
id-etsi-qcs-semanticsId-Natural or	*oid=0.4.0.194121.1.0*
(id-etsi-qcs-semanticsId-Legal)	*(oid=0.4.0.194121.1.2)*
id-etsi-qcs-QcCompliance (QcSSCD)	*oid=0.4.0.1862.1.4*
id-etsi-qcs-QcType	*oid=0.4.0.1862.1.6*
id-etsi-qct-esign or	*oid=0.4.0.1862.1.6.1*
(id-etsi-qct-eseal)	*(oid=0.4.0.1862.1.6.2)*

- For qualified certificates for AES/AESeal:

Attribute in X.509 v.3 certificate	**Attribute value**
AES/AESeal – Natural/Legal Person	
Key Usage (critical)	*Non-Repudiation*
Qualified Statement:	
id-qcs-pkixQCSyntax- v2	*oid=1.3.6.1.5.5.7.11.2*
id-etsi-qcs-semanticsId-Natural or	*oid=0.4.0.194121.1.0*
(id-etsi-qcs-semanticsId-Legal)	*(oid=0.4.0.194121.1.2)*
id-etsi-qcs-QcCompliance	*oid=0.4.0.1862.1.1*
id-etsi-qcs-QcType	*oid=0.4.0.1862.1.6*
id-etsi-qct-esign or	*oid=0.4.0.1862.1.6.1*
(id-etsi-qct-eseal)	*(oid=0.4.0.1862.1.6.2)*

8.5.7 Cryptographic Constraints

The cryptographic constraints of the SERVICE on cryptographic algorithms and hash function (according to ETSI TS 119 312) are as follows:

- Cryptographic algorithms for signing – RSA2048, RSA4096, ECC;

- Hash algorithm – SHA1, SHA256, SHA512.

In any case, the RSA key length must be at least 1024 bits, and the ECC key length must be at least 192 bits.

8.5.8 Signature Elements Constraints

None.

8.5.9 CA scope constraints

The signature/seal contains the signature/seal certificate with reference to the operational or base certificate of the CA required to build the verification path for the validation process. This applies to the Holder/Creator's Certificate and the QTSP Certificates that publish Certificate Status data (CRL/ OCSP), with reference to the validation process.

8.5.10 Certificate status constraints

The signature/seal validated by the SERVICE must contain proof confirming the validity of the certificate at the time of signing/sealing.

The status of the signature/seal certificate must be in the form of an OCSP-confirmation from the CA issued this certificate.

The validation process of the SERVICE does not require additional certificate revocation data other than data (OCSP status) originally included in the signature/seal.

Verification of revocation of certificates accepted as a basis of trust (for example, Operational or Base CA) is performed based on the TL/Trust Lists data.

8.5.11 Certificate validity constraints

For signature/seal with BASELINE_T or BASELINE_LT profile: Data freshness on revocation (i.e., OSCP-status of certificate) is verified according to the following rules:

- Revocation data (OCSP status) must be issued after the time of generating the time-stamp of the signature/ seal.

8.5.12 Trusted time constraints

The credible signing/sealing time (the closest time to the signature generation), which can be trusted (proven by the Proof-of-Existence in the signature) that the signature/seal existed, is thus determined:

- For a signature/seal with a time-stamp (BASELINE_T, BASELINE_LT or BASELINE_LTA) – this is the value in the genTime field of the earliest valid time stamp in the signature/seal;
- For basic signature (BASELINE_B profile) – Trusted / True time of signing/sealing cannot be determined because there is no Proof-of-Existence / POE for the signature / seal.

9 BUSINESS AND LEGAL ISSUES

As described in section 9 of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

10 COMPLIANCE WITH REGULATION (EU) N 910/2014 (Art. 32 and 33)

The Table below presents the B-Trust QSVS SERVICE for Qualified Validation of Electronic Signature/Seal (QES) and advanced electronic signature/seal with Qualified Certificates (AdES_QC/ AdESeal_QC):

Requirements in Art. 32	**Execution by the Service**	**Comments**
a) the signature supporting certificate at the moment of signing was a qualified certificate for an electronic signature	Validates QC profiles according to B-Trust Policies for QES/QESeal of the QTSP BORICA AD	ETSI EN 319 412-1/5
b) the qualified certificate has been issued by qualified trusted services provider and has been valid at the moment of signing	QC is verified following a verification chain that starts from a trusted source (CA) included in a national TL	DECISION 1505/2015 on TL
c) the signature validation data corresponds to the data provided by the relying party	The validation process provides the User/ Relying party with a report including the Holder/Creator's certificate containing the validation data (public key, etc.)	See the Validation Report in the DSS Guide
d) the unique set of data representing the signatory of the electronic signature in the certificate is duly handed to the relying party	see c)	See the Validation Report in the DSS Guide
e) if at the moment of signing a pseudonym has been used, this has been clearly indicated to the relying party	see c)	
f) the electronic signature has been created by a device for electronic signature creation	Mandatory constraint for QES/QESeal is the requirement to use QSSCD; for AdES/AdESeal this requirement is dropped.	Regulation / Annex II (QSSCD) B-Trust Policies for QES/QESeal of BORICA AD

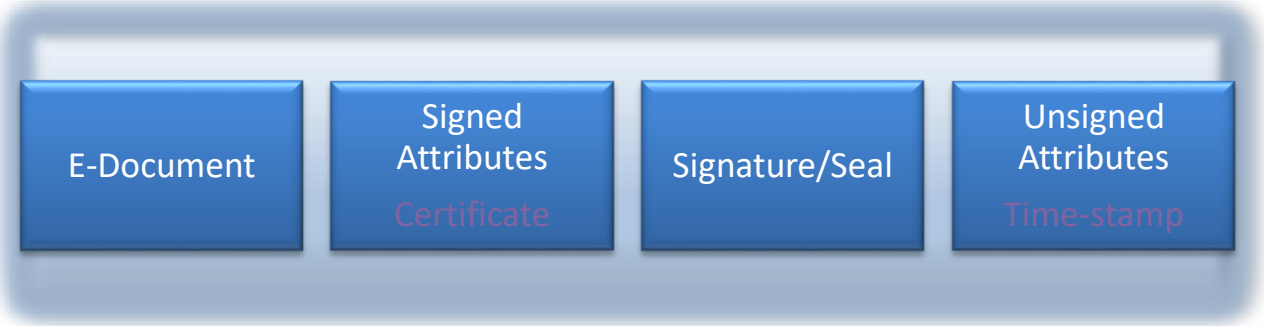
	The signature/seal certificate contains this requirement - see "Restrictions on the X.509 Certificate	ETSI EN 319 412-5
g) the integrity of the signed data is not compromised	The validation process compares the hash of the signature / seal with the data of the signed document	Feature of the digital signature and cryptographic algorithms used for signature / seal and for hash functions See "Cryptographic Limitations" ETSI TS 119-312
h) the requirements cited in art. 26 have been complied with at the moment of signing	The signature / seal validation process verifies the status and attributes of the certificate at the time of signature generation	For base BASELINE_B, this is uncertified time. For BASELINE_T, _LT, and _LTA accounts, it uses verified time (qualified time stamp).
Requirements in Art. 33	**Execution by the Service**	**Comment**
The Qualified Service for Electronic Signature Validation may only be provided by a Qualified Trusted Services Provider	BORICA AD is a QCSP in accordance with the Regulation 910/2014 and the EDETSA	http://www.crc.bg/files/_bg/Register_site_bg_30092017_Last_LAST.pdf
validation shall be carried out in accordance with Article 32 (1)	The SERVICE fulfills the requirements of Article 32 (1)	See "Compliance with Regulation 910/2014, Art. 32 "
enables trusted parties to obtain the result of the validation process in an automated way that is reliable and efficient and has an advanced electronic signature or advanced electronic seal to the Qualified Validation Service Provider	THE SERVICE provides to the User / Relying party a Validation Report as follows: • For a web client in the GUI with a graphical interface, a document in .pdf format; • For application / system with SOAP interface (Request / Response commands) automatic (program) mode of obtaining the validation result via this interface.	See Interfaces and protocols for validation

Appendix 1. E-Signature/E-Seal Profiles Validated by the SERVICE

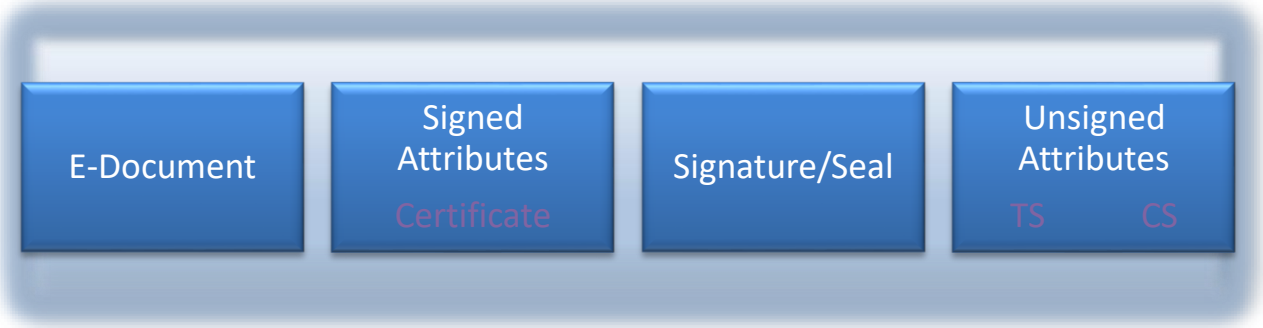
1. E-Signature/E-Seal common structure

2. **BASELINE_B** Profile

3. **BASELINE_T** Profile (with a time-certified signature/seal)



4. **BASELINE_LT** Profile (time-certified + certificate status)



5. **BASELINE_LTA** Profile (time + status + additional status + time)

TS – Time-Stamp

CS – Certificate Status

AVD – Additional Validation Data