Public

B-Trust Qualified Signature Validation Service (B-Trust QSVS)

B-TRUST® DISCLOSURE STATEMENT OF THE QUALIFIED TRUSTED SERVICE PROVIDER BORICA AD

Version 1.0

1 JULY 2018

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	18.04.2018	Approved	Initial release.

CONTENTS

This document is a Disclosure Statement/PDS of the Qualified Trusted Services Provider (QTSP) BORICA AD concerning the service for qualified validation of qualified electronic signatures and seals - B-Trust QSVS - eIDAS (in short, SERVICE).

This statement follows the structure of Annex A of the document ETSI TS 319-411-1, and is informative only for the Users of the SERVICE. This document does not substitute or replace the Policy and Practice Statement of the QCSP for the SERVICE, according to which qualified validation of qualified electronic signatures and seals is provided.

1 Contact Information

Any inquiries regarding this document can be addressed to:

Republic of Bulgaria
1612 Sofia, 41 “Tsar Boris III” Blvd.
Tel.: 0700 199 10
Fax: 02/ 981 45 18
E-mail: info@b-trust.org
Official web site of the Provider: www.b-trust.bg

2 Introduction

This document is a Disclosure Statement concerning the service for qualified validation of qualified electronic signatures and seals and of advanced electronic signatures and seals accompanied by qualified certificates B-Trust QSVS (in short, SERVICE) of the Qualified Trusted Services Provider (QCSP) BORICA AD.
The Disclosure Statement provides to users general information of the requirements of the SERVICE and is compliant with the requirements for this service contained in EU Regulation 910/2014.
The audit of the compliance assessment of the SERVICE has been performed by the independent auditor LSTI East Europe.

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

The SERVICE validates signatures/stamps with formats /profiles under the Provider’s Policy following the terms and procedures included in its Practice Statement for the service.

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)	Object Identifier
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 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 confirms compliance of the Validation Policy of the Provider with ETSI TS 119 441.

The identifier **0.4.0.9441.1.2** confirms that the SERVICE is qualified.

4 Formats and levels of compliance of signatures/seals

THE COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 has defined the technical specifications and standards referring to the formats and levels of qualified and 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.

5 Validation model

5.1 Validation process

The process of qualified validation of QES/ QESeal or AdES/AdESeal with a qualified certificate follows the validation model in accordance with ETSI EN 319 102-1.

The validation process receives an e-signature/e-seal, and in accordance with the Validation Policy (set of constraints), validates it by generating status-indicator and validation report interpreted by the User (Relying party) in respect to the applicability of the signature/seal.

In order to validate one of the specified in section 4 signature/seal format, several sub-processes are being executed within the SVA (validation process for a selected format/level): format checking, qualified certificate verification, cryptographic verification, etc. The status-indicator of each such single process is PASSED, FAILED or INDETERMINATE.

The status-indicator provided 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 for 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 4; *The User/Relying party accepts the signature/seal for* ***technically invalid****;*
- 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.*

5.2 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 SERVICE provided by the QCSP BORICA AD implements the model of validation process, specified in section 5.1, applicable to qualified validation of QES/ QESeal or AdES/AdESeal with a qualified certificate in compliance with Regulation 910/2014, following the Practice and the Policy of the Provider for this service.

6 SERVICE

The SERVICE uses exchange of requests/responses with the Users. The exchange is secured by supporting SERVICE (server) authentication and customer authentication can be supported. The validation protocol corresponds to the technical specification 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 User (browser interface or program) generates and sends a validation request containing the signed document or sends also the document.

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

Step 2: The SERVICE 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 SERVICE 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 or an AdESeal with a QC (BASELINE_LT profile). Validation report is generated for each signature/seal of the document.

Step 4: The validation report is submitted; the web-client submits/visualizes the validation report in the appropriate format that can be output/printed. Based on 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 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 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 with a QC (PAdES-BASELINE_ LT) of the SERVICE certifying their origin, intact data and time of sealing.

7 Usage

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 (if such document is available).

When the signature/seal for 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(s).

The rules on the legal applicability of the e-signature/seal for business purposes are outside the scope of validation, they should be prepared by Users/ Relying parties of e-signature/e-seal ad are their property. 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.

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

8 Rights and Obligations of Users

8.1 Liability of the User

The User's liability is determined by the Trusted Services Contract and its annexes (including the terms and conditions).

8.2 Obligations of the User

It is the responsibility of the User to act in accordance with the contractual terms and Policy and Practice of the Provider when using the SERVICE.

The User's obligations are determined by the terms and procedures of the Practice for the Qualified Service, the Trusted Services Contract and the standard terms and conditions thereof, which are an integral part of the General Policy of the Provider.

8.3 Rights of the User

The Users are entitled to use the SERVICE in accordance with the Provider's Policy and Practice for Qualified Validation of Signatures and Stamps.

8.4 Obligations to verify the legal applicability of a validated signature/seal

Under section 7 of this document.

9 Limited Warranty and Disclaimer/Limitation of Liability in providing the SERVICE

The QCSP BORICA AD declares and guarantees the following:

- the requirements and the operational procedures of the SERVICE are in compliance with the Providers Policy and Practice for it;
- to validate only the specified formats/profiles of signatures/seals;
- the Status-Indicators and Validation Reports issued by the Service correspond to the status of the signature/seal at the time of validation and not at the time of applying/use for a particular business purpose;

- complies with the requirements for confidentiality of information in a signed / stamped document/file;
- supports 24x7 availability of the SERVICE;
- Performs procedures for verification of certificates and time-stamps of external qualified Providers by using their authorities/sources (CRL/OCSP, TSA, TL_BG).

Borica AD shall not be liable in the case of:

- SERVICE unavailability due to natural disasters, war, telecommunications/energy disturbance, etc.;
- Illegal applicability of technically validated by the SERVICE signatures/seals for specific business purposes (applications).

10 Applicable Agreements, CPS, CP

The document SIGNATURE VALIDATION POLICY AND SIGNATURE VALIDATION PRACTICE STATEMENT OF B-TRUST QUALIFIED VALIDATION SERVICE PROVIDED BY BORICA AD can be found in the B-Trust repository of documents at https://www.b-trust.bg/documents.

Accordingly, Trusted Services Contract concerning Holders/Relying parties of the SERVICE can be found on the above B-Trust web address.

11 Privacy Policy/Statement

Borica AD fully complies with the Personal Data Protection Act and other applicable legislation of the Republic of Bulgaria.

Any information about Users that is not disclosed through the qualified certificates issued by B-Trust or the through the CRLs is considered personal information. All the information contained in the qualified certificates for signatures/seals validated through the SERVICE, CRLs, or provided by a publicly available service, shall not be considered confidential.

The SERVICE keeps all events relating to the signatures/seals validation process for a period of three months, after which this information is not stored.

12 Refund Policy

BORICA AD strives to provide the highest level of quality of the trusted services it offers and provides. Any User or Relying party may request revocation/termination of the service and refund, if the respective party is not satisfied with the SERVICE, but only if the Provider fails to fulfill its obligations defined in the User Contract and in this document.

13 Applicable Law, Complaints and Dispute Resolution

The operational activity of the Provider of the SERVICE follows the general rules set out in the Policy and Practice, and is in line with the applicable regulatory framework of the Republic of Bulgaria and applicable international acts. Disputes related to qualified services of BORICA AD shall be settled initially through a conciliation procedure. If the complaint is not settled within 30 days of the commencement of the conciliatory process, the parties may refer the dispute to the appropriate court. In the event of disputes and complaints arising from the use of a certificate or services provided by B-Trust, Users shall undertake to notify Borica AD of the cause of the dispute.

14 Conformity assessments, trust marks/logos, and audit

Audits to verify the conformity with procedural and legal provisions, particularly the conformity the document SIGNATURE VALIDATION POLICY AND SIGNATURE VALIDATION PRACTICE STATEMENT OF B-TRUST QUALIFIED VALIDATION SERVICE PROVIDED BY BORICA AD are performed every 24 months by an Authority for Conformity Assessment, based on Art. 20 of REGULATION 910/2014 EU (eIDAS).

15 Registration and identity verification points

B-Trust offices of the QCSP BORICA AD register and conclude Trusted Services Contracts. The list of B-Trust offices can be found on the B-Trust website at https://www.b-trust.bg/contacts.