# DISCLOSURE STATEMENT

# for B-TRUST® QUALIFIED LONG-TERM PRESERVATION SERVICE

# (B-Trust Qualified LTPS)

Version 1.0

June 1, 2018

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

# CONTENTS

This document is the Disclosure Statement of the Qualified Trust Service Provider (QTSP) BORICA AD concerning the Qualified Long-Term Preservation Service (hereinafter SERVICE) for Qualified Electronic Signatures and Seals (B-Trust Qualified LTPS – eIDAS).

This Disclosure Statement is based on the structure defined in Annex A of the document ETSI TS 319-411-1, and is for information purpose for the users of the SERVICE. This document does not substitute or replace the Policy and Practice Statement of the TSP for the SERVICE, according to which qualified long-term preservation of qualified electronic signatures and seals is provided.

# 1 Contact Information

BORICA AD
41 Tsar Boris III Blvd.
1612 Sofia
Bulgaria

Tel: +359 0700 199 10
E-mail: info@b-trust.org
Web: www.b-trust.bg

# 2 Introduction

This Disclosure Statement applies to the qualified long-term preservation service B-Trust Qualified LTPS (SERVICE) for qualified electronic signatures and seals, and for advanced electronic signatures and seals based on qualified certificates, operated by BORICA AD as a QTSP.

The Disclosure Statement provides to users general information of the terms and conditions of the SERVICE and is compliant with the requirements for this service contained in EU Regulation 910/2014.

The conformity assessment audit for the SERVICE has been carried out by the independent auditor LSTI East Europe.

# 3 General requirements

The qualified long-term preservation service (the SERVICE) for qualified electronic signatures and seals of the QTSP BORICA (the Provider) uses the B-Trust® Public Key Infrastructure operated by the Provider.

The Provider, through this SERVICE (B-Trust Qualified LTPS), provides long-term preservation of a qualified electronic signature/seal, and/or an advanced electronic signature/seal based on a qualified certificate, to any interested party, in compliance with a general Policy of long-term preservation of the signatures/seals.

The SERVICE preserves signatures/seals with formats/profiles under the Provider's Policy following the terms and procedures included in the Provider's Practice Statement for the SERVICE.

The Provider's Practice Statement for the SERVICE is implemented by a B-Trust object (B-Trust Qualified LTPS) identified by an object identifier 1.3.6.1.4.1.15862.1.6.7:

| | |
|---|---|
| Long-term preservation service for qualified electronic signatures/seals (B-Trust Qualified LTPS) | OID |
| Practice Statement of the Provider | **1.3.6.1.4.1.15862.1.6.7** |

The Practice Statement of the Provider complies with a Policy for the SERVICE identified as follows:

| | |
|---|---|
| SERVICE (B-Trust Qualified LTPS) | OID |
| SERVICE Policy | **1.3.6.1.4.1.15862.1.6.7.1** |

The SERVICE **does not** verify to the User/Relying Party the feasibility of the long-term preserved valid signature/seal, **it only verifies the long-term technical validity of the signature/seal**.

If a preserved successfully validated signature/seal contains a Signature Policy OID, the Relying Party can estimate the feasibility of this signature/seal for the specific business purpose after having become acquainted with the general SERVICE Policy and the Signature Policy (if available).

If a preserved valid signature/seal does not include a Signature Policy OID, the User/ Relying Party can estimate the feasibility of this signature/seal following their own rules/conditions or by the indicated Certificate Policy.

Actually, the legal feasibility of a preserved valid signature/seal for a particular business purpose is entirely within the prerogatives of the User/Relying Party. The necessary information related to the applicability of the signature/seal (format, profile, certificates, Provider, validity, etc.) and hence its relevance for a particular business purpose, is contained in the preservation evidence.

## 4 Formats and levels 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.

BORICA as a QTSP provides and supports B-Trust QSVS-eIDAS qualified service for qualified/advanced e-signature/e-seal validation in accordance with Regulation (EU) No 910/2014 and meeting the requirements (Art. 1-4) of the abovementioned DECISION. In addition, B-Trust QSVS-eIDAS validates formats of the specified signatures/seals at LTA level of compliance, as well as signature/seal with ASiC-S/E profile.

Pursuant to the abovementioned IMPLEMENTATION DECISION and based on the B-Trust QSVS – eIDAS service, BORICA provides the Long-Term Preservation Service to the B-Trust Users.

# 5 Long-term preservation model

## 5.1 Mechanism and scheme

Following the general normative established technical specifications for long-term preservation of signatures/seals (RFCs or TS) of the IETF or the ETSI, BORICA has implemented in the SERVICE **a scheme for long-term preservation based on preservation of signatures/seals via AdES (Advanced Electronic Signature) augmentation.**

An e-document with AdES digital signature is submitted to the SERVICE. If the signature is detached, the originally signed document is also needed or at least the hash for the respective hash algorithm (if there is a requirement for confidentiality of the document). If the signature/seal is basic (B level), the SERVICE adds a time stamp to it. The SERVICE then validates the signature (via internal or external process) by including the missing validation material (_LT level).

Note: If the signature is already augmented (_LTA level), the SERVICE validates and augments only the latest time stamp.

According to the format/level of the signature/seal, after adding the missing validation material to the signature/seal, the SERVICE computes the hash of the originally signed/sealed document and of the augmented signature/seal, generates a time stamp for these hashes and adds it to the e-document (signature/seal).

## 5.2 Validation

Validation within the scope of the SERVICE is a process to check the validity of digital signatures of e-documents and of time stamps before preservation.

The SERVICE shall use an internal validation process or an external qualified validation service to check the validity status of a signature/seal before storing an e-document(s) in the storage container.

BORICA as a QTSP provides and supports a qualified service for QES/QESeal validation in accordance with the Regulation (EU) No 910/2014. See the document “Signature Validation Policy and Signature Validation Practice statement of the B-Trust Qualified Validation Service” (B-Trust QSVS-eIDAS).

In order to verify the validity of time stamps to e-documents (signatures and seals) subject to preservation, the SERVICE can use an internal and/or an external process (a qualified time-stamping service). The validity verification of time stamps is direct (independent) and does not require mandatory use of the qualified time-stamping service. The Provider’s B-Trust QTSA-eIDAS qualified time-stamping service can also be used for the verification of the time-stamps.

## 5.3 Archive/Storage

The Archive is a specialized database for storage and management/maintenance of containers for long-term preservation of digital objects (e-documents, evidence).

BORICA provides the SERVICE to Users/Subscribers with integrated Archive for storage of e-documents and evidence materials for the goals of preservation.

## 5.4 Long-term preservation goals

The SERVICE supports the following goals for long-term preservation:

- Proof of integrity of an e-document (signature/seal);
- Proof of existence (at a time/in the past) of an e-document (signature/seal);
- Maintenance of the validity status of e-signatures/seals (e-documents) over long periods of time.

## 5.5 Evidence regarding the long-term preservation goals

The SERVICE supports and provides the following evidence regarding the long-term preservation goals:

- Evidence of integrity of an e-document (signature/seal);
- Evidence of existence (at a time/in the past) of an e-document (signature/seal);
- Evidence of the validity status of signatures/seals (e-documents).

This evidence is based on the implemented long-term preservation scheme, through which evidence material is collected, enhanced and stored together with initially signed/sealed e-documents/files in the Archive of the SERVICE.

## 5.6 Policy and Practice Statement Administration

The Policy and the Practice Statement of the Provider are subject to administrative management and control by the Board of Directors of BORICA.

Changes, modifications and additions are admissible, which do not affect the rights and obligations arising from this document and the standard service agreement between the Provider and 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.

The current Policy and Practice Statement shall be reviewed at least annually in order to reflect potential requirements and prerequisites for changes in security levels of algorithms, formats and profiles of signatures/seals. Each submitted and approved new version of this document shall be immediately published on the website of the Provider.

The Provider’s Policy and Practice Statement for the SERVICE should be used together with the following documents for qualified services of BORICA:

- B-Trust CPS-eIDAS;
- B-Trust CP-eIDAS;
- B-Trust QSVS-eIDAS.

# 6 Long-Term Preservation SERVICE

The main task of the SERVICE is long-term preservation of the validity of the electronic signature or

seal on the electronic document/file (e-document). In this respect and in accordance with the Policy, the SERVICE does not accept preservation of digital objects (documents and files) without signature/seal.

## 6.1 Basic Procedures

### 6.1.1 Upload of e-document

1. The SERVICE uploads e-documents, which have to be archived, only after identification of the Subscriber/Submitter within a secure session/procedure. The secure session (SSL/TLS) ensures the integrity and confidentiality of the uploaded e-documents.

2. The Policy and the Practice Statement inform the Subscriber/Submitter of the file formats of signature/seal on e-document accepted by the SERVICE, how the electronic signatures and seals are validated and which are the conditions for uploading e-documents.

3. The validity of electronic signature(s) or seal(s) of the e-document received by the SERVICE is validated through the complete long-term validation material. The validation may be based on a partial or the complete long-term validation material, attached to an electronic signature or seal. Any information still necessary for the validation and for a long-term evidence material is collected from internal or external sources, and is kept with the document. After compiling the long-term validation material, the SERVICE provides a qualified time stamp to the long-term validation material.

4. The SERVICE stores an uploaded e-document encrypted. The encryption ensures that unauthorized staff cannot detect the contents of the e-document. Deciphering of the encrypted e-document is done only in cases related to procedures such as download, regulation (on the side of the National Regulator) or re-encryption (for already weak crypto-algorithm).

5. The Provider (the SERVICE) verifies the received e-documents as soon as possible, but not later than 3 days from the receipt, and sends an acknowledgement to the Subscriber that the long-term validation material (proof of validity of a signature/seal) has been successfully completed, and the SERVICE has accepted the e-document. If the process of compiling the evidence material fails, the Provider (the SERVICE) notifies the Subscriber via error message. Based on the error message, the document and the reason for rejection should be clearly established.

6. If the verification for acceptance of the e-document is not confirmed to the Subscriber within the specified term, it is assumed that the Provider (the SERVICE) has not accepted the electronic document. The Provider is responsible for storing the e-document and for ensuring long-term validity of the included signatures/seals after sending a positive confirmation for acceptance of the e-document for preservation.

### 6.1.2 E-Document Download

The Provider, via the SERVICE, ensures that the Subscriber can download his documents stored in the Archive and the respective materials for long-term validation (evidence material) during the period of the Service Agreement.

1. The Subscriber has access to e-documents and to long-term validation materials (evidence), only through a secure channel.

2. The SERVICE ensures that each Subscriber has access only to e-documents and long-term validation materials, which he is actually authorized to access.

### 6.1.3 Issuance of Acknowledgement (ACK) for a preserved e-document

At the request of the Subscriber, the SERVICE issues an acknowledgement in relation with a

preserved e-document. The acknowledgement includes:

1. A statement that the advanced or qualified electronic signatures, seals, time-stamps on the relevant e-documents, and the respective certificates, have been valid at the time of certifying by the SERVICE with a time stamp, and upon validation after their acceptance into the Archive

2. Hash of the e-document, name and identifier of the Subscriber.

3. A statement that an e-document has a specified hash, so it is identical to the e-document with the same hash submitted by the Subscriber.

4. The time of the acceptance of the e-document into the Archive.

The SERVICE issues the acknowledgement as an e-document with a qualified electronic signature or on paper. The acknowledgement is created by an official responsible for issuing Acknowledgements of the Storage who, in case of an electronic Acknowledgement, applies his/her qualified electronic signature and qualified electronic time stamp; in case of issuing the Acknowledgement on paper, he/she certifies it with his/her handwritten signature.

An authorized representative of the Subscriber may request issuance of Acknowledgement, if he/she presents a notarized power of attorney.

### 6.1.4 Display of a preserved e-document

The SERVICE provides the Subscriber with the opportunity to view their e-documents preserved in the storage on a predetermined date and location.

### 6.1.5 Deletion of a preserved e-document

The SERVICE provides at the request of the Subscriber selective deletion of e-documents and all corresponding long-term validation materials (evidence) preserved in the Archive. Deletion means physical erasure of a preserved e-document in a way it cannot be restored later (or only with unreasonably high financial costs). The deletion is performed on the entire system of the Provider by deleting any saved copy of the e-document.

## 6.2 Termination of the Service Agreement

Upon termination of the Agreement for the SERVICE, the Provider shall provide the e-documents and long-term validation materials, which the Subscriber has ordered to be preserved, to be downloaded by the Subscriber or by another authorized person. After termination the Provider shall delete the documents and the long-term validation material of the Subscriber.

# 7 Usage

See Section 4 and section 5 of this document.

# 8 Rights and Obligations of Users and Relying Parties

## 8.1 User Responsibility

The responsibility of the User is set by the Service Agreement and its appendixes (including the terms and conditions).

## 8.2 User Obligations

The obligation of the User is to act in accordance with the contractual terms and the Policy and

Practice Statement of the Provider while using the SERVICE.

The obligations of the User are determined by the terms and procedures of the Practice Statement for this qualified SERVICE, the service agreement and its standard conditions that are an integral part of the common Policy of the Provider.

### 8.3 User Rights

Users have the right to use the SERVICE in accordance with the Policy and Practice Statement of the Provider for the Qualified Long-Term Preservation Service.

### 8.4 Relying Party Responsibility

The Relying Parties decide based on their discretion and/or their policies about the way of accepting and using the preserved signatures and seals. During the verification of the validity for keeping the security level guaranteed by the SERVICE it is necessary for the Relying Party to act with caution, so it is recommended to:

- Assess the conformity with the Policy and Practice Statement of the Provider for the SERVICE;
- use reliable IT environment and applications;
- verify the current CRL or OCSP response;
- take into consideration every restriction in relation to the usage of the signature seal that is included in the Policy and Practice Statement for the SERVICE.

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

BORICA as a QTSP declares and guarantees the following:

- the requirements and the operational procedures of the SERVICE are in compliance with the respective Provider's Policy and Practice Statement;
- only the specified formats/profiles of signatures/seals are preserved;
- the evidence validation material 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;
- compliance with the requirements for confidentiality of information in a signed/sealed document/file;
- 24x7 service availability;
- verification of certificates and time stamps (currently) only of B-Trust signatures/seals.

The service has national scope only to B-Trust clients.

The Provider may extend the customer scope of the SERVICE on the territory of the country also for customers of other QTSPs registered by the National Regulator (CRC) and operating in the country on the basis of bilateral agreements. In this case, the SERVICE will apply the same strict requirements that apply to the B-Trust domain.

BORICA shall not take responsibility for:

- 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, Policy and Practice Statement

The document POLICY AND PRACTICE STATEMENT FOR B-TRUST® QUALIFIED LONG-TERM PRESERVATION SERVICE can be found in the B-Trust repository of documents at https://www.b-trust.bg/documents.

A Certification Service Agreement concerning Users/Relying parties of the SERVICE can also be found on the above B-Trust web address.

## 11 Privacy Policy/Statement

BORICA 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 strives to provide the highest level of quality of the certification 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 Service Agreement 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 Statement, 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 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 the SERVICE, Users shall undertake to notify BORICA of the cause of the dispute.

## 14 Conformity assessments, trust marks/logos, and audit

Audits to verify conformity with procedural and legal provisions, and especially conformity with the document POLICY AND PRACTICE STATEMENT FOR B-TRUST® QUALIFIED LONG-TERM PRESERVATION SERVICE, are performed every 24 months by an Authority for Conformity Assessment, based on Art. 20 of REGULATION 910/2014 EU (eIDAS).

## 15 Subscription details

B-Trust offices of BORICA perform registration and conclude Service Agreements for trust services. The list of B-Trust offices of BORICA is published on the B-Trust website at: https://www.b-trust.bg/contacts.