POLICY AND PRACTICE STATEMENT

for B-TRUST® QUALIFIED LONG-TERM PRESERVATION SERVICE

(B-Trust Qualified LTPS)

Version 1.0

Date of Effect: June 1, 2018

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	18.04.2017	Approved	Initial release

CONTENTS

1 SCOPE AND APPLICABILITY

The present document:

- Has been drawn up by BORICA AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- Is effective as of 01.06.2018;
- Specifies the policy and the security requirements on the provision of the service for qualified long-term preservation of qualified electronic signatures and seals (hereinafter: SERVICE) operated by BORICA as a Qualified Trust Service Provider (QTSP), in accordance with the Regulation 910/2014 of the European Parliament and of the Council;
- Has the nature of general terms under Art. 33, para. 2 of the Ordinance on the Activities of Trust Service Providers and within the meaning of Art. 16 of the Obligations and Contracts Act;
- Includes a description of the policy and practice in the provision of the SERVICE by the Provider and is a public document with the purpose to ascertain the compliance of the Provider's operation with the legal framework;
- Defines the practice for operating and managing the SERVICE to provide users and relying parties, who have concluded a B-Trust Qualified Trust Service Agreement and have signed a Service Level Agreement, with description and security assessment of this qualified service;
- Serves to assess the operation of BORICA as a QTSP related to the provision of qualified preservation of qualified e-signatures/seals in accordance with Regulation 910/2014;
- Defines the basic formats of signatures/seals, to which the SERVICE is applicable;
- Defines the mechanisms and the scheme for storing qualified signatures and seals of the SERVICE;
- Defines the relations/links to "external" trusted/qualified services (e.g., CRL, OCSP, TSA) providing information to the SERVICE;
- Addresses only the technical aspects of long-term preservation of the validity of e-signatures/e-seals but not their applicability (i.e., legal feasibility) for different business purposes;
- May be amended by the QTSP and each new revision of this Policy and Practice Statement shall be published on the Provider's website by repealing the previous version of this document.

Outside the scope of the document are:

- The legal feasibility (applicability rules) of the long-time preserved qualified electronic signatures/seals to different business purposes;
- Technical aspects of formats, syntax, e-signature/seal coding, and specific formats, profiles and coding of documents for signature/seal;
- The process of signing/sealing, i.e. generating qualified e-signatures/e-seals, which are subject to this SERVICE.

2 COMPLIANCE AND REFERENCES

The present document has been prepared in accordance with:

- Regulation (EU) № 910/2014 of the European Parliament and of the Council on certification services and refers to information on international recommendations, specifications and standards prepared in accordance with this Regulation;
- Electronic Document And Electronic Certification Services Act (EDECSA);
- Ordinance on the Activities of Certification-Service-Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services;

- The document should be used together with the general documents B-Trust CPS-eIDAS (Provider's Practice Statement) and B-Trust CP-eIDAS (Provider's Policy) when auditing the SERVICE to establish compliance of the Provider's operation with the regulatory framework.

The contents and structure of this document is based on the following ratified international specifications:

- ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI) Data Preservation Systems Security; Part 1: Requirements for Implementation and Management";
- ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI) Data Preservation Systems Security; Part 2: Guidelines for Assessors";
- ETSI SR 019 510 V1.1.1 (2017-05) Electronic Signatures and Infrastructures (ESI) Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures.

The following documents (technical specifications) are not directly related to this document but may be of assistance to users:

- ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part1: Creation and Validation;
- ETSI TS 119 102-2: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- ETSI TS 119 101: Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for applications for signature creation and signature validation;
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services";
- ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures";
- ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures";
- ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures;
- ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures;
- ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures;
- ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles;
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers;
- ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI);
- Associated Signature Containers (ASiC); Part 2: Additional ASiC containers;
- RFC 6970 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP.

Any information related to the present document may be obtained from the Provider at:

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

3 DEFINITIONS AND ACRONYMS

3.1 Definitions

SERVICE (Preservation Service) – a qualified service for long-term preservation of qualified electronic signatures/seals in accordance with Regulation (EU) № 910/2014

Preservation – a function that supports a data object in a proper and independently understandable form, possibly over extended periods of time

Long term – long enough time for storage, related to the time of possible technological changes (in crypto algorithms, key size, hash functions) or of storage technology

Preservation goal – one of the following objectives achieved during the preservation period: proof of integrity, proof of existence, availability, maintenance of validity status of a digital signature/seal or time assertion, confidentiality, authenticity of the submitter, identification of the DPS

E-document – an electronic document that contains at least one eIDAS Regulation conformant electronic signature or seal. Depending on the type of the e-document it may contain additional electronic documents and the corresponding profiles (metadata), signatures, countersignatures and time stamps

Container – data structure, which contains e-signature(s)/e-seal(s) and related metadata; the metadata can comprise associated signatures, seals, time stamps, evidence records, validation data (CRLs, OCSP responses) and validation reports as well as other metadata specific to long-term preservation.

Archive – database for storing data objects in storage containers with specific purpose(s) and related components (computer systems, communication links, power supply, physical and fire protection and security systems and their redundancy)

Client – A person or organization signing the service agreement with the Provider in order to use the SERVICE

Submitter – a person who sends e-documents to the SERVICE, who may be different from the Subscriber, but has (access) rights to use the SERVICE

Evidence record – unit of data, which can be used to prove the existence of a data object or data object group at a certain time

Preservation evidence – data that can be used to demonstrate that the various preservation goals (e.g. proof of integrity or proof of existence) are met for the preserved data objects

Preservation mechanism – a mechanism used for storing e-document(s)

Preservation scheme – preservation mechanism(s) used to achieve specific goal(s) in signature/seal preservation

Long-term Preservation Policy/LTPP – a set of rules, applicable to the SERVICE that define the mechanisms (preservation scheme) and the internal processes applied to achieve the preservation goals

Preservation period – duration specified in the service agreement

Proof of existence – the existence of an e-document (signature/seal) at a specific (past) time (e.g. a qualified time-stamp)

Proof of integrity – maintenance of the integrity and completeness (hash, signature/seal)

Proof of validity – maintenance of the validity status of a signature/seal

3.2 ACRONYMS

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

OCSP – Online Certificate Status Protocol

PKI – Public Key Infrastructure

LTPP – Long-Term Preservation Policy

LTPS –Long-Term Preservation Service

CA – Certification Authority

TSA – Time Stamping Authority

4 INTRODUCTION

The power and suitability of cryptographic mechanisms is a function of time and it is necessary to apply appropriate storage mechanisms that are able to maintain the validity of the signed object over long periods by applying different storage technologies and schemes, and cryptographic algorithms.

This necessity is recognized and referred to in the Regulation (EU) No 910/2014 of the European Parliament and of the Council, as can be seen in the Preamble:

(61) This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

Furthermore, Art. 34(1) of the Regulation states that:

A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

This document presents the Policy and Practice Statement for the SERVICE of BORICA as a Qualified Trust Service Provider and the preservation scheme (mechanisms), which are used to preserve the validity status of qualified e-signatures/e-seals and of data objects using signatures/seals.

5 CONCEPT

5.1 General requirements

The Provider's Policy and Practice Statement for the SERVICE is addressed to:

- the long-term preservation of e-documents;
- the validity status of preserved signatures/seals.

The preservation (of integrity) of digital objects that are not signed/sealed is outside the scope of this document. The legal validity of preserved signatures/seals is also outside this scope.

5.2 Long-term preservation goals

The long-term preservation schemes presented in this document address the following goals:

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

Data integrity is verified during the preservation period by means of a proof of integrity (hash, signature/seal).

The existence of a digital object at a specific time is maintained by a combination of a proof of integrity (completeness) and a qualified time-stamp.

According to this document, the two basic types of digital objects, for which the SERVICE is used, are:

- Signed/sealed e-documents (enveloped and enveloping signature/seal), for which validity status has to be preserved over a long period of time;
- Detached signature/seal and associated digital object (document/file).

To preserve the validity status of the electronic signature/seal, each data of their validation has to be preserved, the validity of which is subject to expiration (cannot be guaranteed) in the future (certificates, information of suspension/revocation – CRL, OCSP responses, trusted lists, etc.).

Additional goals for preservation may be identification of the SERVICE Provider, non-repudiation of submission of digital objects to the SERVICE and data confidentiality in the exchange. These preservation goals are (for now) out of the scope of the present Policy.

The SERVICE creates preservation evidence that are used to verify the performance of the respective preservation goals for the specified digital objects.

5.3 E-document and container

E-document is data processed by the SERVICE for the purpose of long-term preservation of the signatures/seals. It can be a basic data object(s) (enveloped/enveloping signature/seal), which has to be preserved or metadata submitted by an Applicant/Submitter or collected and added by the service itself. Multiple e-documents can be combined into a storage container.

The storage container may include:

- more than one e-document;
- locally associated multiple e-documents – for example, within a single sending/submission or stored in a single directory by the Submitter.

Digital objects added by the SERVICE can be for example certificates of CAs, CRL/OCSP- responses, signatures/seals, time stamps, evidence, validation reports.

Not all e-documents should be submitted together for preservation.

An elementary storage container contains only one e-document (i.e. it addresses at least one preservation goal).

The Submitter is the subject who sends e-document(s) to the SERVICE. He may me different form the Subscriber (owner) of the e-documents submitted for preservation. The SERVICE generates a POCID (container identifier), which is returned to the Submitter (if the SERVICE includes archive). POCID is a unique identifier of the storage container. It is generated on the basis of a hash-function, i.e. it is a hash code with a specified identifier of the hash-algorithm.

5.4 Preservation mechanisms and schemes

The Long-term Preservation Scheme is a set of preservation mechanisms for achieving specific goals for preservation of e-documents. Basic preservation schemes, applicable for the SERVICE are:

- Time stamp;
- Advanced Electronic Signature/Seal with extended format (AdES);
- Evidence Record (ER);
- Validation report (from a qualified signature/seal validation service)
- and others.

5.4.1 Time stamp

The time-stamp protects all data, which are input of a hash function with an identified algorithm, and serves as an evidence of existence of that digital data at a particular time certified in the time-stamp. This evidence is valid as long as the used algorithms are suitable and the certificate is trustworthy (i.e. the certificate of the TSA is valid and not revoked).

This mechanism is an easy way to prove the existence of some digital data. To support additional functionalities, such as validation data protection, this mechanism is combined with other mechanisms (such as AdES or ER). It cannot provide by itself a long-term evidential strategy (collection of validation material or vulnerability/weakness in hash algorithms).

5.4.2 Advanced Electronic Signature/Seal

The Advanced Electronic Signature/Seal with extended format/profile provides an internal mechanism, through which it remains verifiable after a long term. For more information regarding the validation of qualified signatures/seals, see the document “Signature Validation Policy and Practice statement of B-Trust qualified Validation Service” (B-Trust QSVS – CP and CPS). All advanced BASELINE profiles at conformance level: B_T, B_LT and B_LTA are extensions to the previous level with additional evidence material for long-term signature/seal preservation:

- _T level – a time-stamp is added to the basic signature/seal; the signature/seal has been created before the certified time – an important evidence in case the certificate of the signature/seal becomes invalid in future (after expiry or revocation);
- _LT level - this format extends the previous one with additional evidence of the validity of the signature/seal certificate (OCSP status, CRL); A signature/seal at this level allows for validation provided that there are no technological changes (for example, the algorithms used become weak).
- _LTA level – a specific hash-algorithm recalculates the hash of the originally signed/sealed document with the signed attributes and together with previously added validation material and time-stamp is protected with a new time-stamp; a signature/seal at this level allows for validation of the original signature provided that the last added time-stamp is validated and the last used hash-algorithm is still reliable.

A signature/seal at LTA level is the most suitable for long-term preservation. The mechanism is alike for the different formats. It is based on standardized formats and has a high degree of interoperability – it can easily be exported from the SERVICE to another such service. All the missing validation material is added, a hash is computed over the existing signature including the originally signed document, and a time-stamp is generated over the final hash computation. The disadvantage is that a single time stamp is needed to protect a single parallel signature.

5.4.3 Evidence Record

In accordance with IETF RFC 4998 (ASN.1 coding) or IETF RFC 6283 (XML encoding). It contains a set of archive time stamps and some additional data. This Evidence Record can be stored separately from the archived data as a file, or integrated into the archived data as an attribute. Time stamps are renewed by generating a new time stamp that covers the original data and its time stamps prior to the compromise of mechanisms (algorithms) used to generate time stamps.

5.4.4 Long-term preservation schemes

Based on the above feasible mechanisms and their characteristics for long-time preservation of an e-document, different schemes involving one or more of these mechanisms are admissible:

5.4.4.1 Long-term preservation via Evidence Records (ER)

If there is no ER for the document, the AdEs is validated, collected and the missing validation material is added to the container; the SERVICE creates an ER protecting all the elements of the container and stores it in the Archive.

If the document is already covered by an ER, the preservation SERVICE only augments the ER (via Time-stamp Renewal).

5.4.4.2 Long-term preservation via AdES augmentation

An e-document with AdES signature/seal is submitted to the SERVICE. If the signature is detached, the original document is also needed or at least its hash for the respective hash algorithm. If the signature/seal is basic (B level), the SERVICE adds a time-stamp to it. The SERVICE then validates the e-document (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 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).

An internal process monitors when the signature/seal (e-document) needs to be augmented again – e.g., the certificate of the latest time-stamp expires, and/or the cryptographic algorithm or the hash algorithm becomes weak.

5.4.4.3 Using time stamps with a long validity period

This scheme addresses a special case of the above scheme (5.4.4.2).

The validity period of the time stamp, instead of being limited by the validity period of the TSA basic certificate, is extended as long as the cryptographic algorithms remain secure, with the purpose to augment the signatures/seals less often.

5.4.4.4 Based on a validation report

When receiving an e-document for preservation signed/sealed by AdES, the SERVICE will first request a validation report from the signature/seal validation service. Instead of augmenting the original signature of the e-document, the service augments the signature/seal of the validation report to keep it verifiable for a long term. To guarantee the integrity of the original e-document even after the original hash algorithm becomes weak, before augmenting a hash value with a latest used hash algorithm is added to the signature/seal of the validation report.

The scheme stores the document together with the augmented validation report. The originally submitted signature/seal (e-document) is not changed.

5.5 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. The process of qualified signature/seal validation is outside the scope of this document.

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 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 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 must use an internal and/or an external process (a qualified time-stamping service). The validity verification of time stamps is direct and does not require mandatory use of a qualified time-stamping service. The Provider's B-Trust QTSA-eIDAS qualified time-stamping service may also be used for verification of the time stamps.

5.6 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).

When the SERVICE supports an integrated Archive/Storage, it performs the following operations/procedures:

- UPLOAD (DEPOSIT) - the service verifies the electronic signatures/seals in the e-document(s) or file(s), completes and/or generates the long-term validation material (evidence), places a qualified time stamp on this material, creates the container and stores it together with the e-document to the Archive; subsequently it returns to the submitter a POCID (a unique identifier of the preservation container);
- DOWNLOAD (RETRIEVE) – The Submitter/Subscriber can download his e-documents stored in containers in the Archive and the respective long-term validation material (evidence);
- ACK (RETRIEVE PROOF) – At the request of the User/Subscriber, the Provider issues an acknowledgement (preservation evidence) related to an archived e-document; the SERVICE returns the requested preservation evidence. This procedure may be performed jointly within the RETRIEVE/DOWNLOAD procedure;
- DISPLAY – at a specified date and place the User/Subscriber has the opportunity to view his e-documents stored in the Archive;
- UPDATE STORED ELEMENTS (option) – a User/Subscriber sends a POCID to the SERVICE and "Delta e-document" to update an e-document in the Archive container, creating a new version of the container; the SERVICE returns the new version of the updated container and (optionally) the updated preservation evidence. The original version of the container is retained;
- DELETE - At the request of the User/Subscriber the SERVICE provides selective deletion of e-document(s) (and all respective evidence for long-term validation), stored in the Archive. Deletion means physical erasure of the PDO (document) from the Archive in such a way that it cannot be recovered later (or only with unrealistically high financial costs);
- AUGMENTATION – This procedure/operation is not a part of the User interface and it is activated/started automatically (internally) in order to ensure the long-term preservation of the validity of the signature(s)/seal(s) of e-documents, i.e. to extend the period during which the proof of it is supported (the validity of signature(s)/seal(s));
- MONITORING – This procedure is not a part of the User interface and it is activated automatically (internally), in accordance with the Policy of the SERVICE. The operation monitors various events, which could threaten the validation of the preservation evidence. It can activate (internally) the AUGMENTATION procedure.

The SERVICE may be provided to Users in a version without Archive. In this model of the SERVICE, the Subscriber is responsible for the local (at his sites) long-term preservation and management/maintenance of signatures/seals.

BORICA as a QTSP provides the SERVICE to Subscribers with integrated Archive for storage of e-documents and preservation evidence.

5.7 Policy and Practice Statement

This document defines the common elements of the Policy and Practice Statement of the Provider of the SERVICE and has the nature of general terms under Art. 33, para. 2 of the Ordinance on the Activities of Certification-Service-Providers (OACSP) and within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These terms are part of a written Service Agreement that is concluded between the Provider and Users.

The Policy sets out the terms and conditions, to which the Provider adheres, to implement the Practice Statement for providing the SERVICE.

The Practice Statement describes how the Provider implements the described Policy, and the procedures followed for providing the SERVICE.

Through this SERVICE (B-Trust Qualified LTPS) the Provider preserves a qualified e-signature/seal and/or an advanced signature/seal accompanied by a qualified certificate of any interested party, subject to a common Validation Policy.

A rule in the Practice Statement of the Provider of the SERVICE is to provide long-term preservation of validated signatures/seals with formats/profiles according to its Policy following the terms and procedures included in this document.

The Provider's Practice Statement for the provision of the SERVICE is implemented by the B-Trust Qualified Preservation Service (B-Trust QPS) identified by OID 1.3.6.1.4.1.15862.1.6.7:

SERVICE for long-term preservation of QES/QESeal (B-Trust Qualified LTPS)	**OID**
Practice Statement of the SERVICE Provider	**1.3.6.1.4.1.15862.1.6.7**

In accordance with this document, the Provider's Practice Statement complies with a Policy for the Service with identifier as follows:

SERVICE (B-Trust QLTPS)	**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.

When 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 this general Policy and the Signature Policy.

When a long-time 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 of the certificate.

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 (format, profile, certificates, Provider, validity, etc.) is contained in the preservation evidence, with regard to the applicability, and as a consequence, its relevance for a particular business purpose.

5.8 Policy and Practice Statement Administration

The Provider's Policy and Practice Statement 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 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.

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.: (02) 9215 115, fax: (02) 981 45 18.

5.9 Other Related Documents

This document should be used together with the following documents concerning the qualified services of BORICA as a QTSP:

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

6 Long-Term Preservation SERVICE

6.1 Participants

The parties involved in the process of long-term preservation of signature/seal are:

- A Provider (QTSP) that operates the long-time preservation process;
- Subscribers (Relying parties);
- Applicant/User - a person authorized by the Subscriber to use the SERVICE;
- Indirect/external parties/participants in the long-term preservation process:
  - Parties that have signed/sealed documents;
  - External QTSP (their certifying authorities – CA, TSA, CRL/OCSP);
  - National Trusted List;
  - European List of Trusted Lists.

The service has national scope only for 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.

6.2 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 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.

BORICA as a QTSP operates and provides a qualified trust service for validation of advanced/qualified signature/seal that complies with EU Regulation 910/2014 and meets the requirements (Article 1-4) of the above-mentioned Decision. See document B-Trust QSVS-eIDAS.

In addition, the B-Trust QSVS-eIDAS also validates the formats of the specified signatures/seals at LTA level as well as signature/seal with ASiC-S/E profile.

Appendix 1 to this document presents the formats of containers of signatures/seals with specified profiles and levels.

6.3 Long-term preservation model

The SERVICE provided by BORICA as a QTSP, following the general normative established technical specifications for long-term preservation (RFCs or TS) of the IETF or the ETSI, and in compliance with the Concept for long-term preservation of signatures/seals (i.e. e-documents) presented in this document, implements the scheme under section 5.4.4.2 herein (Long-term preservation via AdES augmentation).

Considerations for Choosing the Scheme:

- The SERVICE can be considered as an extension to the functionality of the qualified B-Trust signature/seal validation service QSVS-eIDAS that complies with EU Regulation 910/2014;

- The eligible formats of signatures/seals for long-term preservation are equivalent to those supported by the B-Trust QSVS-eIDAS;
- The B-Trust QSVS-eIDAS validates signature/seal (e-document) formats/profiles in strict accordance with IMPLEMENTING DECISION (EU) 2015/1506 on the Regulation, including the B_LTA level; Additionally, the service validates signature/seal in ASiC-S/E format (Signature/Seal Document Container) at signature levels (B, B_T, B_LT, and B_LTA);
- The B-Trust QSVS-eIDAS is a part of the common platform of the QTSP BORICA for qualified signing/sealing of documents and files, following the formats/profiles specified in the DECISION (B, B_T, B_LT and B_LTA);
- The scheme using AdES is easily adaptable/applicable to the different formats/profiles of signatures/seals (e-documents);
- Interoperability (in the future) with another similar service (e.g. on a national scale).

6.4 Long-term preservation goals

The SERVICE supports the following long-term preservation goals:

- 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.

For more information, see section 5.2 of this document.

6.5 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.

6.6 Functional model

The SERVICE (B-Trust Qualified Long-Term Preservation Service/B-Trust Qualified LTPS) of the Provider BORICA includes the following software components:

- Qualified Preservation Service Client (QPS_Client) – the component is at the side of the Submitter/User. It can be a web-browser/web-client with a graphical interface (GUI), with the following functionality:
  - Requests/functions
  - Storage protocol
  - Providing preservation evidence.
- Qualified Preservation Service Server (QPS_Sever) – a web service (Signature/Seal Preservation Service/SPS) at the Provider's side with the following functionality:
  - SPS-Upload – according to section 5.6. of this document
  - SPS-Download – according to section 5.6. of this document
  - SPS-ACK (Retrieve Proof) – according to section 5.6. of this document
  - SPS-Delete – according to section 5.6. of this document
  - SPS-Monitor (internal function) – monitors acceptable strong cryptographic and hash algorithms
  - SPS-Augmentation (internal function) – according to section 5.6. of this document
  - storage protocol

- interfaces to internal and external/indirect participants/parties to the SERVICE – CRL/OCSP of Certifying Authority(ies), TSA, BG-TL.

Figure 1 presents the functional model of the SERVICE.

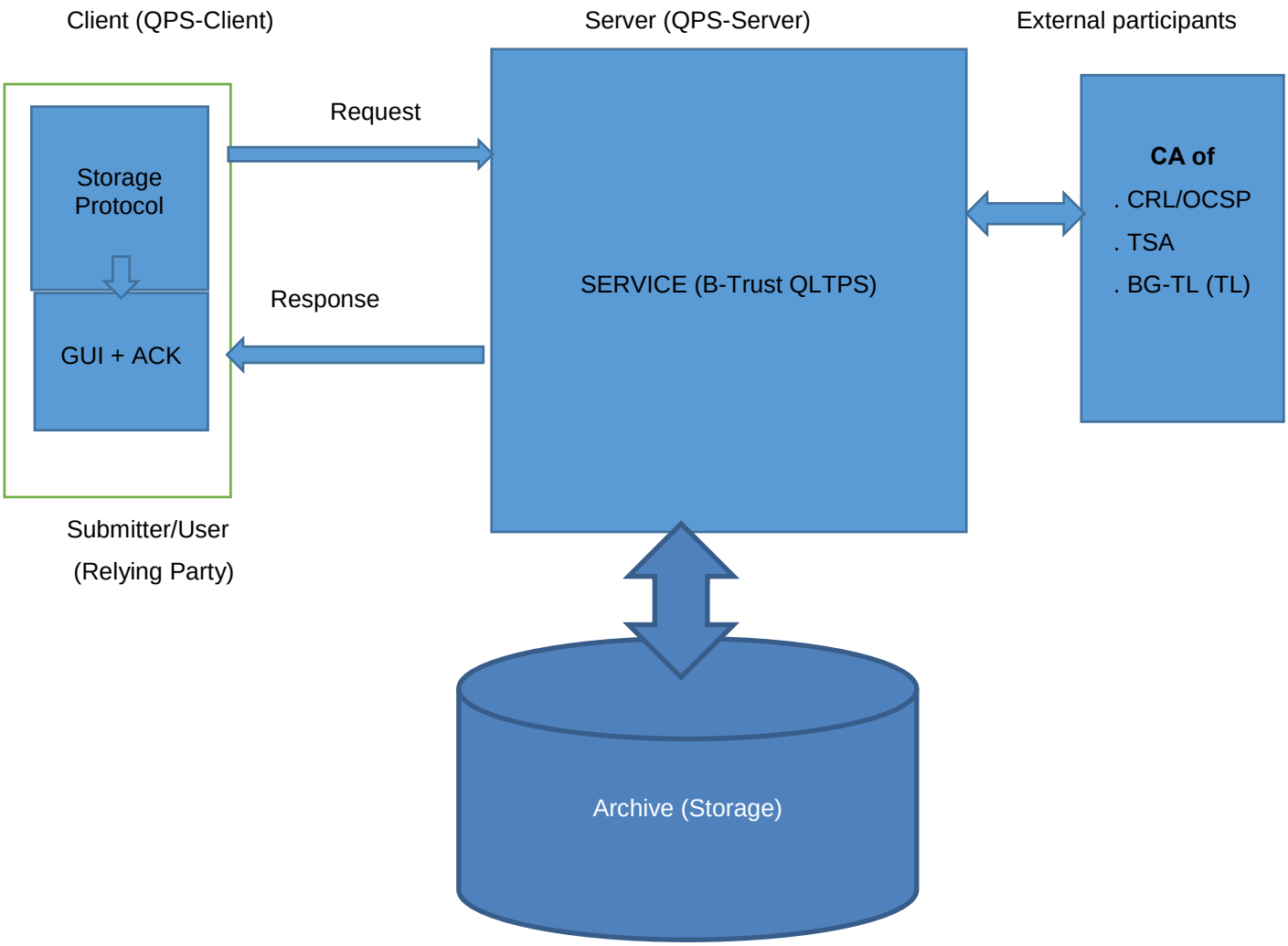

Fig.1 Functional model of the SERVICE

6.7 Basic processes and procedures

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.

6.7.1 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 acknowledgement to the Subscriber that the long-term validation material (evidence 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 an 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.

6.7.2 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.

6.7.3 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 respective e-documents and 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 advanced electronic signature or on paper. The acknowledgement is created by an official responsible for issuing Acknowledgements of the Archive who, in case of an electronic Acknowledgement, applies his/her advanced 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.

6.7.4 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.

6.7.5 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.

6.8 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 of the Subscriber, 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.

6.9 Interfaces and protocols

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

- OASIS DSS interface;
- GUI interface.

Both interfaces use secure communication channel supporting authentication of the Applicant/User of the SERVICE.

The SERVICE is authenticated to the Applicant/User (the Relying Party) via a Qualified Website Authentication Certificate issued on its Component (SPS_Server) by the CA of B-Trust.

6.9.1 OASIS DSS interface

SVS_Client application accesses the SERVICE via OASIS DSS Interface that defines a set of XML Requests/Responses of the SERVICE protocol.

The protocol of OASIS DSS interface uses a SOAP protocol to transport the Requests/Responses of the SERVICE.

6.9.2 GUI interface

The Service is accessed by the Applicant/User (Relying Party) through a web application that operates with its browser and uses a graphical interface. Through it the User performs the procedures/functions under section 6.7 of the document.

This interface uses HTTP (S) POST protocol for transport/exchange.

6.10 External sources of preservation evidence

In certain cases, for example, collecting evidence validation material for preservation of signatures/seals, the SERVICE requires access to external sources related to the validation process of a signature/seal to a signed/sealed document that is subject to long-term preservation in the Service Archive. Such external participants in long-term preservation are:

- repositories of certificates maintained by the QTSP - public registers, CRL/OCSP sources; TSA/time stamping authorities (time stamps);
- National Trust List, External (Member States) Trust Lists (TL);

The SERVICE uses standardized software interfaces to access these external sources to deliver evidence validation material of preservation signatures/seals in the Archive.

7 TECHNICAL SECURITY MEASURES

7.1 Security Guarantees

The Provider uses reliable systems and products that are protected against unauthorized modification. The Provider keeps the archived e-documents in a physically protected environment in accordance with the Physical and Procedural Requirements described in Section 5 of the B-Trust CPS-eIDAS Document (the General Practice of BORICA) and is guaranteed by internal security policies and regular audits of internal and external security.

The Provider encrypts electronic documents always with an algorithm that is considered safe/secure at a given state of the technology and stores e-documents via encryption.

7.2 Computer Security Precautions

The Provider uses reliable IT systems and solutions, technologies, and redundancy in the systems of the SERVICE. The critical components of the system are redundant. A system of firewalls is used in the IT infrastructure of the SERVICE.

7.3 Life-cycle Safety Precautions

System components for the SERVICE are used, taking into account the safety considerations related to the component lifecycle.

7.4 Regular Audit/Certification

The Service Provider is a QTSP and its activity is subject to a regular Audit in accordance with Regulation 910/2014. Issued or renewed certificates of the Service Provider verify the compliance of the SERVICE with this document. See section 8 of the document "Certification Practice Statement for Provision of Qualified Certificates and Certification Services" (B-Trust CPS-eIDAS).

7.5 Re-Encryption of the Archive

The Provider ensures that archived e-documents are encrypted with an encryption algorithm that is secure/reliable anytime. This requirement determines the need to re-encrypt the Archive in the future when the crypt-algorithm used is considered weak/insecure.

7.6 (Continuous) technology monitoring

The Service Provider continuously monitors development of technologies related to electronic signature and cryptography. In the event that a technical specification or normative document declares a

cryptographic algorithm with a given parameter to be unsafe, the Provider shall act appropriately to eliminate any risk.

7.7 Selection of external providers

The scope of Service addresses (so far) only B-Trust Users. It does not use external sources to collect evidence validation material for signatures/seals.

7.8 Interoperability of signatures/seals

According to the Policy of the SERVICE, the Provider preserves only signatures/seals (e-documents) with internationally validated profiles and signature levels in view of future interoperability with other similar preservation services.

8 RISK ASSESSMENT

Taking into account detected business and technical problems in the delivery, operation and maintenance of the SERVICE, the Provider performs risk assessment to identify, analyze and assess the related risks.

Relevant/appropriate measures to avoid identified risks are chosen in view of the results of the risk assessment. The measures ensure a level of security equivalent to the degree of identified risks.

The Provider documents via the Practice Statement and the Policy included as parts of this document the security requirements and operational procedures necessary to avoid identified risks for the SERVICE.

Periodic review and risk assessment is 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 Trust Services" (B-Trust CPS-eIDAS).

9 PRACTICE STATEMENT

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

9.1 Service Certificates

The SERVICE has two public certificates:

- Qualified certificate for advanced electronic seal;
- Advanced certificate for website authentication.

The certificate for e-seal of the B-Trust Qualified LTPS is a qualified certificate for advanced electronic seal and is electronically sealed with a private key of the B-Trust Operational Advanced CA of the Provider. With the private key of the SERVICE corresponding to the public key in this certificate, the

Provider seals electronically the Acknowledgement for long-term preservation that is provided to the User/Relying party.

This certificate authenticates the SERVICE as the source of the generated Acknowledgement for preservation of an electronically signed/sealed e-document and validates the integrity of the data in the Acknowledgement.

The website certificate of the B-Trust Qualified LTPS is an advanced website certificate and is electronically sealed with a private key of the B-Trust Operational Advanced CA of the Provider. This certificate authenticates online the site of the SERVICE to the User and services a secure SSL/TLS session with the User.

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

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	29 b9 2a 56
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	-	2019-02-27T14:34:27Z
Validity to	-	2022-02-26T14:34:27Z
Subject	CN =	B-Trust Qualified Long-Terms Preservation Service
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 Bits)
Subject Key Identifier		87 b3 81 c2 a2 78 1d dd 3f d6 18 53 1f 58 c6 ae 84 ce ab 6f
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=1.3.6.1.4.1.15862.1.7.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.1
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 (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-TrustOperationalACA.cer	
Key Usage(critical)	-	Digital Signature	
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 (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/qltps_pds_en.pdf language=en
Thumbprint (Sha1)		4f 4a 4c fc 6e 52 20 c3 96 d2 a7 79 8a 01 2c f9 db f5 8a a2	
Thumbprint (Sha256)		a9 b9 16 b4 7e 21 fe 32 05 04 d5 17 4a c4 ee b8 1b b9 32 bf 44 18 a0 86 f9 80 16 b1 c2 f4 a5 53	

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

Field	Attributes	Value/meaning
Version	-	V3
Serial number	-	29 b9 2a 55
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	-	2019-02-27T11:52:42Z
Validity to	-	2021-06-01T12:52:42Z
Subject	CN =	qltps.b-trust.org
	O =	BORICA AD
	2.5.4.97= (organizationIdentifier)	NTRBG-201230426
	OU	OV SSL
	C =	BG
Public key	-	RSA(2048 bits)
SubjectAlternativeName		https://qltps.b-trust.org
Subject Key Identifier	-	8b 07 4f 9d fc 60 23 1c da be 68 a2 dd 1d fe 90 c3 f0 cc 67
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/qltps_pds_en.pdf language=en
Thumbprint (Sha1)		ed 14 85 aa c9 38 44 c0 11 7a 27 c2 01 d1 d1 b0 44 4e c0 6f	
Thumbprint (Sha256)		33 ea 95 fc f1 7f d2 bc fa c4 f3 af 06 25 bd 8f 8f d1 0e b0 c7 dd fb 7a c4 a1 0a 0b 24 31 b3 c6	

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

Name	**Algorithm**
Hash-algorithms:	SHA 256
Asymmetric algorithms:	RSA
Symmetric algorithm:	AES

9.2 Facility, Management, and Operational Controls of the SERVICE

9.2.1 Internal organization at the Provider

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

9.2.2 Personnel

The characteristics of the personnel of the QTSP 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 Trust Services" of BORICA (B-Trust CPS-eIDAS).

9.2.3 Asset Management

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

9.2.4 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, as described in the document "Certification Practice Statement for Provision of Qualified.

9.2.5 Cryptographic security - Key management

9.2.5.1 Key pair generation

The RSA key pair to the qualified certificate for e-seal and for website authentication of the SERVICE is generated in a highly secure software environment (PKCS#12) by Provider's personnel eligible to perform this role. The generated pairs of RSA keys have length of 2048 bits.

The description and role of these personnel are specified in the document "Certification Practice Statement for the Provision of Qualified Certificates and Certification Services" of BORICA (B-Trust CPS-eIDAS).

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

The procedures for generating these key pairs are in accordance with the documents: „Policy on the provision of qualified certificates for advanced electronic signature and advanced electronic seal" (B-Trust QCP-eIDAS AES/AESeal), and "Policy on the provision of Qualified Certificates of Website authentication" (B-Trust QCP-eIDAS Web SSL/TLS).

9.2.5.2 Private Key protection

The generated private keys of the SERVICE are stored in a PKCS # 12 cryptographic file protected by a secure password. A copy of the cryptographic file is stored in a special safe for restoration purposes.

9.2.5.3 Public key distribution

The public keys of the SERVICE are certified by the qualified e-seal and website authentication certificates issued by the respective Operational CA in the B-Trust hierarchy of the Provider.

The Provider publishes the website authentication certificate of the SERVICE on its website.

In order to authenticate the SERVICE, a User/Relying Party should have loaded on his computer/system the certificate of the B-Trust Operational Advanced CA (part of the B-Trust Certification chains, also published on the Provider's website).

9.2.5.4 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 3 years. After this period a new key pair is generated,

the private key from which is stored in a new cryptographic file PKCS#12, and the public key is certified by issuing a new certificate of the SERVICE. The key pair with expired validity period is stored as follows:

- private key - stored for a period of 10 years;
- public key - stored for a period of 10 years.

9.2.6 Physical and Environmental Controls

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

9.2.7 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 Trust Services" (B-Trust CPS-eIDAS) (sections 6.6, 6.7, and 6.8).

9.2.8 Network security

See section 6.9 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.2.9 Management of journals

See section 5.4 of the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

9.2.10 Continuity

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

9.2.11 Termination of the 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 Trust Services" (B-Trust CPS-eIDAS) are performed.

9.3 Information security

BORICA shall not publish a specific 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 Trust Services (Qualified Signature/Seal Certificates and Qualified Time Stamps) under Regulation 910/2014.

The information security of the components of the B-Trust infrastructure is part of the common information security policy of BORICA, 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 personnel having direct relations to these systems and assets is acquainted with and implement this Policy. See the document „Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

The preserved signatures/seals (e-documents) in the Archive may contain information to be considered personal data. In accordance with the legislation on such data, BORICA as a QTSP, respectively as the Provider of the SERVICE, is registered by the Commission for Personal Data Protection as a data controller.

The preserved e-documents in the Archive are encrypted. Only authorized persons of the Provider's personnel perform decryption or encryption function of the stored signatures/seals (e-documents) in the Archive.

10 BUSINESS AND LEGAL ISSUES

See section 9 of the document „Certification Practice Statement for Qualified Certificates and Qualified Trust Services" of BORICA (B-Trust CPS-eIDAS).

Appendix 1. E-Signature/E-Seal Profiles and Levels eligible for 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