Public document

# QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE

# POLICY AND PRACTICE STATEMENT

Version 1.0

Effective October 20, 2024

| Document history | | | | |
|---|---|---|---|---|
| **Version** | **Author(s)** | **Date** | **Status** | **Comment** |
| 1.0 | Margarita Boneva | 1.08.2024 | Approved | Initial release |

# CONTENTS

# ACRONYMS

| | |
|---|---|
| AD | JSC (Joint-stock company) |
| CA | Certification Authority |
| CC | Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) |
| CEN | Comité Européen de Normalisation, the European Committee for Standardization |
| CRC | Communications Regulation Commission |
| EDETSA | Electronic Documents and Electronic Trust Services Act |
| EGN | Bulgarian Unified Civil Number, a 10-digit unique number assigned to each Bulgarian citizen. It serves as a national identification number. |
| eIDAS | Electronic Identification, Authentication and trust Services |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| HSM | Hardware Security Module |
| IP | Internet Protocol |
| ISO | International Standardization Organization |
| PIN | Personal Identification Number |
| QTSP | Qualified Trust Service Provider |
| RA | Registration Authority |
| RA-VI | Registration Authority using remote video identification |
| UIC/BULSTAT | Unified Identification Code (UIC). All legal entities in Bulgaria receive a UIC upon registration. The UIC is assigned by the Registry Agency who manages the Trade Register or the BULSTAT Register. |

# TERMS AND DEFINITIONS

**Identity Document** - a valid document containing data for the identification of a natural person in accordance with the national legislation of the respective country.

**RegiX**/Registry Information eXchange System – a national information hub for access to national databases (registers) of official primary data.

**Personal Data** – any information as defined in Article 4, point 1 of Regulation (EU) 2016/679

**Identity Verification** – a process by which an individual's identification data or means of electronic identification is compared or linked to an existing profile of the same individual.

**Qualified Electronic Registered Delivery Service (QERDS)** – a service that meets the requirements of Regulation (EU) No. 910/2014 and Regulation (EU) No. 2024/1183.

**Qualified Electronic Registered Delivery Service Provider** – Entity providing the SERVICE - a Qualified Trust Service Provider providing the Qualified Electronic Registered Delivery Service.

**ERDS Evidence** – data generated by the SERVICE as (irrevocable) evidence of the occurrence of a specific event at a specific point in time in the electronic delivery process.

**Sender** – a natural or legal person who sends specific Content;

**Recipient** – a natural or legal person receiving specific Content;

**e-Delivery** – data, including User Content and metadata, to be sent to the SERVICE.

**Transmission** – an act of successful passage of User Content across the boundary of the infrastructure/system of the SERVICE to the Recipient.

**Delivery** – an act of making the User Content available to the Recipient within the boundaries of the infrastructure/system of the SERVICE.

**Handover** – occurs when the content sent by the Sender successfully enters the information system of the Recipient.

**User Agent** – a means consisting of software and/or hardware through which Senders and Recipients participate in data exchange with the SERVICE.

**Transmission Metadata** – data related to User Content generated by the SERVICE and transmitted to the User Agent.

## COMPLIANCE AND USE

This document:

- has been issued by the company "BORICA" AD (hereinafter referred to as BORICA), a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- is valid from 20.10.2024;
- has the character of general terms and conditions within the meaning of Art. 16 of the Obligations and Contracts Act. These conditions are part of the Trust Services Contract concluded between the Provider and the Users on the basis of art. 23 of the EDETSA, in the cases in which it is applicable. The contract may contain special conditions that prevail over the general conditions of this document;
- is a public document with the purpose of establishing the conformity of the activity of the Provider BORICA, and in particular of the RA-VI, with the EDETSA and the legal framework;
- is available at any time on the website of the Provider at https://www.b-trust.bg/documents;
- may be modified by the QTSP BORICA, as each updated version of the Policy and Practice Statement shall be published on the website of the QTSP.

**This document has been prepared to comply with the following**:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market;
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1: Framework and Architecture;
- ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents;
- ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats;
- ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1: Message delivery bindings;

- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2: Evidence and identification bindings;
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-3 Capability and requirements bindings;
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- ETSI EN 319 412-5 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI TR 119 520-1 Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 1: New (Q)ERDS/(Q)ERDSP standardization rationalized framework as a result of the new components brought by eIDAS 2.0;
- ETSI TR 119 520-2 Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 2: Impact of emerging technologies on ERDS/REM Models.

- The Electronic Government Act (E-Government Act) and its Regulations;
- The Electronic Identification Act and its Regulations;
- The Electronic Document and Electronic Trust Services Act (EDETSA);

For more information about this document, contact the Provider at:

41 “Tsar Boris III” Blvd.
1612 Sofia
BORICA AD
Phone: 0700 199 10
www.b-trust.bg

# 1. GENERAL PROVISIONS

Qualified registered delivery is the digital equivalent of traditional registered mail with return receipt and has the same legal value. Qualified registered delivery provides proof of sending and receipt of data and protects transmitted documents against the risk of loss, theft or unauthorized alteration. The service is intended for individuals and legal entities, government institutions, municipalities and public organizations. Data sent and received via QERDS can be used in legal proceedings in all EU member states. The legal validity and admissibility of an electronic document as evidence in legal proceedings cannot be contested solely on the basis of its electronic format.

The Registered Delivery Service includes:

- C2C (Client to Client) – Sender and Recipient of User Content are natural persons;
- B2C (Business to Client) – Sender is a legal entity and Recipient(s) are natural persons;
- C2B (Client to Business) – Sender is a natural person, and Recipient is a legal entity;
- B2B (Business to Business) – Sender and Recipient are legal entities operating business applications.

The User Agents through which the Sender and the Recipient communicate with the SERVICE are as follows:

- B-Trust Mobile Application
- My B-Trust Web Portal
- Application Programming Interface (API)

The Service is provided in accordance with Art. 44 of Regulation (EU) No. 910/2014 and in accordance with Regulation (EU) No. 2024/1183 and allows registered delivery from a mobile application to a mobile application, from a mobile application to a specialized web portal and vice versa, from an API to a mobile application and vice versa.

## 1.1. BORICA Certification Authority

BORICA has informed the CRC about the commencement of its activity as a QTSP in accordance with the EDETSA and the applicable legislation. The Provider shall inform the Users about its accreditation when providing Qualified Trust Services.

he accreditation of BORICA as a QTSP in accordance with the Regulation and EDETSA is aimed at achieving the highest level of security of provided Qualified Trust Services and better synchronization of these activities with related activities provided in other Member States of the European Union.

In relation to users and third parties, only the version of this document that is in force at the time of the use of the respective service shall be considered as valid.

## 1.2. Identifiers

The Certificate Policy and Certification Practice Statement of the QTSP BORICA regarding the SERVICE complements the general Certificate Policy and Certification Practice Statement for the Qualified Trust Services provided by the Provider. In particular, this document describes the applicability of the SERVICE, sets out the conditions and rules to which the Provider adheres.

The SERVICE is provided through the object identified by the identifier 1.3.6.1.4.1.15862.1.6.11 in the document "Practice statement for the provision of qualified certificates and qualified trust services by BORICA (B-Trust CPSeIDAS)".

| Policy name | Object Identifier |
|---|---|
| QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE POLICY AND PRACTICE | 1.3.6.1.4.1.15862.1.6.11 |

### 1.3. Policy Management

Amendments, revisions and additions are allowed, which do not affect the rights and obligations arising from this document and the standard Trust Services Contract between the Provider and the Users/Relying Parties. They shall be reflected in the updated version or revision of the document.

This Policy and Practice Statement should be reviewed at least annually to reflect potential requirements and conditions associated with changes.

Any updated version or revision of this document that is submitted and approved shall be posted promptly on the Provider's website.

The document is subject to change at any time and shall be made available to interested parties via the Company's website. This document is an integral part of the policies and practices for the provision of qualified services.

## 2. PARTICIPANTS IN THE INFRASTUCTURE

**2.1.** The **B-Trust® Certification Authority** of QTSP BORICA is an organizationally separate entity that performs activities related to the issuance, provision and maintenance of qualified certificates and related qualified trust services. The CA does not have its own legal personality, and all actions and acts of its employees are performed in their capacity as employees of the Provider, within the scope of the powers granted to them.

**2.2.** The **B-Trust® infrastructure** has a two-level hierarchy of Certification Authorities for issuing and maintaining a QC for QES and QC for QESeal, as follows:

- Basic CA "B-Trust Root Qualified CA" - issues certificates to subordinate Operational CAs of the Provider;
- Operational CA "B-Trust Operational Qualified CA" - issues QC for QES and QC for QESeal in accordance with the policy for issuance of these QCs.

**2.3.** The **B-Trust® infrastructure** has a two-level hierarchy of Certification Authorities for issuing and maintaining a QC for AES, QC for AESeal, and Website Authentication Certificates as follows:

- Basic CA "B-Trust Root Advanced CA" - issues certificates to subordinate Operational CAs of the Provider;
- Operational CA "B-Trust Operational Advanced CA" - issues QC for AES and QC for AESeal in accordance with the policy for issuance of these QCs.

**The QTSP reserves the right to extend the B-Trust® infrastructure with a different hierarchy of CAs.**

*A detailed description can be found in the document "Practice Statement for the Provision of Qualified Certificates and Trust Services by BORICA AD".*

### 2.4 Users

Any natural person or legal entity that has entered into a contract with BORICA for QERDS is a user of the SERVICE and may function as a sender and/or as a recipient.

Where practicable, QERDS trust service and products are available to disabled persons.

Third Parties, also referred to as Relying Parties, are individuals or entities that rely on evidence provided by the Provider in connection with QERDS.

## 3. CERTIFCATE PROFILES

**The profile of the B-Trust Qualified Time Stamp Authority certificate is presented below:**

| Field | Attributes | Value/Meaning |
|---|---|---|
| Version | - | V3 |
| Serial number | - | 4431e2c388ab5130 |
| Signature algorithm | - | Sha256RSA |
| Signature hash algorithm | - | Sha256 |
| Issuer | CN = | B-Trust Operational Qualified CA |
| | OU = | B-Trust |
| | O = | BORICA AD |
| | OrganizationIdentifier(2.5.4.97) = | NTRBG-201230426 |
| | C = | BG |
| Validity from | - | 2023-03-14 T12:14:21Z |
| Validity to | - | 2028-03-13 T12:14:21Z |
| Subject | CN = | B-Trust Qualified Time Stamp Authority |
| | OU = | B-Trust |
| | O = | BORICA AD |
| | OrganizationIdentifier(2.5.4.97) = | NTRBG-201230426 |
| | C = | BG |
| Public key | - | RSA(2048 Bits) |
| Subject Key Identifier | | c3 bb 28 36 0a 9f d9 b6 57 65 ca dc 8f bb 00 6c 6a d9 52 52 |
| Authority Key Identifier | KeyID = | 27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0 |
| Issuer Alternative Name | URL= | http://www.b-trust.org |
| Subject Alternative Name | URL= | http://tsa.b-trust.org |
| Basic Constraints | Subject Type =<br>Path length Constraint = | End Entity<br>None |
| Certificate Policy | - | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.6.3<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier: |

| | | | |
|---|---|---|---|
| | | http://www.b-trust.org/documents/cps<br>[2]Certificate Policy:<br>Policy Identifier=0.4.0.2042.1.2 | |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl | |
| Authority Information Access | - | [1]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer | |
| Key Usage(critical) | - | Digital Signature, Non-Repudiation (c0) | |
| Enhanced Key Usage (critical) | - | Time Stamping (1.3.6.1.5.5.7.3.8) | |
| Thumbprint (Sha1) | | 2D:1E:10:B1:E7:1E:BC:05:80:50:F3:22:8F:80:10:36:8C:30:DB:F1 | |
| Thumbprint (Sha256) | | 4A:D9:BA:68:27:5C:5B:73:0B:D8:78:6A:38:3A:54:9D:DA:74:7F:09:BD:D0:F1:B7:08:A9:BA:8D:C4:2C:38:4D | |
| 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-QcSSCD (oid=0.4.0.1862.1.4) | |
| | | id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf<br>language=en |

**The profile of the B-Trust Qualified Electronic Registered Delivery Service is presented below:**

Qualified Certificate for Qualified Electronic Seal of the Qualified Electronic Delivery Service. It electronically signs evidence.

| Field | Attributes | Value/Meaning |
|---|---|---|
| Version | - | V3 |
| Serial number | - | 6a9f017bafede92d |
| Signature algorithm | - | Sha256RSA |
| Signature hash algorithm | - | Sha256 |
| Issuer | CN = | B-Trust Operational Qualified CA |
| | OU = | B-Trust |
| | O = | BORICA AD |
| | OrganizationIdentifier(2.5.4.97) | NTRBG-201230426 |

| | | | |
|---|---|---|---|
| | = | | |
| | C = | BG | |
| Validity from | - | 2024-10-16 T12:28:56Z | |
| Validity to | - | 2029-10-15 T12:28:56Z | |
| Subject | CN = | B-Trust Qualified Electronic Registered Delivery Service | |
| | OU = | B-Trust | |
| | O = | BORICA AD | |
| | OrganizationIdentifier(2.5.4.97) = | NTRBG-201230426 | |
| | C = | BG | |
| Public key | - | RSA(4096 Bits) | |
| Subject Key Identifier | | 3d0721d99ed3f1cb34accc8cd0646912e6c8f3bb | |
| Authority Key Identifier | KeyID = | 27cf084304f0c583376781174dfc05e6db658bb0 | |
| Issuer Alternative Name | URL= | http://www.b-trust.org | |
| Basic Constraints | Subject Type =<br>Path length Constraint = | End Entity<br>None | |
| Certificate Policy | - | [1]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2]Certificate Policy:<br>Policy Identifier=**1.3.6.1.4.1.15862.1.6.11.1** | |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl | |
| Authority Information Access | - | [1]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer | |
| Key Usage(critical) | - | Digital Signature, Non-Repudiation (c0) | |
| 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-QcSSCD (oid=0.4.0.1862.1.4) | |
| | | d-etsi-qcs-QcType (oid=0.4.0.1862.1.6) | d-etsi-qct-eseal (oid=0.4.0.1862.1.6.2) |
| | | id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf<br>language=en |

# 4. QUALIFIED ELECTRONIC REGISTERED DELIVERY – MAIN FEATURES AND PURPOSE

The Qualified Electronic Registered Delivery Service:

- Guarantees secure identification of the recipient and the sender;
- Ensures confidentiality, integrity and authenticity of the data sent;
- Provides irrevocable confirmation of data delivery.

Provides evidence of each step in the data transfer process between parties that can be used in legal proceedings. All information provided by QERDS is stored for a period of 10 years in accordance with the national legislation of the Republic of Bulgaria (EDETSA).

## 4.1. Initial Identification and Establishment of Identity

### 4.1.1. Identity verification of a natural person

Establishing the identity of a natural person is done by:

- remote video identification or
- the physical presence of the individual or an authorized representative of the legal entity or
- means of electronic identification that meet the requirements of Article 8 of Regulation (EU) No. 910/2014 and Regulation (EU) No. 2024/1183 in terms of "significant" or "high" security levels.

The minimum set of data for a natural person, verified in a reliable source, includes full name (first name, second name, last name), date of birth, national unique identifier. The minimum set of data for a natural person may also include additional specific data: mobile phone number and e-mail address, place of birth, home address and others.

In order to prevent unauthorized use of the services and to ensure the possibility of verifying the authenticity of the data provided by the User, it is in the interest of both the User and the Provider to achieve the highest level of security by taking a copy of the User's identity document and storing it in paper or electronic form. An arrangement for taking and storing a copy of the User's identity document may be included in the Trust Services Contract concluded between the Parties. In the event that no agreement on the collection and storage of a copy of the identity document is reached, the Provider may refuse to provide the qualified trust service, as it is impossible to guarantee the unhindered provision of the SERVICE.

### 4.1.2. Identity verification of a legal entity

The initial identity of a legal entity is established through an automated check in primary registers.
The minimum set of data for a legal entity must include name of the legal entity, unique national identifier (for Bulgaria this is UIC/BULSTAT). The minimum set of data for a legal entity may include additional data: management address, VAT registration number, other data.

### 4.1.3. Identity verification of a natural person, authorized representative of a legal entity

For natural persons, initial identity verification is performed according to the order of point 4.1.1. The

authority of a natural person to represent a legal entity is verified in the relevant public register. If the natural person is not a legal representative, the authorization is proven by an express power of attorney certified by a notary.
In the event of a repeated request to use the SERVICE, identification will not be performed again, but only the validity of the identity data will be checked.

# 5. PROVISION OF THE QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE

QERDS is accessible through an Application Programming Interface (API), mobile application or a web portal. The use of the SERVICE requires the initial identification of the sender and the recipient, which is done remotely or by personal appearance of the persons or their representatives before the RA.
In accordance with the ETSI EN 319 522-1 document, the logical model of the SERVICE follows the "black box" model. This model describes the interactions of the SERVICE with the Sender and Recipients (Fig. 1).

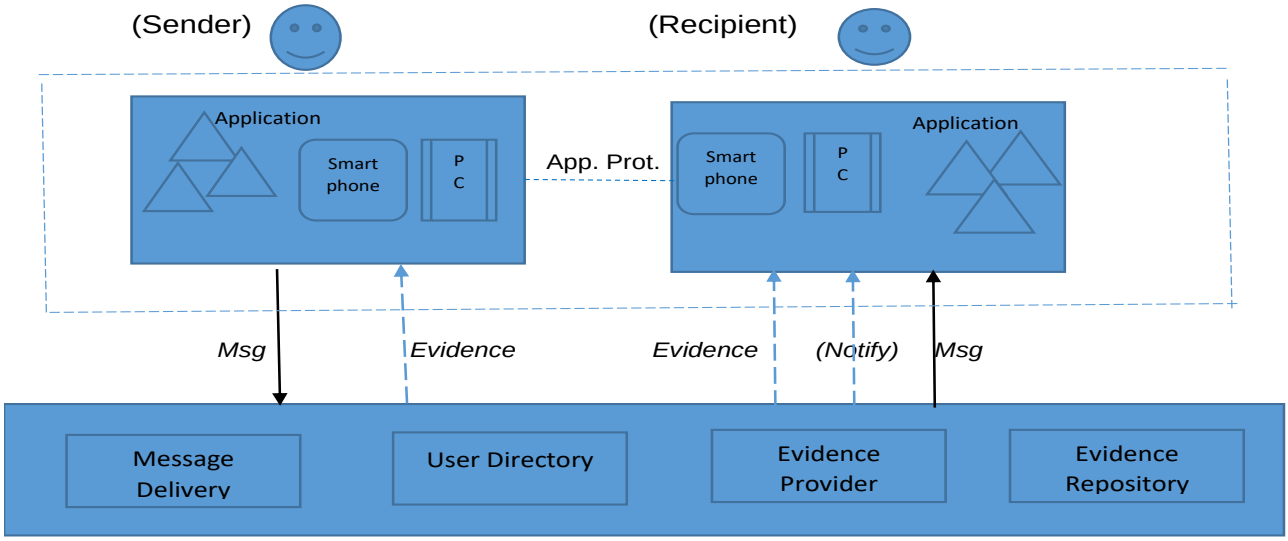


*Figure 1. Logical model of the SERVICE*

According to the Electronic Documents and Electronic Trust Services Act, the moment of sending is the moment when the sent content is not under the control of the sender. The moment of receipt of the sent content is the moment when the content sent by the sender successfully entered the information system of the recipient and the SERVICE makes the electronic content available for receipt by the recipient.

When using the mobile application, the sent content is considered received upon receipt of the electronic content in the recipient's mobile application.

When using the API, the sent electronic content is considered received when it enters the recipient's information system through an interface or when it enters the recipient's mobile application.

When using the web portal, the sent electronic content is considered received when it enters the recipient's mobile application.

Any electronic content received shall be deemed to have been properly delivered to the recipient without the need for confirmation of receipt.

**According to the presented logical model, the SERVICE implements the electronic delivery process as described below:**

1. The sender performs an initial identification or subsequent authentication with the SERVICE.

2. The sender prepares User Content for one (or more) recipient(s) and sends it to the SERVICE. The sender specifies in advance the period of time during which the system will attempt to deliver the User Content. If no option is selected, the default is 7 days.

3. The SERVICE sends a notification of the sent/delivered User Content to the Recipient in a manner specific to the Recipient and ensuring confidentiality.

4. The User Content is transferred to the Recipient, i.e., it crosses the boundary of (the system of) the SERVICE in a SERVICE-specific manner that ensures privacy.

The integrity of user content and associated metadata is protected during transmission, especially during exchange with the sender/recipient or between distributed components of the ERDS system, and during storage. User content is protected by a qualified electronic seal and excludes the possibility of data modification.

## 6. IDENTIFICATION OF THE SENDER/RECEPIENT

BORICA performs automated initial identification of the sender/recipient in one of the following ways:

- When using the API - the initial identification is performed using the B-Trust Mobile application.
- When using the mobile application - the initial identification is performed using the remote identification methods implemented in the mobile application.
- When using the web portal - the initial identification is performed using the B-Trust Mobile application, through which they are authenticated for access to the web portal, through which the documents are submitted for sending and receiving is possible.

During the automatic remote identification process, the validity of the identity document is checked against a national database of identity documents, and a liveness detection check is performed. Each successful automated identification is immediately followed by human verification.

If there is a certain percentage of discrepancy between the selfie and the ID photo, the customer is offered the option of initiating a video conference call with an operator. During this interactive session, direct communication is established with the customer, who must answer certain questions and perform certain actions. The video identification process is managed by specially trained and qualified employees of BORICA.

All events related to the initial verification of the identity of the sender/recipient and further authentication are logged and stored.

# 7. AUTHENTICATION

If it is necessary to request the service again, the initial identification is not performed, but only the validity of the identity data is checked. The User can use QERDS after authentication through the mobile application and/or, where possible, with a qualified electronic signature certificate issued by BORICA.

# 8. EVENTS AND EVIDENCE

ERDS provides evidence of events that occur during the transfer of data between parties (e.g., evidence that the data was delivered to the recipient). This evidence can be used to prove to third parties and in legal proceedings that the transaction took place at the time and between the parties as indicated in the evidence. ERDS evidence can be of two types: immediately delivered to the sender/receiver or stored in a repository for a certain period of time. BORICA stores the evidence in a secure environment for a period of 10 years.

The evidence shall include the exact date and time of sending, receiving and delivery of the User Content with a qualified electronic time stamp. The proof of the actions related to the delivery of the User Content is protected by an electronic seal that excludes the possibility of altering the data. Evidence is provided to the sender and recipient as a separate electronic document in a strictly defined format (human-readable PDF format and machine-readable XML format).

## 8.1. Sender-related evidence

Upon successful identification and subsequent authentication of the sender and interaction with the Service, evidence of sending is created and may be made available to a third party. The evidence includes the exact date and time, with a timestamp, that the User Content was sent by the sender.

1. **Submission Acceptance**

The sender successfully submits the User Content to the sender's system. A date/time stamp is generated as proof that the sender has submitted a consignment to the system that has been accepted, and action is taken to deliver it to the appropriate recipient(s).

2. **Submission Rejection**

The sender submits the User Content to the sender's system. User Content has not been accepted by the sender's system. Evidence is created with the date and time that the sender submitted a content to the system, which was rejected by the system for delivery.

## 8.2. Recipient-related evidence

Upon successful identification and subsequent authentication of the recipient and interaction with the Service, proof of receipt is created and may be provided to a third party. The receipt specifies the exact date and time of receipt of the User Content.

1. **Content Consignment**

Delivery of User Content to the recipient. The content was delivered to the recipient within the specified time after the recipient was initially identified and properly authenticated.

#### 2. Content Consignment Failure

User Content cannot be delivered within the specified time due to technical errors and/or other reasons.

### 8.3. Content handover

#### 1. Content Handover

User content is delivered to the recipient at a specified date and time.

#### 2. Content Handover Failure

User Content has not been delivered to the recipient after a specified number of attempts or after a specified wait time.

## 9. ARCHIVING

BORICA archives at least the following information:
All documents and data related to the identity verification process, all requests submitted by clients, all correspondence between clients and BORICA, proof of sending, receiving and signing documents are archived.

Long-term data storage is conducted in a secure environment.

## 10. TERMINATION OF THE SERVICE

The Service can be terminated by closing the profile in the B-Trust Mobile application. Termination will be immediate.

## 11. USER OBLIGATIONS

Users shall comply with the Contract and its terms, conditions, policies and practices when using the Service, and shall use the Service only for lawful purposes.

## 12. PHYSICAL CONTROLS

Means of physical control have been implemented for the workplaces of the operators used for the processing and storage of personal data obtained through the “onboarding” process, in order to prevent unauthorized access to these places.

In addition, the Provider uses redundancy to minimize the impact of disasters. Data is not permanently stored at the identification centers.

Physical security is in accordance with the best practices of international standards and recommendations. Equipment is protected in an isolated space and physical integrity is ensured.

Access to data collection and processing is granted only to employees with appropriate roles and qualifications. Rights are granted only when the specific role has been assigned a task that requires access to personal information.

### 12.1. Access Management

All components requiring physical and logical protection of critical data and information (servers, communication devices, keys, repositories archives, etc.) are segregated in rooms and areas with high security protection. The physical and logical control of access to the B-Trust® environment/infrastructure of the QTSP is in accordance with the document "Certification Practice Statement for the Provision of Qualified Certificates and Trust Services", and is applicable to the RA-VI, as a part of the Registration Authority Department in the B-Trust PKI infrastructure of the Provider.

### 12.2. Operational Security

The operational security complies with the requirements for the security of computer systems in the B-Trust infrastructure as specified in the document "Certification Practice Statement for the Provision of Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS).

### 12.3. Network security

The Provider uses advanced technical means to protect the information exchange of the RA with the Users, with the Certification Authority, and with the means providing external services (image analysis and access to national registers) in order to ensure the network security of the systems against external interference and threats.

### 12.4. Information Security

Information security is an integral part of the B-Trust infrastructure and is subject to the general information security policy of BORICA, approved by the company management. This policy defines the organizational measures and procedures for security management of all systems and information assets, through which BORICA provides all its services. Personnel directly involved with these systems and assets are familiar with and implement this policy. Electronic documents signed/sealed with QES/QESeal may contain information that is considered personal data. In accordance with the regulations concerning this type of data, BORICA as a QTSP or as a Provider of the Service, is registered with the Personal Data Protection Commission as a personal data controller.

## 13. CONTINUITY

In accordance with the general measures taken by the Provider to ensure the uninterrupted functioning of the B-Trust infrastructure, including qualified trust services based on the redundancy of the critical components of the infrastructure.

## 14. RISK ASSESSMENT

Considering business and technical issues identified in the provision, operation and maintenance of the Service, the Provider shall conduct a risk assessment in order to identify, analyze and evaluate the associated risks.
Appropriate measures are selected to avoid identified risks, considering the results of the risk assessment. The measures taken ensure a level of security which is appropriate to the level of risk identified.

The results are reported to the operational management of BORICA, which approves the results of the risk assessment, the prescribed measures for overcoming the identified risk factors, and accepts the identified residual risk regarding the Service provided to the RPs/ESPs and their Users.
The Provider shall document the security requirements and operational procedures necessary to avoid identified risks to the onboarding process through the policy and practice statement included as part of this document.
In order to overcome the identified risk factors, periodic risk review and assessment is performed.
The results are reported to the management of BORICA, which approves the results of the risk assessment, the prescribed measures to overcome the identified risk factors, and accepts the identified residual risk with regard to the implemented "onboarding" process for remote video identification of B-Trust users.
In case of a compromise of the services, BORICA shall inform all its customers with whom it has an established relationship for providing ERDS. The information shall indicate that the proofs issued by the compromised key may no longer be valid from the time of the compromise.

## 15. INSPECTION AND CONTROL OF THE PROVIDER'S ACTIVITIES

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

## 16. BUSINESS AND LEGAL ISSUES

The Provider warrants that the RA will perform its functions and duties in full compliance with the terms of this document and the issued internal operating instructions.
The User shall comply with the terms and procedures of the onboarding process set forth in this document.
Disputes or complaints regarding the use of QERDS shall be resolved on the basis of written submissions. If the dispute is not resolved, the parties may refer the dispute to a Bulgarian court. All issues not regulated in this document shall be governed by Bulgarian legislation.