Public document

CERTIFICATE POLICY
AND CERTIFICATION PRACTICE STATEMENT
FOR THE PROVISION OF NATIONALLY QUALIFIED ELECTRONIC IDENTIFICATION SERVICE

Version 1.2

Effective: July 15, 2022

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	01.04.2021	Approved	Initial release
1.1	Margarita Boneva	01.07.2021	Approved	Edited
1.2	Margarita Boneva	15.03.2023	Approved	Edited

CONTENTS

1 ACRONYMS

REIC	Register of Electronic Identity Certificates
REI	Register of Electronic Identifiers
RA-EI	Registration Authority of Electronic Identity
ES	Electronic Service, requiring electronic identification
ESP	Electronic Service Provider, a provider of service(s) requiring electronic identification
RP	Relying Party, in particular ESP
ES	Electronic Signature
EDETSA	Electronic Document and Electronic Trust Services Act
QTSP	Qualified Trust Service Provider
QES	Qualified Electronic Signature
CQES	Cloud Qualified Electronic Signature
eID	Electronic Identifier
OCR	Optical character recognition

2 TERMS AND DEFINITIONS

Video Identification – a process of verification with subsequent validation and registration of personal data from a government- recognized ID document using video technology.

"Onboarding" process – remote video identification of a natural person.

User – a natural person who participates in the "onboarding" process and is the Holder of the QC for CQES the Holder of the electronic identity.

Customer – any third relying party that can use the "onboarding" process for remote video identification as a "cloud service" of BORICA (e.g., another TSP, financial institution - bank/insurer, etc.).

Identification data of a natural person – a set of data that allows to uniquely identify a natural person.

Official Identity Document - a valid official document containing data for unique identification (a national identifier and other data) of a natural person (identity card, international passport, foreigner's identity card and others, according to 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.

Electronic Identification Service (the Service) – infrastructure (hardware, software, protocols, interfaces, metadata) enabling the unambiguous creation, registration, and validation of the electronic identity of natural persons in a virtual (Internet) environment. The BORICA Service uses an "onboarding" process (remote video identification) and provides electronic identity verification or authentication of electronic identity as a "qualified electronic identification service".

QTSP BORICA AD – the service provider (the Provider, BORICA).

Qualified Electronic Identification Service Operator – BORICA as a registered QTSP under EDETSA performing automated electronic identity verification.

Electronic Identification Certificate (consent to provide personal data) – a formalized official electronic document represented by a generally accepted standard, issued with a fixed term of validity and containing an electronic identifier and other data; in the service of BORICA - a formalized electronic document represented by a generally accepted standard, which may contain a unique identifier, other personal data obtained from an official identity document, and may contain a graphic image of the official identity document.

Electronic Identifier – a unique identifier of a natural person for whom an Electronic Identification Certificate has been issued; in the service of BORICA the Electronic Identifier clearly and unambiguously identifies the person in the virtual environment of a domain. The Electronic Identifier is different for different domains, but it uniquely corresponds to the Electronic Identification Certificate

(i.e., it does not allow transferability of the electronic identity in the virtual environment between domains).

Electronic identity of a natural person – an electronic identifier associated with its corresponding Electronic Identification Certificate.

Electronic Identity Holder – a natural person aged 14 or over, to whom an electronic identification certificate is issued and registered through BORICA only upon the request of a Relying Party.

Authentication – the electronic process of confirming the electronic identity of the Holder through verification.

Register of Electronic Identification Certificates – a register containing the issued Electronic Identification Certificates of Users.

Register of Electronic Identifiers – a register containing generated electronic identifiers of Users, corresponding to unique civil identifiers (Personal Identification Number/Personal Foreigner's Number/ Foreigner ID).

Register of RPs/ESPs – an internal register containing data about RPs/ESPs and the electronic services provided by them – a unique identifier and other data about the RP/ESP, as well as information about required personal data of Users from their electronic identification certificates of each registered electronic service. The CEI shall inform the User about the personal data required in the electronic service before initiating the electronic identification procedure.

Registration Authority of Electronic Identity (RA-EI) – BORICA through the "onboarding" process generates and delivers a unique Electronic Identifier and Electronic Identification Certificate for Users of RPs/ESPs that require electronic identification and authentication.

Electronic Service: a service in a virtual environment that requires electronic identification of a person in order to establish the identity of the user.

Electronic Service Provider – A person who provides electronic services and acts as a Relying Party to the Electronic Identification Service. The RP/ESP concludes a contract for the Electronic Identification Service with the QTSP BORICA, and registers the electronic services it provides with BORICA. RPs/ ESPs can be:

- State authorities;
- Persons performing public functions (notaries, private bailiffs);
- Public service providers (utilities);
- Other private legal entities (banks, insurance companies, merchants, etc.)

3 SCOPE 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 15.07.2022;
- has the character of general terms and conditions within the meaning of Art. 16 of the Obligations and Contracts Act and is an integral part of the Contract for Trust Services and Electronic Identity Services (the Contract);
- contains a description of the policy and security requirements of the operator of the Qualified Electronic Identification Service (the Service) of the QTSP BORICA;
- defines the practice of the QTSP in the operation and management of the Service, in order to enable Users and Relying Parties who have concluded a contract with BORICA to obtain a description and assessment of the security of this Qualified Service;
- serves to evaluate and assess the conformity of the activity of BORICA to provide the Service in accordance with Regulation 910/2014 and with the legislation of Bulgaria;
- defines the relations of the Service with other related qualified services of the QTSP BORICA - remote identification and registration of natural persons (via video identification) for the provision of B-Trust qualified services, Cloud Qualified Electronic Signature (CQES), One-time Cloud Qualified Electronic Signature, and Qualified Electronic Seal;
- addresses the practical aspects of using the Service - registration and validation of electronic identity, and electronic authentication of natural persons by Relying Parties/ Electronic Service Providers, according to specific business objectives and scenarios;
- this document is public and may be changed by the QTSP BORICA, as each new version of the Policy and Practice Statement shall be published on the website of the QTSP – the operator of the Service.

Outside the scope of this document are:

- the legal inapplicability (rules and regulations) that do not allow the use of the "onboarding" (remote video identification and authentication of persons) for various business purposes;
- the technical aspects of the qualified electronic identification service - formats, syntax, encoding of electronic identifiers and electronic identification certificates, registers, protocols and interfaces, etc.;
- The technical elements of procedures for registration and validation of electronic identity (electronic identifier and electronic identification certificate).

4 CONFORMITY AND REFERENCES

This document has been prepared in accordance with:

- Regulation (EU) № 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Directive (EU) 2018/843 of the European Parliament and of the council of May 30, 2018 (Article 13 (1) (b) amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2 Policy and security requirements for trust service providers issuing certificates;
- the relevant applicable legislation in the Republic of Bulgaria;
- the Electronic Document and Electronic Trust Services Act (EDETSA);
- the Regulation on Liability and Termination of the Activities of Trust Service Providers;
- the Rules of Implementation of the Law on Anti-Money Laundering Measures (Art. 42);
- the Law on Anti-Money Laundering Measures (art. 55, paragraph 2).

In order to verify the compliance of the QTSP's activities with the regulations during the audit of the service, this document should be used together with other basic documents of the Provider, as follows:

- “Certification Practice Statement for the Provision of Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)”;
- “Certificate Policy for the Provision of Qualified Certificates for Qualified Electronic Signature/Cloud Electronic Signature/Seal (B-Trust CP-eIDAS QES/CQES/QESeal)”;
- Certificate Policy and Certification Practice Statement for Providing Remote Video Identification for Issuing Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS);
- General Terms and Conditions for Use of the Service "Remote Signing of Electronic Documents with Cloud QES”.

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

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

5 INTRODUCTION

5.1 Purpose

This document describes the general conditions and requirements that the QTSP BORICA fulfills within the process of electronic identification with non-presence remote video identification. The natural person - User uses the Service through an Internet browser or through a smart device (smartphone or tablet) and a mobile application on it. Through the Service the QTSP BORICA collects, verifies and validates the User's personal data (data from a legally valid official national identity document) in order to issue a unique Electronic Identifier (eID) and an Electronic Identification Certificate of the User to Relying Parties (e.g., an Electronic Service Provider/ESP). The Electronic Identifier and the associated Electronic Identification Certificate uniquely and securely identify each user in the virtual environment of an RP/ ESP.

Through this Service, any Relying Party that trusts the Qualified Service (at the national level) for identification purposes can:

- conveniently and securely create profiles with the electronic identity and perform electronic identity verification of users;
- perform direct (without supporting profiles) electronic identification and authentication of users.

The Service complies with the Regulation (EU) 914/2014 and Regulation (EU) 2016/679 (GDPR).

5.2 BORICA as a QTPS

BORICA AD is a legal entity - trader, which performs the activity of a QTSP according to EDETSA and legislation. The company builds, operates and manages Public Key Infrastructure (PKI) under the trademark B-Trust®, according to the legal framework of Regulation EU 910/2014 and the EDETSA and in accordance with the international specifications and standards: ETSI EN 319 411-1/5, and ETSI EN 319 412 related to this regulation.

As a QTSP registered in the National Trusted List of the National Regulatory Authority, the CRC, BORICA provides the following qualified certification services, in accordance with Regulation 910/2014:

- Qualified Electronic Signature (QES) of natural persons;
- Cloud Qualified Electronic Signature (CQES) of natural persons;
- One-time CQES of natural persons;
- Qualified electronic seal (QESeal) of legal persons;
- Advanced electronic signature (AES) of natural persons;
- Advanced electronic seal (AESeal) of legal persons;
- Qualified Time Stamp;
- Qualified validation of QES/QESeal/AES/AESeal, and Cloud QES;
- Qualified long-term preservation (Archive) of qualified electronically signed/sealed documents;

- Qualified signing of electronic documents with CQES;
- Non-present identification (onboarding) of Holders of CQES (for issuance of qualified signatures) – at the national level.

The remote video identification ("onboarding") has been verified and approved to provide an equivalent level of assurance as the physical presence (face-to-face) of individuals whose personal information the Provider collects, verifies and validates to certify them in the QC for CQES issued to them. The equivalent level of assurance with respect to the identification of the natural persons through "onboarding" by the Provider has been confirmed by a Conformity Assessment Body pursuant to Art. 24, paragraph 1 (d) of Regulation (EU) 910/2014.

The Service presented in this document enhances the "onboarding" process in the B-Trust infrastructure with a one-time cloud qualified electronic signature issued to a natural person, cloud qualified electronic signature, and electronic seal of the QTSP in order to provide the electronic identity of a natural person in the virtual environment of an RP/ESP.

BORICA informs Users and RPs/ESPs of its accreditation when providing Qualified Electronic Trust Services (QETS). This accreditation is in accordance with the Regulation (EU) 910/2014 and aims at the highest level of security of the provided QETS and better harmonization of the Provider's activity with the corresponding activities in the Member States of the European Union.

In the contractual relations with Users and Relying Parties, only the version of this document in force at the time of using the Service is valid.

For more information about the B-Trust infrastructure of BORICA, please refer to the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)".

5.3 Policy Identifier

The Certificate Policy and Certification Practice Statement of BORICA for the Service supplement the general Certificate Policy and Certification Practice Statement for the Provider's qualified trust services. Specifically, in this document, the Certificate Policy describes what the Provider offers to demonstrate the applicability of the Service, the terms and conditions it follows when remotely identifying, registering and authenticating Users. The Certification Practice Statement describes the operational procedures that the Provider follows to provide this Service.

The Provider's practice in providing the Service is implemented by the object **B-Trust Remote Video Identification Service (vRA)**, identified by the object identifier: **1.3.6.1.4.1.15862.1.6.10** in the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)":

Qualified service for non-presence electronic identification of natural persons or natural persons representing legal persons (the Service)	Object Identifier
Practice Statement of the Service Provider	**1.3.6.1.4.1.15862.1.6.10**

In accordance with this document, through this Practice Statement, the Provider implements a Policy of the Service with an identifier as follows:

Qualified service for non-presence electronic identification of natural persons or natural persons representing legal persons (the Service)	Policy Identifier
Policy of the of the Service Provider	**1.3.6.1.4.1.15862.1.6.10.2**

5.4 Administration of the Policy and Practice Statement

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

Amendments, revisions, and additions are permitted that do not affect the rights and obligations arising from this document and the standard trust services contract between the Provider, Users, and Relying Parties. They shall be reflected in the updated version or revision of the document after approval by the Board of Directors.

This Policy and Practice Statement should be reviewed at least annually to reflect potential requirements and prerequisites for changes in security levels for the onboarding process. Any new version or revision of this document that is submitted and approved shall be promptly posted on the Provider's website.

5.5 Applicability of the Policy and Practice Statement

This Policy and Practice Statement shall apply in accordance with the contractual relationship9 of BORICA with each individual Relying Party and holder of a qualified certificate that is subject to electronic identification. They shall also apply after the termination of the contractual relationship with the described entities until the final settlement of their obligations to BORICA.

5.6 Other Applicable Documents

This document (Policy and Practice Statement) should be used together with the following general documents of the Provider regarding B-Trust:

- “Certification Practice Statement for the Provision of Qualified Certificates and Trust Services by BORICA AD (B-Trust CPS-eIDAS)”;
- Certificate Policy for the Provision of Qualified Certificates for Qualified Electronic Signature/Cloud Electronic Signature/Seal (B-Trust CP-eIDAS QES/CQES/QESeal);

- Certificate Policy and Certification Practice Statement for Providing Remote Video Identification for Issuing Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS);
- General Terms and Conditions for Using the Service "Remote Signing of Electronic Documents with Cloud QES".

This document contains references to sections of these general documents, which are applicable to the Service in order to avoid repetition.

The screens of the identification process through an Internet browser and the B-Trust mobile application on a smart device (smartphone or tablet), through which the User participates in the "onboarding" process of electronic identification, may be useful in relation to this document.

6 QUALIFIED ELECTRONIC IDENTIFICATION SERVICE

BORICA provides qualified (at national level) Electronic Identification Service, which is the subject of this document. The Service operates on the basis of the B-trust infrastructure for qualified trust services under the EDETSA. The Service provides electronic identity to natural persons who request electronic services requiring electronic identification and/or authentication in the virtual environment of Relying Parties.

The means of electronic identification is a set of information system (backend part of BORICA and B-Trust Mobile application) and CQES issued to the Holder with which the Electronic Identification Certificate is signed – the user gives consent to data processing, consent to provide data and consent to participate in the Electronic Identification scheme.

6.1 Participants of the qualified electronic identification service

6.1.1 User/Holder of electronic identity

A user of this Service is any natural person or legal entity that has concluded a contract with BORICA for the provision of trust and electronic identity services.

An electronic identity holder is a natural person (representing him/herself or a legal entity) to whom a unique electronic identifier and a corresponding Electronic Identification Certificate are issued by the Electronic Identity Authority – BORICA. The Holder of an Electronic Identity is a User of the electronic service(s) of a Relying Party requiring electronic identification. Only a Relying Party that operates electronic services and has a contract with BORICA for a qualified electronic identification service may request the issuance of a User's Electronic Identity.

6.1.2 Identity Authority

The Register of Bulgarian Identity Documents of the Ministry of Interior is the official primary source of the national unique identifiers (Personal Identification Number / Personal Foreigner's Number) of the natural persons in the country. The Commercial Register and the Register of Non-Profit Legal Entities of the Registry Agency are official primary registers containing national unique identifiers and other data of the legal entities in the country.

These registers and other official public registers of personal data available through RegiX (a national information hub for the exchange of information between registers) act as an Identity Authority.

6.1.3 Electronic Identity Registration Authority

The QTSP BORICA performs the role of the Administrator of electronic identity (AEI) when providing the qualified electronic identification service. At the request of the Relying Party the AEI collects and verifies personal data from the official identity documents of natural persons, validates these documents and generates the electronic identity (a unique electronic identifier and an electronic identification certificate) of the natural persons through the “onboarding” process (remote video identification) of the QTSP. The AEI provides the generated electronic identity of the person to the Relying Party (Electronic Service Provider of services requiring electronic identification) or records it in the registers for subsequent electronic identification and/or authentication of the person.

The AEI shares with the CMR of the QTSP BORICA and maintains two registers – the Register of Electronic Identifiers and the Register of Electronic Identification Certificates. These registers may be maintained by a Relying Party, in accordance with its security policy.

6.1.4 Qualified Electronic Identification Service Operator

The QTSP BORICA performs the role of a Qualified Electronic Identification Service Operator. At the request of the Relying Party through the “onboarding” process (remote video identification) of the QTSP, BORICA validates the data from the official identity document of the person at the time of the request and generates (through a hash transformation) a current electronic identifier of the person (electronic identity holder) who has addressed the electronic service, and compares it with an already registered one (associated with a registered electronic identification certificate) or provides it to the Relying party/ Electronic Service Provider for verification .

BORICA maintains both registers – the Register of Electronic Identifiers and the Register of Electronic Identification Certificates. These registers may be maintained by a Relying Party, in accordance with its security policy. In addition, BORICA has established and maintains a common register of Relying Parties and the electronic services requiring electronic identification registered by them.

As part of the electronic identity validation process, BORICA may, with the express consent of the natural person/User, provide the Relying Party with other (non-personal) data, requested by the Relying party when registering for a particular electronic service.

6.1.5 Relying Parties / Electronic Service Providers

Relying Parties are companies and public institutions that provide electronic services that require the electronic identification of persons – Users – in their virtual environment (domain). BORICA offers its corporate customers – RPs/ESPs - a qualified service for electronic identification through a mobile smart device or a dedicated web page based on qualified trust services, for which the Provider is registered in the Trusted List of Qualified Trust Service Providers.

Bulgarian RPs/ESPs shall conclude contracts for integration with BORICA for the purpose of providing electronic identification services, and shall specify the requirements for the electronic services they provide. The applicability of the Electronic Identification Service is related to the authentication of personal and other data of natural or legal persons by BORICA. A Holder of an electronic identity is electronically identified and/or authenticated to a Relying Party in its domain by means of a unique electronic identifier. In different domains (i.e., virtual environments of different Relying Parties), the Holder of the Electronic Identity has different unique eIDs, but they all unambiguously correspond to his unique (i.e., the same for all domains) Electronic Identification Certificate.

6.2 Elements of the Qualified Electronic Identification Service

The electronic identification of BORICA includes a number of elements through which it provides the SERVICE to RPs/ESPs and to Users of their electronic services.

6.2.1 Electronic Identifier

The Electronic Identifier (eID) is unique data that unambiguously and securely identifies a natural person in the virtual environment of a Relying Party (Electronic Service Provider). It is automatically generated during the issuance of the Electronic Identification Certificate by means of hash transformation of a concatenated string (in order to protect against transferability of eIDs between domains/Relying parties), including:

- the data in the Electronic Identification Certificate provided through the “onboarding” process of the QTSP BORICA from a submitted official identity document, and
- a unique permanent national identifier of the RP/ESP provided by RegiX from the relevant public administrative register.

The Electronic Identifier of a natural person shall unambiguously and securely correspond to the national identifier of the person (Personal Identification Number/Personal Foreigner’s Number, passport number). A Holder of an electronic identity has different eIDs in the virtual environment of the different Relying Parties/Providers (domains).

The Electronic Identifier of a legal entity corresponds to the national unique permanent identifier, which is provided and checked for validity in the registers of the Registry Agency or in other official public registers.

The Electronic Identifier of a natural person who represents a legal entity, if the power of representation derives from the law, is his or her Electronic Identifier.

6.2.2 Electronic Identification Certificate

The Electronic Identification Certificate of a natural person - Holder of an electronic identity, is a formalized electronic document represented by a generally accepted standard (PDF-readable and JSON format), which contains and confirms at least the name or pseudonym of a particular person and may also contain the unique national identifier (Personal Identification Number/Personal Foreigner’s Number, passport number) and other personal data of the person from an official identity document, including a graphic image of the official identity document, received and verified for validity through the "onboarding" process of the QTSP BORICA. The Electronic Identification Certificate is sealed by BORICA and delivered to the Relying Party (Electronic Service Provider).

The identity of the legal entity is established based on the national identification code of the legal entity provided by the relying party during the identification. The national identifier is checked for its validity according to a reliable source (in Bulgaria - the Commercial Register and the BULSTAT Register, maintained by the Registry Agency or the Register of Non-Profit Legal Entities). Remote verification and data collection for the legal entity are performed automatically through integration with a reliable source. Based on the obtained data, an electronic identity certificate is issued.

To ensure the process of connecting the electronic identification means of natural persons and legal entities, BORICA AD has developed a technology that enables simultaneous and real-time use of electronic identification means for identity attestation of a natural person representing a legal entity and of the legal entity itself. The verification process for the legal entity’s electronic identification includes confirmation of the natural person's authority to represent the legal entity.

The process is as follows:

- When a relying party requests the identification of a legal entity, both the natural person and the legal entity identifiers are provided to the B-Trust backend to initiate the authentication process.
- The identity of the natural person is verified first, based on which an electronic identity certificate is issued to the natural person.
- The data of the legal entity (as specified in Section 5) is verified, and the system checks if the identified natural person has the authority to represent the legal entity. If the representation authority stems from the law, an automated check is performed against the relevant primary registers (reliable sources). If the authority arises from another document, such as power of attorney, contract or other legal basis, the concerned party must present themselves in person at BORICA AD.
- If no proof of representation is available or presented, the process will be canceled, and no electronic identity certificate will be issued.
- Upon successful verification, the data of the legal entity and the natural person exercising representative authority with respect to the identified legal entity is sent to the relying party.

6.2.3 Electronic Identity carrier

In the qualified electronic identification service of BORICA, the Holder of the Electronic Identity does not have a personal physical carrier on which the the issued Electronic Identifier and Electronic Identification Certificate are recorded. A natural person uses the Service (i.e., is identified and/or authenticated) to a Relying Party via an Internet browser or via a smart device with a mobile application and his/her official identity document (identity card, passport, etc.), containing the person's unique personal national identifier (Personal Identification Number/Personal Foreigner's Number, passport number). This document is the primary source of the personal data of the individual, through which the Electronic Identification Certificate and the Electronic Identifier of the Holder of the Electronic Identity are generated. They are recorded and stored in the registers of BORICA.

The registers play the role of the carrier of the Electronic Identity (eID + Electronic Identification Certificate) of the Holders of the electronic identity.

6.2.4 The "Onboarding" process

The Electronic Identification Service uses the "onboarding" process of the B-trust infrastructure of the QTSP BORICA to establish the identity of the User or Electronic Identity Holder, and his/her specific data. The "onboarding" process includes:

- verification of the real existence of the natural person;
- verification that the person is in possession of the identity document;
- verification that the person is the same as stated (in the document);
- verification of the legal validity of the identity document.

Additional information on the "onboarding" process of the BORICA QTSP and its applicability to video identification of natural persons applying for a QC for CQES is contained in the document "Certificate Policy and Certification Practice Statement for Providing Remote Video Identification for Issuance of Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS)".

6.2.5 Registers

The Electronic Identification Service of BORICA operates and maintains the following registers:

- Register of Electronic Identifiers;
- Register of Electronic Identification Certificates;
- Register of Relying Parties/ Electronic Service Providers (RPs/ESPs).

6.2.5.1 Register of Electronic Identifiers

The Register of Electronic Identifiers (eIDs) contains the unique eIDs of Electronic Identity Holders, which unambiguously correspond to the official national identifiers of natural persons, and the Electronic Identification Certificates issued to them.

The Electronic Identification Service works both with a central register of electronic identifiers and with local registers at the RPs/ESPs.

A central register of electronic identifiers is maintained to supplement the current client register (B-Trust CMR) of the QTSP BORICA, if the Security Policy of the RP/ESP allows it. Otherwise, local autonomous registers of electronic identifiers are operated and maintained at each RP/ESP for its Users –Electronic Identity Holders.

An Electronic Identity Holder has different eIDs for each RP/ESP that are uniquely associated with his/her unique Electronic Identification Certificate.

6.2.5.2 Register of Electronic Identification Certificates

BORICA stores the Electronic Identification Certificates signed by the Holder and sealed by BORICA until they are received/downloaded by the RP/ESP, but not longer than 7 (seven) days. These certificates are unique to each electronic identity holder and unambiguously determine the identity of the natural person in the virtual environment of each RP/ESP.

The RP/ESP stores the received personal data for a period determined according to the categories of personal data, the basis for their processing and the principles related to the processing of personal data, as provided for in Art. 5 of Regulation (EU) 2016/679. The RP/ESP as a personal data processor, is solely responsible for the timely deletion of the stored data.

6.2.5.3 Register of Relying Parties/ Electronic Service Providers

The Register of RPs/ESPs is a central register operated and maintained by BORICA QTSP. In this register, RPs/ESPs that have concluded a contract for the use of the Service are entered, as well as information about their electronic services that require electronic identification of users. During registration, the scope of the personal data from the Holder's Electronic Identification Certificate required for each electronic service is specified.

BORICA presents to the User the personal data required by the electronic service of the Relying Party for verification and consent before starting the electronic identification process. BORICA will initiate the electronic identification of the User/Holder only after the User's explicit consent (provided by a qualified signature through the BTrust Mobile application or by a one-time signature issued when using the Service through a dedicated web page for identification). After successfully verifying the electronic identity, the electronic service uses the User's personal data.

6.2.6 User Cloud QES and Electronic Seal of the QTSP

The qualified electronic trust services of the QTSP BORICA – one-time Cloud QES of a natural person, Cloud QES (CQES) of a natural person and qualified electronic seal (QESeal) of the QTSP BORICA participate and are used in the provision of the Service.

Natural persons – Holders of eID use their CQES or a one-time CQES issued immediately after the identification process within the Service after the successful verification of the eID to certify (consent) their personal data from the Electronic Identification Certificate to be provided to the electronic service/RP/ESP requiring electronic identification and authentication of the User. The Electronic Identification Certificate is sealed by the Service Provider's QESeal.

6.2.7 Identity Verification Web Page

When using the Service through an Internet browser, the User must go to a specific Internet address and follow the instructions, going through the identification process, as a result of which a one-time CQES will be issued, with which the User can participate and use the Service of the BORICA QTSP for an 'onboarding' process at the RP/ESP.

6.2.8 B-Trust Mobile Application

When using the Service through a smart device, the User must install and initialize the mobile application in his/her smart device in order to participate and use the Service of the BORICA QTSP for the following purposes:

- Registration of electronic identity;
- Verification of electronic identity (authentication).

7 THE SERVICE

7.1 General Characteristics

The Electronic Identification Service of BORICA enables a much safer and more reliable unambiguous identification of natural persons in a virtual environment of an RP/ESP through a mobile application on a smart device or a one-time reliable identification via an Internet browser. The identification of a person is based on a created unique electronic identity containing two permanent elements – an electronic identifier (eID) and an electronic identification certificate. When using the Service, the eID is generated each time from the data in a presented valid official identity document (for the purpose of data actuality). The Electronic Identification Certificate contains at least the name or pseudonym of the person and may contain a set of data from an official identity document.

The Service is initiated by the RPs/ESPs that have been integrated and have a contract with BORICA by sending a request for identification to BORICA.

When concluding a contract, BORICA requires the RP/ESP to specify the personal data, necessary for the RP/ESP to provide the Service to the User.

The minimum set of data for a natural person, which is provided to the RP/ESP, and which is verified in a reliable source, includes: the three names (first name, surname, last name), date of birth, national unique identifier, mobile phone number and e-mail, home address.

BORICA sends a notification to the smart device of the person in the mobile application or to a dedicated web page according to the integration of the RP/ESP, thus requesting his/her consent for identification.

Personal data from the electronic identification certificate of the Holder, who has requested an electronic service requiring electronic identification shall be provided to the electronic service only after his/her authorization (consent). A natural person/User of the Service is any person who has concluded a contract with BORICA for trust services and electronic identity services. The contract can be concluded in one of the following ways – on the spot in a BORICA office or through the mobile application after remote identification.

7.2 Terms of Use of the Service

The terms of use of the Service by RPs/ESPs are different for:

- RPs/ESPs that do not support profiles of users – electronic identity Holders.
- RPs/ESPs that support profiles of users – electronic identity Holders.

7.2.1 RPs/ESPs Not Supporting User Profiles

The RP/ESP uses the service under the following conditions:

- To have concluded a framework contract with BORICA; this Policy and Practice Statement is an integral part of the contract between the two parties;
- To possess a valid qualified website authentication certificate (SSL certificate); this certificate authenticates the RP/ESP when using the Service;
- To integrate executable code of the program interface (web services) for using the Service;
- A one-time CQES valid for the active session is issued by the QTSP BORICA to the User of the electronic service, or the issued CQES available in the B-Trust mobile application is used;
- The personal identification data of the User (a structured electronic document) is signed with the issued one-time CQES or with the CQES in the mobile application during the active session of the User with the RP/ESP.

7.2.2 RPs/ESPs Supporting User Profiles

The RP/ESP uses the service under the following conditions:

- To have concluded a framework contract with BORICA; this Policy and Practice Statement is an integral part of the contract between the two parties;
- To register in the Register of RPs/ESPs and to register the electronic services that require electronic identification and/or authentication of Users;
- To possess a valid qualified website authentication certificate (SSL certificate); this certificate authenticates the RP/ESP when using the Service;
- To integrate executable code of the program interface (web services);
- Users have a temporary client account, in which the electronic identity is registered;
- Users are Holders of the CQES or the one-time CQES, issued by the BORICA QTSP; if a User does not have a CQES, it will be issued automatically upon registration of his electronic identity;
- To successfully complete an electronic identification and/or authentication test using the test platform;

- A bilaterally signed protocol for the successful completion of the test.

A user of an electronic service of RPs/ESPs shall use the Service only if the above conditions are fulfilled.

RPs/ESPs inform their Users about the fulfillment of the specified conditions and about the way of using the Service on their websites or through the document “Electronic Identification - User's Guide”.

7.3 Applicability of the Service

The SERVICE of the BORICA QTSP is applicable to RPs/ESPs in different work scenarios:

- *Scenario I:* The user is electronically identified and uses the requested electronic service within one session. This scenario is addressed to RPs/ESPs that do not support profiles of Users/Holders of Electronic Identity.
- *Scenario II:* The user first registers an electronic identity (eID + electronic identification certificate) and can work with the requested electronic service in the same session; in subsequent transactions with this or another electronic service of this RP/ESP, the Holder of the Electronic Identity authenticates only with his/her eID (strict authentication), i.e. an electronic identity verification is performed, after which he/she has access to the electronic service; in case of a change of the eID (i.e., change of personal data) a new electronic identity of the User is generated at this RP/ESP. This scenario applies to RPs/ESPs that support User profiles.

7.3.1 Scenario I – RPs/ESPs Not Supporting User Profiles

This scenario of Service application has certain limitations, but for specific electronic services that do not require maintenance of the user profile, it is convenient for the RP/ESP and receives practical implementation (for example, in a one-time transaction for signing with one-time CQES or CQES an electronic document or a set of electronic documents).

The absence of profiles of Users of the RP/ESP does not allow the Service to register an electronic identity for them - the functionality of the Service is used in part, i.e.:

- the created electronic identity of the User exists only within an established transaction with an active operation for the specific electronic service;
- the RP/ESP (electronic service) does not use the electronic identifier of the User – Holder of Electronic Identity that permanently identifies him/her in a virtual environment;
- as a result of the execution of the electronic service, the User is electronically identified at the RP/ESP only by an electronic identification certificate; it is delivered together with the result of the active operation (e.g. signing); users are holders of a CQES issued after identification via the mobile application or a one-time CQES issued after identification via a browser;
- when the transaction is executed, it provides the electronically identified User with a CQES. A User/Holder of electronic identity can use this CQES outside the SERVICE - to sign electronic documents in any format using a smart device; the CQES is valid during the period of validity of the signature certificate;
- the Holder’s electronic identification certificate is signed with a CQES or a one-time CQES and is sealed by BORICA.

7.3.2 Scenario II –RPs/ESPs Supporting User Profiles

This scenario of using the Service allows the RPs/ESPs to use its full functionality/scope - electronic identification and registration of the profile of the Holder of Electronic Identity, as well as validation of the electronic identity (strict authentication of the Holder).

Specifically, for RPs/ESPs:

- It provides long-term preservation and maintenance of up-to-date and secure electronic identification of Users-Holders of electronic identity;
- it can be provided as a permanent electronic identity of the User, as well as other data about the person from official public registers (if the electronic service requires them); they are stored at the RP/ESP or at the QTSP BORICA;
- the electronic identification certificate is generated once and is stored in the User's profile. The Holder's eID is generated each time when the RP/ESP requires authentication (electronic identity validation);
- it registers and maintains a profile of a User- holder of an electronic identity after secure verification of the national identifiers (Personal Identification Number/Personal Foreigner's Number, passport number) and other data about the person in the database of the Ministry of Interior;
- it identifies a User - holder of an electronic identity by a permanent unique eID, which is unambiguously associated with his/her electronic identification certificate;
- the Holder of the electronic identity remains the Holder of the CQES after the termination of the electronic identity;
- a User/Holder of an electronic identity can use this CQES outside the Service - to sign electronic documents in any format using a smart device;
- the Electronic Identification Certificate is signed by the Holder and sealed by BORICA.

7.4 Functionality (Functional Model) of the Service

7.4.1 Electronic Identification and Signature in a Common Transaction

This functionality of the Service is suitable and very convenient for RPs/ESPs that do not support user profiles, but the electronic services they offer in a virtual environment require electronic identification of the User in the session with the electronic service.

Within the session, after successful electronic identification of the User, the requested electronic service is performed (for example, signing an electronic document or a set of electronic documents with the one-time CQES issued for this session). Within the transaction the RP/ESP receives an electronic identification certificate of the User together with the result of the active operation (e.g., signed document(s)).

Participation of the User in a new session with this or another electronic service of the RP/ESP generates each time his/her electronic identification certificate together with the result of the active operation of the addressed electronic service.

7.4.2 Registration and Maintenance of the Holder's Electronic Identity with the RP/ESP

This functionality of the Service allows the RPs/ESPs to register and maintain an electronic identity (eID + electronic identification certificate) in the profile of a User- Holder of an electronic identity. The

registered electronic identity is permanent until a change occurs in the personal data of the person's official identity document. Correspondingly, the change leads to automatic update (maintenance) - registration of a new electronic identity - eID and electronic identification certificate with the updated personal data.

After registration of the electronic identity in the registers of the RP/ESP or of the QTSP BORICA, the RP/ESP identifies a User- Holder of the electronic identity by his/her eID in strict two-factor authentication for accessing and working with any electronic service in the virtual environment (domain) of this RP/ESP.

7.4.3 Verification/Validation of a Holder's Electronic Identity (Authentication)

This functionality of the Service allows the RP/ESP to identify a User- Holder with an already registered electronic identity. Only after successful two-factor authentication based on the User's eID, the RP/ESP allows access to and work with an addressed electronic service in their domain. After the successful authentication of the electronic identity of the User- Holder and his consent (validation with CQES), the electronic service (i.e., the virtual environment) of the RP/ESP gets access to his personal data from the already registered electronic identification certificate.

After working with the electronic service, i.e., after completing the transaction in the virtual environment of the RP/ESP, the electronic identity of the User - Holder is preserved in the registers of the QTSP or the RP/ESP. When using this electronic service (or a new electronic service) of the RP/ESP again (i.e., in the same domain), the electronic identification certificate is generated again, but the Holder is authenticated only by his/her generated eID. In case of discrepancy between the generated eID and the one registered for the User-Holder, the generated new electronic identity with the updated personal data is stored in the registers of the QTSP or the RP/ESP). In both cases, after successful electronic identification, the User -Holder is granted access to the electronic service, and the service gets access to his/her electronic identity.

7.5 Prohibited Uses of the Service

The Service may not be used in a manner that violates the confidentiality and security of personal data, as well as the integrity and irrevocability of the data in the Electronic Identification Certificate.

7.6 Security of the Service

The security of the Service is based on the following factors:

- Security of the "onboarding" process;
- Security of the one-time CQES, the CQES, and the B-Trust electronic seal;
- Security of communication;
- Security of the identification website and the B-Trust Mobile application.

7.6.1 Security of the "Onboarding" Process

The Service uses the "onboarding" process (remote video identification) of the registration authority RA-VI in the B-Trust infrastructure of the QTSP BORICA to verify the identity of natural persons, who participate in this process of issuing electronic identity (eID + electronic identification certificate) for them. The natural person participates in the "onboarding" process through a web browser or a smart device (smartphone or tablet) and a mobile application on it. The online video identification process

is certified to provide a level of assurance equivalent to the physical (face-to-face) presence of the individuals for whom the QTSP collects, verifies and validates personal information in order to certify them in QCs for CQES and Electronic Identification Certificates issued to them. The "equivalent level" of assurance regarding the identification of natural persons through "onboarding" at the QTSP has been confirmed by a Conformity Assessment Body in accordance with Art. 24, para. 1 (d) of Regulation (EU) № 910/2014.

See the document “Certificate Policy and Certification Practice Statement for Providing Remote Video Identification for Issuing Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS)”.

7.6.2 CQES and Electronic Seal Security

The Service uses QESeal of the QTSP BORICA to seal each generated electronic identification certificate of the eID Holder.

After successful electronic identification (authentication), the Holder of eID uses the issued CQES or one-time CQES to give the RP/ESP consent to use his/her personal data from the Electronic Identification Certificate. In addition, he/she electronically signs a contract for the issued CQES.

The QES and the QESeal are qualified services and have a security level according to EDETSA and Regulation (EU) 910/2014.

See the documents: “Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)”, and “Certificate Policy on the Provision of Qualified Certificates for Qualified Electronic Signature/Cloud Electronic Signature/Seal (B-Trust CP-eIDAS QES/CQES/QESeal)”.

7.6.3 Communication security

When providing the Service, the QTSP BORICA uses advanced technical means for the exchange and protection of information between participants, as well as with the parties providing external services (video image analysis and access to national registers). In order to ensure network security against external interference and threats, the systems use Internet connectivity with two-way SSL/TLS protocol for authentication and protection of data exchange.

7.6.3.1 Service Certificates

The Service uses two certificates:

- Qualified Certificate for Qualified Electronic Seal (QC QESeal);
- Qualified Certificate for Website Authentication (QC OVC SSL/Organization).

The QC QESeal of the Service is electronically sealed with the private key of the Operational Certification Authority, B-Trust Operational Qualified CA of the Provider. The Service automatically seals each generated electronic identification certificate with the QESeal and certifies the source and data integrity ot the certificate, as well as the relationship of the creator of the seal with his public key.

The profile of the QESeal Certificate of the Service is in accordance with the document “Certificate Policy on the Provision of Qualified Certificates for Qualified Electronic Signature/Cloud Electronic Signature/Seal (B-Trust CP-eIDAS QES/CQES/QESeal)” and is specified below:

Field	Attributes	Value/Meaning
Version	-	V3

Serial number	-	[serial number]
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	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN=	[Creator Name (Common Name)]
	O =	[Creator Name (Organization or legal person)]
	2.5.4.97= (organizationIdentifier)	[Creator Identifier. One of the following: • VATBG-XXXXXXXXX – for VAT number • NTRBG-XXXXXXXXX – for UIC]
	E =	[Email]
	C =	BG or YY YY is the two-letter country code according to ISO 3166, where the Creator is registered
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[hash of „Public key "]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.194112.1.1
Enhanced Key Usage	-	Client Authentication, Secure Email

CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol 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-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Key Encipherment, Code Signing	
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-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

The QC OVC/SSL is electronically sealed by the private key of the Operational Certification Authority B-Trust Operational Advanced CA of the Provider. This certificate online authenticates the Service Provider to RPs/ESPs and maintains a secure SSL/TLS session with them.

The profile of the Certificate For Website Authentication (Organization) of the Service is in accordance with the document: “Certificate Policy on the Provision of Qualified Certificates for Website Authentication (B-Trust QCP-eIDAS QWAC)”:

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature	-	Sha256RSA

algorithm		
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	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	URL address of the SERVICE
	O =	BORICA AD
	2.5.4.97= (organizationIdentifier)	NTRBG-201230426
	OU	OV SSL
	C =	BG
Public key	-	RSA(2048 bits)
SubjectAlternativeName		URL address of the SERVICE
Subject Key Identifier	-	[hash of „Public key "]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer“]
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=1.3.6.1.4.1.15862.1.6.9.1 [3[Certificate Policy: Policy Identifier=0.4.0.19431.2.1.2 [4]Certificate Policy: Policy Identifier=2.23.140.1.2.2

		[5]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

7.6.3.2 RP/ESP Certificate

The RP/ESP should have a valid qualified website-client authentication (organization) certificate issued by the QTSP.

This certificate authenticates the RP/ESP (SSL/TLS - client) online to the Service and maintains a secure SSL/TLS session with it.

The QTSP BORICA issues certificates for website authentication (for organization), according to the document : “Certificate Policy on the Provision of Qualified Certificates for Website Authentication (B-Trust QCP-eIDAS QWAC)”.

7.6.3.3 Security and Protection at the RP/ESP

The security and protection of user profiles of Electronic Identity Holders with valid Electronic Identification Certificates, and of signed electronic documents at RPs/ESPs are subject to the security policies of those parties and are outside the scope of this Policy and Practice Statement.

The RPs/ESPs are committed to programmatically checking the validity of documents signed electronically with CQES, and, if not valid, to perform the necessary analysis of the problem.

7.6.4 Mobile Application Security

Users of RPs/ESPs using the Service should have the B-Trust Mobile application installed on a smart device (smartphone or tablet). The smart device with the mobile application shall be initialized and registered with the QTSP BORICA in order to participate in the "onboarding" process. Only after successful registration the User can acquire an electronic identity and a qualified personal certificate for CQES. The generated electronic identity (eID and electronic identification certificate) is securely protected, and the use of the CQES to authorize consent and sign electronic documents requires the Holder to enter a PIN.

Information on the use of B-Trust Mobile can be found in the document "B-Trust Mobile Operation Manual" by BORICA.

7.7 Termination of the Service

The Service is directly addressed to RPs/ESPs, therefore the framework contract for the Service is bilateral – between the RP/ESP and the QTSP BORICA. Each of the parties may terminate the contractual relationship unilaterally before the contract expires - the RP/ESP with one month's written notice and BORICA with two months' written notice.

Termination of the contractual relationship does not release the parties from fulfilling their obligations incurred prior to the termination.

BORICA may unilaterally terminate the Service without notice in the following cases:

- Failure by the RP/ESP to comply with any of the conditions for using the Service set forth in this document;
- In case of non-use of the Service by the Relying Party for a period of more than 1 year;
- In the event of bankruptcy, liquidation, transformation or dissolution of the legal entity of the RP/ESP.

7.7.1 Termination of the Service by an RP/ESP

If an RP/ESP unilaterally terminates the contract before the specified term, the QTSP BORICA shall:

- cancel the registration of the RP/ESP and its electronic services in the Register of Relying Parties;
- deregister all eIDs in the REI corresponding to the users of the electronic services of the respective ESP/RP;
- revoke the electronic identification certificates in the REIC, associated only with the revoked eIDs in the REI; the electronic identification certificates that are associated with other valid eIDs shall be retained (they identify Users of other RPs/ESPs, i.e. in other domains).

Excluded/written off eID holders shall retain their CQES issued for the Service (except for one-time CQES) for the validity period of the QCs for those electronic signatures.

7.7.2 Termination of the Service by a User

The Holder of an electronic identity may terminate the use of the Service by revoking his/her electronic identity at the RP/ESP or at the QTSP BORICA.

7.7.2.1 Revocation of Electronic Identity at RP/ESP

Through the “Revocation” procedure of the RP/ESP, the Holder of Electronic Identity terminates the electronic identity (eID and electronic identification certificate) registered for him/her. The electronic identity in the REI and in the REIC of the RP/ESP is revoked from the user database. The user account in the user database at the RP/ESP shall be kept (for the purpose of re-registration). The client account in the CMR (client database) at the QTSP associated with the CQES issued to the Electronic Identity Holder for the Service shall be kept. The revoked Electronic Identity Holder shall retain the CQES issued to him/her for the Service (if it is not a one-time CQES) for the period of validity of the QC for that electronic signature.

Through the "STOP" procedure of the RP/ESP, an Electronic Identity Holder leaves the ESP (i.e., its virtual environment) and also terminates the electronic identity registered for him/her (eID and electronic identification certificate). The electronic identity is revoked from the user database in the REI and REIC of the RP/ESP. The user account in the user database of the RP/ESP is deleted. The client account in the CMR (client database) at the QTSP associated with the issued CQES of the Holder of Electronic Identity for the Service shall be retained. The revoked Electronic Identity Holder shall retain the CQES issued to him/her for the Service (if it is not a one-time CQES) for the period of validity of the QC for that electronic signature.

7.7.2.2 Revocation of Electronic Identity at QTSP BORICA

If the electronic identity of the User is maintained at the QTSP BORICA, the Holder of the electronic identity may terminate it only by terminating the QC for CQES issued for the Service. The electronic identity (eID and the electronic identification certificate) shall be deleted from the REI and the REIC in the CMR (client register) of the QTSP for this Holder of Electronic Identity. His/her client account in the CMR shall be retained. The user account in the user database at the RP/ESP shall be retained (for the purpose of re-registration of the electronic identity).

8 OPERATING PROCEDURES

It is assumed that the portal of an RP/ESP using the Electronic Identification Service supports one or more of the following procedures within the scope of the Service:

- "*Initial registration*" – creation of an account (username, password, email, mobile phone) of a User of the RP/ESP; this procedure is outside the scope of the Service.
- "*Electronic identity registration*" – registration of the User’s electronic identity (eID and electronic identification certificate). The User is now a Holder of an electronic identity in the domain of the RP/ESP.
- "*Electronic identification without registration*" - verification of electronic identity without registering with the RP/ESP when working with an electronic service. Restricted within a session with an active operation of the electronic service (e.g., signing document(s) with CQES);

- "*Login/Authentication*" – a Holder of electronic identity works with a selected ES that requires electronic identification;
- "*Revocation"* - a User / Holder of an electronic identity at an ESP cancels the electronic identity registered for him/her. The registered electronic identity of the User is revoked - it is deleted from the REI and the REIC at the RP/ESP or at the QTSP BORICA. The user account with the QTSP and the client account at the RP/ESP are kept (for the purpose of re-registration);
- "*Exit*" - a User leaves the virtual environment of an RP/ESP. If the REI and the REIC of BORICA are not used - the registered electronic identity in the REI and the REIC at the RP/ESP is terminated. The user account at the QTSP and the client account at the RP/ESP are terminated.

The RPs/ESPs use the Service through operational procedures that are different for:

- RPs/ESPs that do not support user profiles (with electronic identity);
- RPs/ESPs that support user profiles (with electronic identity).

Note: Pre-registration (name, password, e-mail, mobile phone number) of an (unauthorized) client account with the RP/ESP is outside the scope of this document.

8.1 "*Electronic identification without registration*" Operating Procedure of RPs/ESPs without User Profiles

A User of electronic services without a profile at the RP/ESP uses the Service under the conditions specified section 7.2.1 of this document.

The Service verifies the electronic identity of the User during a session with an electronic service of the RP/ESP without registering the verified electronic identity with the ESP and/or the QTSP BORICA. The electronic identification is limited only within the session with an active operation (e.g., signing document(s) with a CQES).

The documents to be signed by the User with CQES are at the RP/ESP. If these documents need to be signed bilaterally, the RP/ESP can sign them in advance (as the first party), before the User requests the electronic service of the RP/ESP.

8.1.1 "Electronic Identification and Active Operation/ Signing of Document(s)" Transaction

The document signing session is initiated by the User of the electronic service of the RP/ESP and consists of the following steps:

1. A user requests an electronic service from the RP/ESP that requires electronic identification of the requestor.
2. The User provides the RP/ESP with personal data (Personal Identification Number/Personal Foreigner's Number, mobile phone number, e-mail).
3. The RP/ESP sends a request to the RA-EI for electronic identification of the User - the request includes the provided personal data.
4. The RA-EI checks the B-Trust-CMR (client register) for the User's data.
5. If data is available (the User is a customer of B-Trust, i.e., he/she has a CQES), the RA-EI extracts the personal data from RegiX. If no data is available, the procedure continues from step 13.

6. The RA-EI conducts the check in RegiX – “Verification of the validity of Bulgarian personal documents”.
7. The RA-EI generates a unique electronic identifier based on the extracted current personal data and the identifier of the RP/ESP.
8. The RA-EI generates an Electronic Identification Certificate (PDF-document) based on the extracted current personal data.
9. The RA-EI notifies the User (via the B-Trust MOBILE application) of the documents to be signed - PDF (Electronic Identification Certificate) and document(s) of the RP/ESP (Electronic Service), and the User’s consent to the processing and provision of personal data is requested.
10. The User – holder of the electronic identity - views the personal data (PDF) and gives consent by entering the PIN code for CQES for signing the document.
11. The RA-EI seals the generated identification certificate (PDF) as the source of the data in the certificate and for the purpose of integrity.
12. The Electronic Identification Certificate remains with the RP/ESP after the session ends.
13. If the RA-EI does not have any user data (step 4) in the B-Trust CMR/ client register (no CQES issued), the RA-EI sends an email or SMS to the User to start the B-Trust "onboarding" process.
14. The User downloads and initializes the mobile application, enters personal data (Personal Identification Number/Personal Foreigner’s Number, mobile phone number, email).
15. The User validates (with the RA-EI) the e-mail and the mobile phone number.
16. The user takes a photo an official identity document during the "onboarding" process of the RA-EI.
17. The User takes a selfie and participates in the "liveness detection" of the "onboarding" process of the RA-EI.
18. The RA-EI extracts data (via OCR) from the official identity document.
19. The RA-EI performs the check in RegiX – “Verification of validity of Bulgarian personal documents”.
20. The RA-EI extracts personal data through RegiX.
21. The RA-EI verifies the selfie with a photo from an official identity document and with a photo from RegiX.
22. The RA-EI verifies the “Liveness detection”.
23. The RA-EI issues a certificate for CQES to the User, after which **steps 5 - 11** of the procedure are performed.

For more information on signing of documents with CQES at RPs/ESPs via the B-Trust platform for CQES of the QTSP BORICA, please refer to the document "General Terms and Conditions for Using the Certification Service “Remote Signing of Electronic Documents with Cloud QES”.

8.2 Operating Procedures of RPs/ESPs with User Profiles

A user of electronic services with a profile at an RP/ESP uses the Service under the conditions specified in section 7.2.2 of this document.

The Service creates and permanently registers an Electronic Identity (eID and Electronic Identification Certificate) and/or verifies a registered one of the User during an active session with an electronic service of the RP/ESP. The registered permanent electronic identity is stored in the registers of the RP/ESP and/or the BORICA QTSP. Registration of an Electronic Identity is a one-time process when using the Service. The verification of the Electronic Identity is performed each time the holder of the Electronic Identity addresses the Electronic Service with an active operation. The holder of the

Electronic Identity is also the holder of the CQES issued upon registration of the Electronic Identity. A change in the User's personal data detected during work with the Service triggers the creation of a new Electronic Identity of the RP/ESP User.

8.2.1 "Registration of Electronic Identity" Procedure

This procedure is initiated by an RP/ESP when a User, who is not a holder of an Electronic Identity requests an electronic service requiring an Electronic Identity. The registration of the Electronic Identity at a RP/ESP and consists of the following steps:

1. A user registers at an RP/ESP, provides personal data (Personal Identification Number/Personal Foreigner's Number, mobile phone number, e-mail); the phone number and e-mail are validated by the RP/ESP.
2. The RP/ESP creates a profile with a client number, in which the personal data is recorded.
3. The user requests/chooses *"Registration of electronic identity"* at the RP/ESP.
4. The RP/ESP submits a request to the RA-EI for electronic identification of a natural person using the provided personal information.
5. The RA-EI checks the availability of the user's data in the B-Trust CMR (client register).
6. If data is available (the user is a customer of B-Trust, i.e., he/she **has a CQES**), the RA-EI extracts the personal data from RegiX.
7. The RA-EI carries out the check in RegiX – "Verification of the validity of Bulgarian personal documents".
8. The RA-EI generates a unique electronic identifier based on the extracted current data and the identifier of the RP/ESP.
9. The RA-EI stores the generated electronic identifier in the REI (a part of the B-Trust CMR).
10. The RA-EI generates an Electronic Identification Certificate (PDF document) based on the extracted current personal data.
11. The RA-EI notifies the User (via the B-Trust Mobile application) of a document to be signed – PDF (Electronic Identity Certificate), and requests the User's consent.
12. The User – holder of the Electronic Identity – views the personal data (PDF) and gives the consent by entering the PIN for CQES to sign the document.
13. The RA-EI seals the generated identification certificate (PDF) as the source of the data in the certificate and for integrity purposes.
14. The QTSP BORICA (RA-EI) stores the Electronic Identity of the User.
15. The RA-EI enters the Electronic Identity (eID and Electronic Identification Certificate) of the Holder into the registers that are part of the BTrust CMR - the client register of BORICA.
16. The RA-EI provides the RP/ESP with the personal data of the Holder of the Electronic Identity (only the data specified by the RP/ESP when registering the electronic service with BORICA). The RP/ESP may use personal data from the registered Electronic Identity of the Holder in the electronic service addressed.

8.2.1.1 Storage of the Electronic Identity by the RP/ESP

1. The RA-EI sends the Holder's Electronic Identity (eID and Electronic Identification Certificate) to the RP/ESP.
2. The RP/ESP stores the Electronic Identity in the Holder's profile.

8.2.2 "Verifying Electronic Identity (Strong Authentication)" Procedure

This procedure is initiated by the RP/ESP when a User, who is a holder of electronic identity requests an electronic service that requires electronic identification.

If the User is not an Electronic Identity Holder and the RP/ESP does not support user profiles, the scope of the user transaction includes the user's electronic identification, **verification of the established electronic identity** and performance of an active operation (e.g., signing).

If the User is an Electronic Identity Holder, the following scenarios of electronic identity verification (authentication) of the User are possible:

- The RP/ESP does not support a user profile, and the electronic identity (electronic identifier and certificate) of the user-holder is registered with the QTSP BORICA;
- The RP/ESP supports a user profile, and the electronic identity (electronic identifier and certificate) of the user-holder is registered with the RP/ESP.

Electronic identity verification (strong authentication) at the RP/ESP consists of the following steps:

8.2.2.1 Electronic Identity (Electronic Identifier and Certificate) of the User-Holder in the REI/REIC of the QTSP BORICA

Note: The REGISTERS of B-Trust CMR indicates that the RP/ESP does not support electronic identity profiles.

1. A user–holder of an electronic identity addresses an electronic service of an RP/ESP that requires electronic identification (verification).
2. The user–holder sends personal data (Personal Identification Number/Personal Foreigner's Number, mobile phone number, e-mail) to the electronic service of the RP/ESP.
3. The RP/ESP sends the personal data to the RA-EI.
4. The RA-EI checks the B-Trust CMR registers for eID and Certificates of the user-holder. If none are found, this user does not have a registered Electronic Identity – he/she should be registered.
5. The RA-EI extracts current personal data from RegiX.
6. The RA-EI performs the check in RegiX – "Verification of the validity of Bulgarian personal documents".
7. The RA-EI generates an electronic identifier based on the current personal data and the identifier of the RA-EI.
8. The RA-EI generates a certificate of electronic identity with the personal data (PDF).
9. The RA-EI notifies of a document to be signed via the B-Trust Mobile application – a consent to provide personal data to the RP/ESP.
10. The user views the PDF document and consents by signing the electronic identification certificate.
11. The RA-EI signs the PDF (electronic identification certificate with current personal data) with the user's CQES.
12. The RA-EI seals the certificate (indicating its source and integrity).
13. The RA-EI compares the generated electronic identifier with the one in the REI of the B-Trust CMR (BORICA). In case of a match - the User-Holder is authenticated at the RP/ESP, and is granted access to the electronic service. In case of mismatch, **step 15** follows.
14. The RA-EI sends personal data (from the Electronic Identification Certificate) - only those specified by the RP/ESP when registering the electronic service, or the entire certificate (PDF). The RP/ESP uses the data of the Electronic Identity Holder.
15. In case of no correspondence in **step 13**, the RA-EI invalidates the registered Electronic Identity of the User-Holder in the registers of the B-Trust CMR (BORICA).
16. The RA-EI registers the User's new current electronic identity in the registers.

8.2.2.2 The Electronic Identity (Electronic Identifier and Electronic Identification Certificate) of the User-Holder in the RP/ESP Registers

Note: The REGISTERS at the RP/ESP means that the RP/ESP supports electronic identity profiles.

1. A user-holder of an electronic identity addresses an electronic service of an RP/ESP that requires electronic identification (verification).
2. The user-holder enters his/her personal data (Personal Identification Number/Personal Foreigner's Number, mobile phone number, e-mail).
3. The RP/ESP checks for a registered Electronic Identity of the user-holder. If there is none, **the procedure in section 8.2.3.1 is performed**.
4. The RP/ESP has a registered Electronic Identity of the User-Holder. It extracts personal data from the registered Electronic Identification Certificate.
5. The RP/ESP sends the user-holder's personal data to the RA-EI.
6. The RA-EI extracts the user's current personal data from RegiX.
7. The RA-EI performs the check in RegiX – "Verification of the validity of Bulgarian personal documents".
8. The RA-EI generates an electronic identifier based on the current personal data and an RP/ESP identifier.
9. The RA-EI generates an Electronic Identification Certificate (PDF) with the personal data.
10. The RA-EI notifies the User of a document to be signed via the B-Trust Mobile application – a consent to provide personal data to the RP/ESP.
11. The user views the PDF and consents by entering the PIN of the CQES.
12. The RA-EI signs the PDF (Electronic Identification Certificate with current personal data) with the CQES of the User.
13. The RA-EI seals the certificate (an indication of its source and integrity).
14. The RA-EI returns a current Electronic Identity (Electronic Identifier and Certificate) to the RP/ESP.
15. The RP/ESP compares the generated Electronic Identifier with the one registered with it; if there is a mismatch, **step 17** follows.
16. In case of a match, the User-Holder of the electronic identity is authenticated before the RP/ESP; the User is granted access to the electronic service.
17. In case of discrepancy in **step 15,** the RP/ESP cancels/invalidates the registered Electronic Identity of the User-Holder in its registers.
18. The RP/ESP registers the User's new current electronic identity in its registers.

8.2.3 "Electronic Identity Change" Procedure

The registered Electronic Identity of an Electronic Identity Holder is permanent in time until the personal data in a valid official identification document of the person is changed. Any change in the data results in an automatic update – termination of the registered electronic identity and registration of a new electronic identity (with a generated eID and Electronic Identification Certificate based on the current personal data) of the person.

8.2.4 "Electronic Identity Revocation" and "Exit" Procedures

See section 7.7. of this document.

9 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

9.1 Physical controls

Means of physical control have been introduced for the workplaces (of the operators) used for processing and storing personal data obtained through the “onboarding” process, in order to prevent unauthorized access to these places – the RA-EI with “onboarding” process (Identification Center and Data Center/Register of Users). Only authorized persons related to the activity of implementation of procedures and functions have access to them.

In addition, the QTSP BORICA uses redundancy to minimize the effect of disasters. Data is not permanently stored in the identification centers.

See section 5.1 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

9.2 Procedural controls

BORICA implements a “role concept” which ensures that the relevant tasks and responsibilities in the ‘onboarding” process are segregated in such a way as to ensure effective control. Access to data collection and processing is granted only to employees with relevant roles and qualifications. Rights are granted only if the specific role has been assigned a task that requires such access to personal data.

For more information, see section 5.2 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

9.3 Staff qualification and training

The QTSP BORICA guarantees that the operators participating in the “onboarding” process for electronic identification via videoconference and registration have the necessary qualifications and skills. This is achieved by conducting training after the appointment of the operators and before the implementation of production operations. The training documentation is part of the human resources management system. The responsibility for conducting the training lies with the team leader and the human resources manager.

The QTSP requires from each employee the relevant documents (certificate of no criminal record, police clearance, CV, conflict of interests, credit information, etc.) to determine his/her reliability to work in the electronic identification process.

See section 5.3 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

9.4 Logging Procedures

Audit logs are generated at the RA-EI for all events related to the security of the “onboarding” process and related procedures. Where possible, security audit files are collected automatically. Where this is

not possible, an operator shall use a log, paper form or other physical mechanism. All security audit files, both electronic and non-electronic, are stored and made available during compliance audits.

See section 5.4 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

9.5 Archiving

See section 5.5 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

9.6 Cryptographic security

The electronic identification process uses pairs of asymmetric cryptographic keys, corresponding to the qualified certificates used by the Service:

- Qualified Electronic Seal – to seal each generated Electronic Identification Certificate.
- Website authentication – to authenticate the Service (Provider).
- Qualified CQES or one-time CQES - the User authorizes access to personal data (from the electronic identification certificate) and for signing electronic documents.

9.7 Management of Cryptographic Keys

In accordance with Chapter 6 (section 6.1 – 6.5) of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)”, applicable to the asymmetric key pairs of the Qualified Certificates used to provide the Service.

9.8 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 Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)”, and is applicable to the Electronic Identification Service, as a part of the B-Trust PKI infrastructure of the QTSP BORICA.

9.9 Network security

The QTSP BORICA uses advanced technical means to exchange and protect information with users, and with the means providing external services (image analysis and access to national registers) to ensure the network security of the systems used for electronic identification against external interference and threats.

9.10 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 Providing Qualified Certificates and Trust Services" (B-Trust CPS-eIDAS) (sections 6.6, 6.7, and 6.8) of the QTSP BORICA.

9.11 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.

9.12 Continuity

The QTSP BORICA ensures the continuity of operation of the provided Service by respecting and applying the general measures that ensure the continuity of operation of the B-Trust infrastructure, based on the redundancy of the critical components of this infrastructure.

9.13 Termination of Activity of the QTSP BORICA

In accordance with section 5.9 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

10 RISK ASSESSMENT

Considering identified business and technical problems in the provision, operation and maintenance of the Service, the QTSP BORICA performs risk assessment in order to identify, analyze and evaluate the associated risks.
The QTSP BORICA documents the requirements for safety and operational procedures necessary to avoid identified risks with the provided Service. Periodically, risk review and assessment are performed in order to overcome the identified risk factors.
Appropriate measures are selected to avoid identified risks, considering the results of the risk assessment. The measures taken ensure a level of security that is appropriate to the level of identified risk.

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.

11 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

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

12 BUSINESS AND LEGAL ISSUES

The QTSP BORICA is responsible and guarantees that it complies with the conditions of this document, the requirements of EDETSA, and the regulations when carrying out the activity of a registered QTSP.

The RPs/ESPs using the Electronic Identification Service should inform and/or provide this document to their customers – users of the Service. The user must strictly follow the conditions and the procedures of the "onboarding" process, which are identical to those of the issuance of QC for CQES according to the document "B-Trust Registration Authority for Video Identification / B-Trust RA-VI CPS /CP -eIDAS ", as well as the respective Certificate Policy for the use of CQES.

Detailed information on business conditions and legal aspects of the relationship between the QTSP BORICA and the users of certification services, is contained in section 10 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).