Public document

CERTIFICATE POLICY
AND CERTIFICATION PRACTICE STATEMENT
OF THE QUALIFIED TRUST SERVICE PROVIDER
BORICA AD
FOR PROVIDING QUALIFIED
ELECTRONIC IDENTIFICATION SERVICE

Version 1.1

Effective from: 01 July 2021

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

CONTENTS

1 ACRONYMS

REIC	Register of Electronic Identity Certificates
REI	Register of Electronic Identifiers
AEI	Administrator of Electronic Identity
CEI	Center for Electronic Identification
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
CRC	Communications Regulation Commission
QC	Qualified Certificate
QES	Qualified Electronic Signature
QTS	Qualified Trust Services
CQES	Cloud Qualified Electronic Signature
SA EG	State Agency "Electronic Governance”
eID	Electronic Identifier

2 TERMS AND DEFINITIONS

Video Identification – a process of verification with subsequent validation and registration of personal data from a nationally approved identity document through video technology.

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

User – a natural person participating in the "onboarding" process and is the Titular of the QC for CQES, respectively the Titular of electronic identity.

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

Natural person's identification data – a set of data enabling the identity of a natural person to be unambiguously established.

Official identity document - a valid official document containing data for unique identification (national identifier and other data) of a natural person (identity card, international passport, foreigner 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) with official primary data.

Electronic Identification Service (the Service) – infrastructure (hardware, software, protocols, interfaces, metadata), which allows to unambiguously generate, register and validate the electronic identity of natural persons in a virtual (Internet) environment. The Service of BORICA uses an "onboarding" process (video identification from a distance) and provides electronic identity verification, respectively authentication of electronic identity as "qualified electronic identification service".

QTSP BORICA – the Provider of the SERVICE

Qualified Electronic Identification Service Operator – BORICA as a registered QTSP under the EDETSA

Electronic Identity Certificate: a formalized official electronic document represented through a generally accepted standard, issued with a fixed term of validity and containing an electronic identifier and other data; within the service of BORICA - a formalized electronic document represented through a generally accepted standard containing a unique identifier, other personal data obtained from an official identity document, including a graphic image of the official identity document and verified for validity through an "onboarding" process.

Electronic identifier: a unique identifier of a natural person for whom an electronic identity certificate has been issued; within the service of BORICA the electronic identifier unambiguously and uniquely identifies the person in the virtual environment of a domain. For various domains the electronic identifier is different, but uniquely corresponds to the electronic identity certificate (i.e. does not allow transferability of electronic identity in a virtual environment between domains).

Electronic identity of a natural person - an electronic identifier associated with its corresponding electronic identity certificate.

Titular of electronic identity: a natural person aged 14 and over, to whom an electronic identity certificate is issued and registered through the Administrator of Electronic Identity BORICA only at the request of a Relying Party.

Authentication – electronic process, through which the electronic identity of the Titular is certified by means of a verification.

Register of electronic identity certificates – an internal register, containing the issued electronic identity certificates of Users; BORICA may support a central REIC to the B-Trust CMR (the client register of BORICA - AEI/CEI) or a local register of a RP/ ESP, if a relying party does not wish to store electronic identities of their Users.

Register of electronic identifiers – an internal register, which contains generated electronic identifiers of Users, corresponding to unique civil identifiers (Personal Identification Number/Personal Foreigner's Number/ Foreigner ID); BORICA may support a central REI to the B-Trust CMR (the client register of BORICA - AEI/CEI or a local register of a RP (ESP), if a relying party does not wish to store electronic identifiers of their Users.

Register of RPs/ESPs – an internal register, which contains data about RPs/ESPs and the electronic services provided by them – a unique national and other data about the RP/ESP, as well as information about required personal data of Users from their electronic identity 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.

Administrator of Electronic Identity – BORICA/AEI is an Administrator of electronic identity and through the "onboarding" process it generates and delivers a unique electronic identifier and electronic identity certificate for Users of RPs/ESPs, requiring electronic identification and authentication.

Center for Electronic Identification: performs automated verification of electronic identity.

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

Electronic Service Provider – A person who provides electronic services and is in the role of a Relying Party to the electronic identification service. The ESP concludes a contract with the QTSP BORICA for the electronic identification service, and registers at BORICA/the CEI the electronic services provided by them. ESPs can be:

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

3 SCOPE AND USE

This document:

- has been developed by "BORICA" AD (hereinafter, BORICA), a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- is effective as of 01.07.2021;
- has the character of general conditions within the meaning of Art. 16 of the Law of Obligations and Contracts and is an integral part of the Certification Services Contract (the Contract);
- includes 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 operating and managing the SERVICE in order to allow Users and Relying Parties who have concluded a contract with BORICA to receive a description and assessment of the security of this qualified service;
- serves for evaluation and conformity assessment of the activity of BORICA to provide the SERVICE in accordance with Regulation 910/2014 and with the legislation of Bulgaria;
- determines the relations of the SERVICE with other qualified services of the QTSP BORICA - identification and registration of natural persons from a distance (via video identification) in providing B-Trust qualified services, cloud qualified electronic signature (CQES), one-time cloud qualified electronic signature, and qualified seal;
- addresses the practical aspects of applicability of the SERVICE - registration and validation of electronic identity, as well as electronic authentication of natural persons by Relying Parties/ Electronic Service Providers, according to specific business aims and scenarios;
- is public and may be changed by the QTSP BORICA, as each new version of this Policy and Practice 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) not allowing the use of the "onboarding" (video identification and authentication of persons from a distance) for various business purposes;
- the technical aspects of the qualified electronic identification service - formats, syntax, electronic identifier and electronic identity certificate coding, registers, protocols and interfaces, etc.;
- The technical elements of procedures for registration and validation of electronic identity (electronic identifier and electronic identity 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 27 April 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 30 May 2018 (art. 13, para 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 certificate;
- with the relevant applicable legislation in the Republic of Bulgaria;
- The Electronic Document and Electronic Trust Services Act (EDETSA);
- The Ordinance on Liability and Termination of Trust Service Providers;
- The Implementing Rules of Measures Against Money Laundering Act (Art. 42);
- The Measures Against Money Laundering Act (art. 55, para. 2).

In order to ascertain compliance of the activity of the QTSP with the regulations in audit of the SERVICE, this document should be used together with other fundamental documents of the Provider, as follows:

- “Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)”;
- “Certificate Policy on 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 Issuance of Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS);
- General terms and conditions for using the certification service "Remote signing of electronic documents with cloud QES”.

For additional information related to this document, please contact the Provider at:

41 “Tsar Boris III” Blvd.

1612 Sofia

BORICA AD

Tel.: 0700 199 10

E-mail: info@borica.bg

Official Website: www.b-trust.bg

5 INTRODUCTION

5.1 Subject

This document describes the general conditions and requirements that the QTSP BORICA complies within the process of electronic identification with non-presence remote video identification in the roles of an Administrator of Electronic Identity (AEI) and a Center for Electronic Identification (CEI). The natural person - user uses the SERVICE through an internet browser or via a smart device (smartphone or tablet) and a mobile application on it. Through the Service the QTSP BORICA collects, verifies and validates 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 identity certificate of the User before Relying Parties (e.g. an Electronic Service Provider/ESP). The electronic identifier and its corresponding electronic identity certificate unambiguously and securely identify each User in a virtual environment of a RP/ ESP.

Through this SERVICE, any Relying Party that trusts the Qualified Service for identification purposes:

- creates profiles with the electronic identity and performs verification of the electronic identity of Users conveniently and securely;
- performs direct (without supporting profiles) electronic identification and authentication of Users.

The SERVICE is in accordance with the Regulation (EU) 914/2014 and Regulation (EU) 2016/679 (GDPR).

5.2 The QTSP BORICA

BORICA AD is a legal entity - merchant, carrying out activity of a QTSP according to the EDETSA and the legislation. The company builds, operates and manages public key infrastructure (PKI) under the B-Trust® trademark, 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 regarding this Regulation.

As a registered QTSP 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-presence identification (onboarding) of Titulars of CQES (for issuing qualified signatures).

The remote video identification ("onboarding") has been verified and approved for equivalent assurance as the physical presence (face-to-face) of persons to whom the Provider collects, verifies

and validates their personal data to certify them in the QC for CQES issued for them. The equivalent level of assurance regarding the identification of the natural persons through "onboarding" by the Provider has been confirmed by a Conformity Assessment Body pursuant to Art. 24, para. 1 (d) of Regulation (EU) 910/2014.

The SERVICE presented in this document upgrades the “onboarding” process in the B-Trust infrastructure with 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 a RP/ESP.

BORICA shall notify Users and RPs/ESPs of its accreditation on the provision of qualified electronic certification services (QECS). This accreditation is in accordance with the Regulation and aims at the highest level of security of the provided QECS and better harmonization of the activity of the Provider with the corresponding activities in the member states of the European Union.

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

For additional information about the B-Trust infrastructure of BORICA see 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 the QTSP BORICA regarding the SERVICE supplement the general Certificate Policy and Certification Practice Statement for the qualified certification services provided by the Provider. Specifically, for this document, the Certificate Policy describes the applicability of the "onboarding" process, sets out the conditions, and rules it adheres to when remotely identifying and registering Users. The Certification Practice Statement describes the operational procedures that the Provider follows to provide this SERVICE.

The Provider's practice in providing remote/online video identification 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 of the Provider of the SERVICE	**1.3.6.1.4.1.15862.1.6.10**

In accordance with this document, through this Practice, 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 Provider of the SERVICE	**1.3.6.1.4.1.15862.1.6.10.2**

5.4 Management of the Policy

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.

Changes, revisions, and additions are allowed, which do not affect the rights and obligations arising from this document and the standard contract for certification services between the Provider and the Users/Relying Parties. They are reflected in the new 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 submitted and approved new version or revision of this document shall be immediately published on the Provider's website.

5.5 Applicability of the Policy and Practice Statement

This Policy and Practice Statement shall apply according to the contractual relationships of BORICA with each separate Relying Party. They shall also apply after the termination of the contractual relationships with the Relying Party 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 on 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 Issuance of Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS);
- General conditions for using the certification service "Remote signing of electronic documents with cloud QES”.

This document contains references to chapters/sections of these general documents, which are applicable to the SERVICE, to avoid recurrences.

The screens of the process of identification 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, can be useful regarding this document.

6 QUALIFIED ELECTRONIC IDENTIFICATION SERVICE

BORICA provides qualified electronic identification service, subject of this document. The SERVICE functions on the basis of the B-trust infrastructure for qualified trust services under the EDETSA. The SERVICE provides electronic identity to natural persons who address e-services requiring e-identification and/or authentication in the virtual environment of Relying Parties.

6.1 Participants in the qualified electronic identification service

6.1.1 Titular of electronic identity

Titular of electronic identity is a natural person (representing himself/herself or a legal person), to whom a unique electronic identifier and a corresponding certificate for electronic identity are issued through the Administrator of Electronic Identity, BORICA. The Titular of Electronic Identity is a User of electronic service(s) requiring electronic identification of a Relying Party. Only a Relying Party, which operates such electronic services, and which has concluded a contract with BORICA for qualified electronic identification service may request the issuance of an electronic identity of the User.

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, which contain national unique identifiers and other data of the legal entities in the country.

These registers and other official public registers with personal data available through RegiX (a national information hub for inter-register exchange) act as an Identity Authority.

6.1.3 Administrator of Electronic Identity

The QTSP BORICA performs the role of Administrator of electronic identity (AEI) when providing the qualified electronic identification service. At the request of the Relying Party through the "onboarding" process (video identification from a distance) of the QTSP, the AEI collects and verifies personal data from official identity documents of natural persons, validates these documents and generates electronic identity (a unique electronic identifier and electronic identity certificate) of the natural persons. 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 can be maintained by a Relying Party, in accordance with its security policy.

6.1.4 Center for Electronic Identification

The QTSP BORICA performs the role of a Center for electronic identification. At the request of the Relying Party through the "onboarding" process (video identification from a distance) of the QTSP, the CEI validates at the time of the request the data from the official identity document of the person, and generates (through a hash transformation) an up-to-date electronic identifier of the person (Titular of electronic identity), who has addressed the electronic service, and compares it or provides it to the Relying party/ Electronic Service Provider for verification with an already registered one (associated with a registered electronic identity certificate.

The CEI 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 can be maintained by a Relying Party, in accordance with its security policy. In addition, the CEI implements and maintains a common register of the Relying Parties and of the electronic services registered by them that require electronic identification.

Within the electronic identity validation procedure, the CEI may provide other data (except for personal) to the Relying Party, requested by it at the registration for a specific electronic service.

6.1.5 Relying Parties / Electronic Service Providers

Relying Parties are business and public entities providing electronic services that require electronic identification of persons – Users, in their virtual environment (domain). They conclude contracts with BORICA for the SERVICE, they are registered at the CEI and specify the requirements for the electronic services provided by them. A Titular of electronic identity is electronically identified and/or authenticated before a Relying party through a unique electronic identifier in its domain. In different domains (i.e., virtual environments of different Relying Parties) the Titular of Electronic Identity has different distinctive eIDs, but they all unambiguously correspond to his unique (i.e. the same for all domains) electronic identity certificate.

6.2 Elements of the Qualified Electronic Identification Service

The electronic identification of BORICA includes a set 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 an individual in the virtual environment of a Relying Party (Electronic Service Provider). It is generated automatically by the AEI upon issuing an electronic identity certificate by hash transformation of a concatenated string (in order to protect against transferability of eIDs between domains/Relying parties), including:

- the data in the electronic identity certificate, which are delivered through the “onboarding” process of the QTSP BORICA from an official identity document, and
- a unique permanent national identifier of the RP/ESP delivered through RegiX from the respective public administrative register.

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

The electronic identifier of a legal person corresponds to the national unique permanent identifier, which is delivered and verified for validity in the registers of the Registry Agency or in other official public registers.

The electronic identifier of a natural person representing a legal entity, when the representative power derives from law, is his/her electronic identifier.

6.2.2 Electronic identity certificate

The electronic identity certificate of a natural person - Titular of electronic identity, is a formalized electronic document represented through a generally accepted standard (PDF-readable and JSON

format), containing 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 (AEI). The electronic identity certificate is sealed by the AEI (BORICA) and provided for storage at the Relying Party (Electronic Service Provider). The electronic identity certificate is a long-term valid document until change of personal data in it (except for the national permanent identifier).

A titular of an electronic identity has **identical** copies of the certificate of electronic identity at each Relying Party/Electronic Service Provider registered at the CEI, but different electronic identifiers.

6.2.3 Electronic Identity carrier

In the qualified electronic identification service of BORICA, the Titular of Electronic Identity does not have a personal physical carrier, where the AEI records the issued electronic identifier and electronic identity certificate. A natural person uses the SERVICE (i.e., is identified and/or authenticated) before a Relying Party through an internet browser or through a smart device with Mobile application and his/her official identity document (identity card, passport, etc.), containing the unique personal national identifier of the person (Personal Identification Number/Personal Foreigner's Number, passport number). This document is the primary source of personal data of the individual, through which the AEI generates the electronic identity certificate and the electronic identifier of the Titular of Electronic Identity. They are recorded and stored in registers of the Relying Party or of BORICA (the CEI).

The registers perform the role of carrier of electronic identity (eID + certificate of electronic identity) of the Titulars of electronic identity.

6.2.4 "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, respectively the Titular of electronic identity, and his/her specific data. The "onboarding" process includes:

- verification of the actual existence of the natural person;
- verification of possession of the identity document by that person;
- verification that the person is the same as indicated in the document);
- verification of the legal validity of the identity document.

Additional information on the "onboarding" process of the QTSP BORICA and its applicability in video identification of individuals applied 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 identity 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 Titulars of electronic identity generated by the AEI, which unambiguously correspond to the official national identifiers of natural persons and of the electronic identity certificates generated for them.

The electronic identification service operates both with a central register of electronic identifiers and with local ones at the RPs/ESPs.

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

A Titular of Electronic Identity has different eIDs for each RP/ESP, which are unambiguously associated with his/her unique electronic identity certificate.

6.2.5.2 Register of electronic identity certificates

The Register of electronic identity certificates stores the valid electronic identity certificates generated by the AEI. These certificates are unique to each Titular of electronic identity and unambiguously determine the identity of the natural person in the virtual environment of each RP/ESP.

A Titular of electronic identity has a single unique electronic identity certificate registered, which is unambiguously associated with the different eIDs of the Titular for different RPs/ESPs (domains).

6.2.5.3 Register of Relying Parties/ Electronic Service Providers

The Register of RPs/ESPs is central and is operated and maintained by the CEI of the QTSP BORICA. In this register RPs/ESPs, which have concluded a Contract for use of the SERVICE are entered, as well as information about their electronic services requiring electronic identification of Users. Upon registration, the scope of the personal data from the Electronic Identity Certificate of the Titular required by each electronic service is specified. The CEI present to the User the required by the ES personal data before starting the electronic identification procedure. Only after User's consent (given by signature with a valid CQES) the CEI initiate the electronic identification of the User/Titular. After a successful verification of the electronic identity, the electronic service uses his or her data.

6.2.6 Cloud QES of a User 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 the qualified electronic seal (QESeal) of the QTSP BORICA participate and are used in providing the SERVICE.

Natural persons – Titulars of eID use their CQES or a one-time CQES issued immediately after the identification process within the SERVICE after a successful verification of the eID to certify (give consent) their personal data from the electronic identity certificate to be provided to the electronic service, which has required electronic identification, and respectively the authentication of the User.

The Provider of the SERVICE uses QESeal to seal the generated electronic identity certificate as a valid electronic document for electronic identification in a virtual environment with secure integrity and origin of delivery of the certificate.

6.2.7 Identity verification website

Users use the SERVICE through an internet browser. They have to access a specific internet address and follow the instructions passing through the identification process as a result of which a one-time CQES will be issued with which to participate and use the SERVICE of the QTSP BORICA for electronic identity registration.

6.2.8 Mobile Application

Users use the SERVICE via a smart device. They have to install and initialize the mobile application in the smart device to participate and use the SERVICE of the QTSP BORICA for:

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

7 SERVICE

7.1 General Characteristics

The electronic identification SERVICE of BORICA allows much more secure and reliable unambiguous identification of natural persons in a virtual environment of a RP/ESP through an internet browser or via a mobile application on a smart device. The identification of the person is based on a created unique electronic identity including two permanent elements – an electronic identifier (eID) and an electronic identity 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 updating the data). An electronic identity certificate is a long-term structured electronic document containing the data from an official identity document. Only after a change of data in the official identity document a new certificate is generated.

The SERVICE is always initiated by the RPs/ESPs, integrated and concluded a contract with BORICA. Personal data from the electronic identity certificate of the Titular, who has requested an electronic service requiring electronic identification shall be provided to the electronic service only after authorization (giving consent) by him.

The SERVICE is intended for RPs/ESPs, and their Users use it conveniently, easily and securely, through a browser or via a mobile application, having only a valid official identity document.

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 – Titulars of electronic identity.
- RPs/ESPs that support profiles of Users – Titulars of electronic identity.

7.2.1 RP/ESP not supporting User profiles

The RP/ESP uses the SERVICE subject to the following conditions:

- To have concluded a Framework Agreement with BORICA; this Policy and Practice Statement of the Provider are an integral part of the contract between the two parties;
- To have 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) to use the Service;
- A one-time CQES valid for the active session is issued by the QTSP BORICA to a 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) are signed with the issued one-time CQES or with the CQES in the mobile application - within the active session of the User with the RP/ESP.

7.2.2 RP/ESP supporting User profiles of Titulars of electronic identity

The RP/ESP uses the SERVICE subject to the following conditions:

- To conclude a Framework Agreement with BORICA; this Policy and Practice Statement of the Provider are an integral part of the contract between the two parties;
- To register in the Register of RPs/ESPs and to register the electronic services requiring electronic identification and/or authentication of Users;
- To have 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);
- The Users have a temporary client account, in which electronic identity is registered;
- The Users are Titulars of the CQES or the one-time CQES, issued by the QTSP BORICA; if a User does not have a CQES, it is issued automatically upon registration of his electronic identity;
- To perform a successful test for electronic identification and/or authentication through the test platform;
- A bilaterally signed Protocol for successfully completed test.

A User of electronic service of RPs/ESPs uses the SERVICE only if the above conditions are met.

RPs/ESPs shall notify their Users of the fulfillment of the specified conditions and about the way of using the SERVICE on their websites or through a document “Electronic identification - User's Guide”.

7.3 SERVICE Applicability

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

- *Scenario I:* The user is electronically identified and uses the electronic service addressed by him within one session. This scenario addresses RPs/ESPs not supporting profiles of Users/Titulars of Electronic Identity.
- *Scenario II:* The user initially registers an electronic identity (eID + electronic 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 Titular of Electronic Identity only authenticates (strict authentication) using his/her eID, i.e. an electronic identity verification is performed, after which he/she has access to the electronic service; in case of change of eID (i.e., change in personal data) a new electronic identity of the User is generated at this RP/ESP. This scenario addresses RPs/ESPs supporting profiles of Users - Titulars of electronic identity.

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 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 Users of RP/ESP does not allow the SERVICE to register an electronic identity for them - the functionality of the SERVICE is used in part, namely:

- 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 – Titular 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 through an electronic identity certificate; it is provided together with the result of the active operation (e.g. signing);
- the Users are Titulars of a CQES issued via the mobile application or a one-time CQES via identification through a browser;
- upon the transaction execution it provides a CQES to the electronically identified User;
- a User/Titular of electronic identity can use this CQES outside the SERVICE - to sign electronic documents in any format via a smart device; the CQES is valid during the period of validity of the signature certificate;
- the electronic identity certificate of the Titular is signed with a CQES or a one-time CQES and is sealed by its provider BORICA.

7.3.2 Scenario II –RPs/ESPs supporting User profiles

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

Specifically, for the RPs/ESPs:

- It provides long-term preservation and maintains updated and secure electronic identification of Users-Titulars of electronic identity;
- it can be provided as 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 in the REI and the REIC at RPs/ESPs or at the QTSP BORICA.;
- the electronic identity certificate is generated once and is stored in the User's profile. The eID of the Titular is generated when the RP/ESP requires authentication (validation of electronic identity);
- it registers and maintains a profile of a User- Titular of electronic identity in the REI and the REIC 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 - Titular of electronic identity through a permanent unique eID, unambiguously associated with his/her electronic identity certificate;
- the Titular of electronic identity remains a Titular of the CQES after termination of the electronic identity;
- a User/Titular of Electronic Identity can use this CQES outside the SERVICE - to sign electronic documents in any format via a smart device ;
- the Electronic Identity Certificate is signed by the Titular and sealed by the Provider (BORICA).

7.4 Functionality (functional model) of the SERVICE

7.4.1 Electronic identification and signing in a common transaction

This functionality of the SERVICE is suitable and very convenient for RPs/ESPs, which 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 a certificate of electronic identity of the User together with the result of the active operation (for example, signed document(s)).

A participation of the User in a new session with this or another electronic service of the RP/ESP shall generate each time his/her electronic identity certificate together with the result of the active operation of the addressed electronic service.

7.4.2 Registration and maintenance of electronic identity of the Titular at the RP/ESP

This functionality of the SERVICE allows the RPs/ESPs to register and maintain an electronic identity (eID + electronic identity certificate) in the profile of a User- Titular of electronic identity. The registered electronic identity is permanent until a change in the personal data of the official identity document of the person occurs. Respectively, the change leads to automatic update (maintenance) - registration of a new electronic identity - eID and electronic identity certificate with the updated data of the person.

After registration of the electronic identity in the REI and the REIC of the RP/ESP or of the QTSP BORICA, the RP/ESP identifies a User- Titular of electronic identity through his/her eID in strict two-factor authentication for access and work with each electronic service in the virtual environment (domain) of this RP/ESP.

7.4.3 Verification/Validation of electronic identity of a Titular (Authentication)

This functionality of the SERVICE allows the RP/ESP to identify a User- Titular with already registered electronic identity. Only after successful authentication via two-factor mechanism based on the eID of the User, the RP/ESP allows access and work with an addressed electronic service in their domain. After the successful authentication of the electronic identity of the User- Titular 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 identity certificate.

After working with the electronic service, i.e. completion of the transaction in the virtual environment of the RP/ESP, the electronic identity of the User - Titular is preserved (in the REI and the REIC). When using again this electronic service (or a new electronic service) of the RP/ESP (i.e., in the same domain), the electronic identity certificate is generated again, but the Titular is authenticated only through his/her generated eID. In case of discrepancy of the generated eID with the registered one for the User-Titular, the created new electronic identity with the updated personal data is stored in the REI/REIC (at the QTSP or the RP/ ESP). After successful electronic identification, in both cases the User -Titular gets access to the electronic service, and it has access to his electronic identity certificate.

7.5 Prohibited use of the SERVICE

The SERVICE must not be used in a way that violates the confidentiality and security of personal data, as well as the integrity and irrevocability of the data in the electronic identity certificate.

7.6 SERVICE security

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 electronic seal of B-Trust;
- Communication security;
- security of the website for identification and 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 identity 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 for an equivalent level of assurance as a physical presence (face-to-face) of the persons for whom the QTSP collects, verifies and validates personal data in order to certify them in issued for them QCs for CQES and electronic identity certificates. The "equivalent level" of assurance regarding the identification of natural persons through "onboarding" at the QTSP has been confirmed by a Conformity Assessment Body pursuant to 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 Issuance of Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS)”.

7.6.2 Security of CQES and electronic seal

The SERVICE uses QESeal of the QTSP BORICA to seal each generated electronic identity certificate of the eID Titular.

After successful electronic identification (authentication), the Titular of eID uses the issued CQES or one-time CQES to give consent to the RP/ESP to use his/her personal data from the electronic identity certificate. Additionally, he/she electronically signs a contract for the issued CQES.

QES and QESeal are qualified services and have security level in accordance with the 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

The QTSP BORICA uses advanced technical means when providing the SERVICE for exchange and protection of information between participants, as well as with the parties providing external services (analysis of video images and access to national registers). To ensure network security against external interventions and threats, the systems use Internet connectivity with two-way SSL/TLS protocol for authentication and protection in data exchange between them.

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 SEAL 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 with the QESeal each generated electronic identity certificate and certifies the source and integrity of the data in this certificate, as well as the relation 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 Provider of the SERVICE to RPs/ESPs and services a secure SSL/TLS session with them.

The profile of the certificate for website authentication (organization) of the SERVICE is according to 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 algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[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 certificate for website-client authentication (organization) issued by the QTSP.

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

The QTSP BORICA issues website authentication certificates (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 Titulars of Electronic Identity with valid electronic identity certificates, as well as of signed electronic documents at RPs/ESPs are subject to the Security Policy of these parties and are outside the scope of this Policy and Practice Statement.

The RPs/ESPs shall undertake to programmatically check the validity of documents electronically signed with CQES, and if it is not valid to make the necessary analysis of the problem.

7.6.4 Mobile Application Security

Users of RPs/ESPs who use the SERVICE should have the B-Trust Mobile application installed on a smart device (smartphone or tablet). The smart device with the mobile application is initialized and registered with the QTSP BORICA for participation 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 identity certificate) is securely protected, and the use of the CQES to authorize consent and sign electronic documents requires the Titular to enter a PIN.

Information on the use of B-Trust Mobile is contained in the document "B-Trust Mobile Operation Manual" of BORICA.

7.7 Termination of the SERVICE

The SERVICE directly addresses RP/ESP, therefore the Framework Agreement for the SERVICE is bilateral – between a RP/ESP and the QTSP BORICA. Each of the parties may unilaterally, before the term of the Agreement, terminate the contractual relations – the RP/ESP by one month’s written notice, and BORICA by two months’ notice.

Termination of the contractual relationship does not release the parties from performance of their obligations incurred before the termination.

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

- In case of non-fulfillment of any of the conditions for use of the SERVICE according to this document by the RP/ESP;
- In case of non-use of the SERVICE by the RELYING PARTY for a period of more than 1 year;
- Upon initiation of insolvency, liquidation, transformation or termination of the legal entity of the RP/ESP.

7.7.1 SERVICE Termination by RP/ESP

When a RP/ESP unilaterally terminates the Contract before the term specified in it, the QTSP BORICA:

- revokes the registration of the RP/ESP and its electronic services in the Register of Relying Parties;
- deregisters all eIDs in the REI, corresponding to the Users of electronic services of the respective ESP/RP;

- writes off the electronic identity certificates in the REIC, associated only with the written off eIDs in the REI; the electronic identity certificates that are associated with other valid eIDs are retained (they identify Users of other RPs/ESPs, i.e., in other domains).

Excluded / written off Titulars of eID keep their CQES issued for the SERVICE (except for one-time CQES) for the period of validity of the QCs for these electronic signatures.

7.7.2 SERVICE termination by User

A Titular of electronic identity may terminate the use of the SERVICE by canceling his/her electronic identity at the RP/ESP or at the QTSP BORICA.

7.7.2.1 Revocation of Electronic Identity at a RP/ESP

Through the “Revocation” procedure of the RP/ESP, the Titular of Electronic Identity terminates the electronic identity registered for him/her (eID and electronic identity certificate).The electronic identity is revoked in the REI and the REIC of the RP/ESP from the user database. The user account in the user database at the RP/ESP is kept (for the purpose of new registration). The client account in the CMR (client database) at the QTSP related with the issued CQES of the Titular of Electronic Identity for the SERVICE is retained. The excluded Titular of Electronic Identity retains 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 this electronic signature.

Through the "STOP" procedure of the RP/ESP, the Titular of Electronic Identity leaves the ESP (i.e., their virtual environment) and also terminates the electronic identity registered for him/her (eID and electronic identity certificate). The electronic identity is revoked in the REI and the REIC of the RP/ESP from the user database. The user account in the user database at the RP/ESP is deleted. The client account in the CMR (client database) at the QTSP related with the issued CQES of the Titular of Electronic Identity for the SERVICE is retained. The excluded Titular of Electronic Identity retains the CQES issued to him/her for the SERVICE (if it is not a one-time OKEP) for the period of validity of the QC for this electronic signature.

7.7.2.2 Revocation of electronic identity at the QTSP BORICA

In case the electronic identity of the User is maintained at the QTSP BORICA, the Titular of electronic identity can terminate it only by terminating the QC for CQES, which is issued for the SERVICE. The electronic identity (eID and the electronic identity certificate) is deleted from the REI and the REIC in the CMR (client register) of the QTSP for this Titular of Electronic Identity. His/her client account in the CMR is retained. The user account in the user database at the RP/ESP is retained (for the purpose of new registration of electronic identity).

8 OPERATIONAL PROCEDURES

It is assumed that the portal of a RP/ESP using the electronic identification service supports one or more of the following procedures within the scope of the SERVICE:

- "*Initial registration*" - creates an account (Username, password, email, mobile phone) of a User of RP/ESP; this procedure is outside the scope of the SERVICE.
- "*Electronic identity registration*" - registers the electronic identity of a User (eID and electronic identity certificate). The User is already a Titular of Electronic Identity in the domain of RP/ESP.

- "*Electronic identification without registration*" - verification of electronic identity without registration 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 Titular of electronic identity works with a selected ES, which requires electronic identification;
- "*Revocation"* - a User / Titular of electronic identity at an ESP terminates the electronic identity registered for him. The registered electronic identity of the User is terminated - it is deleted from the REI and the REIC at the RP/ESP or the QTSP BORICA. The user account at the QTSP and the client account at the QTSP are retained (for the purpose of new registration);
- "*Exit*" - a User leaves the virtual environment of a RP/ESP. In case the REI and the REIC of BORICA are not used - the registered electronic identity is terminated in the REI and the REIC at the RP/ESP and/or the QTSP BORICA. The user account at the QTSP and the client account at the RP/ESP are terminated.

The RPs/ESPs use the SERVICE through operating 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 a client account (unauthorized) at the RP/ESP is outside the scope of this document.

8.1 Operational procedure "*Electronic identification without registration*" of RPs/ESPs without user profiles

A User of electronic services without a profile at RP/ESP uses the SERVICE subject to the conditions according to section 7.2.1 in this document.

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

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

8.1.1 Transaction "Electronic identification and active operation/document(s) signing"

The User of the electronic service of a RP/ESP initiates the session for signing documents and follows the steps below:

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

6. The AEI/ CEI checks for validity the official identity document of the User in the Ministry of Interior.
7. The AEI/CEI generates a unique electronic identifier based on the extracted current personal data and the identifier of the RP/ESP.
8. The AEI/CEI generates an electronic identity certificate based on the extracted current personal data (PDF-document).
9. The AEI/CEI notifies the User (via the B-Trust MOBILE application) of documents for signing - PDF (identity certificate) and document(s) of the RP/ESP (electronic service), and requests consent from the User.
10. The User – Titular of electronic identity views the personal data (PDF) and gives consent by entering the PIN code for CQES.
11. The AEI/CEI signs the document with the CQES of the User – a PDF-file with personal data (electronic identity certificate).
12. The AEI/CEI seals the generated identity certificate (PDF) as a source of the data in the certificate and for integrity purposes, and stores the PDF file for proof. The certificate of electronic identity after the end of the session remains at the RP/ESP.
13. If the AEI/CEI does not have User data (step 4) in the B-Trust CMR/ client register (no CQES issued); the AEI/CEI sends the User an email or SMS to enter 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 AEI/CEI) the email and the mobile phone number.
16. The user captures an official identity document in the "onboarding" process of the AEI/CEI.
17. The user takes a selfie and participates in the "liveness detection" of the "onboarding" process of the AEI/CEI.
18. The AEI/CEI extracts data (via OCR) from the official identity document.
19. The AEI/CEI checks for validity the official identity document in the Ministry of Interior.
20. The AEI/CEI extracts personal data through RegiX.
21. The AEI/CEI verifies the selfie with a photo from an official identity document and with a photo from RegiX.
22. The AEI/CEI makes verification of "Liveness detection".
23. The AEI/CEI issues to the User a certificate for CQES, after which **steps 5 - 12** of the procedure are performed.

For additional information regarding the signing of documents with CQES at RPs through the B-Trust platform for CQES of the QTSP BORICA, see the document "General terms conditions for using the certification service "Remote signing of electronic documents with cloud QES"".

8.2 Operational procedures of RPs/ESPs with User Profiles

A user of electronic services with a profile at a RP/ESP uses the SERVICE subject to the conditions according to section 7.2.2 in this document.

The SERVICE creates and permanently registers an electronic identity (eID and electronic identity certificate) and/or verifies a registered one of the User within an active session with an electronic service of a RP/ESP. The registered permanent electronic identity is in the REI/REIC at an ESP and/or the QTSP BORICA. The registration of an electronic identity is a one-time process in using the SERVICE. Electronic identity verification is performed each time the Titular of Electronic Identity addresses the electronic service with an active operation. The Titular of electronic identity is also the Titular of the CQES issued at the registration of his/her electronic identity. A change in personal data

of the User discovered when working with the SERVICE initiates creation of a new electronic identity for the User of the RP/ESP.

8.2.1 "Registration of Electronic Identity" Procedure

This procedure is initiated by a RP/ESP when a User, who is not a Titular of Electronic Identity addresses an electronic service requiring it. The registration of electronic identity at a RP/ESP follows the steps below:

1. A user registers at a RP/ESP, provides personal data (Personal Identification Number/Personal Foreigner's Number, mobile phone number, email); the phone number and email are validated by the RP/ESP.
2. The RP/ESP creates a profile with 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 makes a request to the AEI/CEI for electronic identification of a natural person with the provided personal data.
5. The AEI/CEI checks for availability of data of the User in B-Trust CMR (client register).
6. If data is available (the user is a client of B-Trust, i.e. he/she **has a CQES**), the AEI/CEI extracts the personal data from RegiX.
7. The AEI/CEI checks for validity the official identity document of the User in the Ministry of Interior.
8. The AEI/CEI generates a unique electronic identifier based on the extracted current data and the identifier of the RP/ESP.
9. The AEI/CEI stores the generated electronic identifier in the REI (a part of B-Trust CMR).
10. The AEI/CEI generates an electronic identification certificate based on extracted current personal data (a PDF document).
11. The AEI/CEI notifies the User (through the B-Trust Mobile application) of a document for signing (electronic identity certificate, PDF), and requests consent from the User.
12. The User – Titular of electronic identity views the personal data (PDF) and gives consent by entering the PIN for CQES.
13. The AEI/CEI signs with the User's CQES the PDF file with personal data (the electronic identity certificate).
14. The AEI/CEI seals the generated identity certificate (PDF) as a source of the data in the certificate and for integrity purposes, and stores the PDF file for proof. The certificate of electronic identity after the end of the session remains with the RP/ESP.

8.2.2 The QTSP BORICA (AEI/CEI) stores the electronic identity

1. The AEI/CEI records the electronic identity (eID and electronic identity certificate) of the Titular in the REI/REIC , a part of B-Trust CMR of the QTSP BORICA.
2. The AEI/CEI provides personal data of the Titular of electronic identity to the RP/ESP (only those that the RP/ESP has specified in registration of the service at the CEI); The RP/ESP may use personal data of the registered electronic identity of the Titular in the electronic service addressed by him.

8.2.2.1 The RP/ESP stores the electronic identity

1. The AEI/CEI sends the established electronic identity (eID and electronic identity certificate) of the Titular to the RP/ESP.
2. the RP/ESP stores the electronic identity in the profile of the Titular (the REI/REIC).

8.2.3 "Verification of electronic identity (strict authentication)" Procedure

This procedure is initiated by the RP/ESP when a User, who is a Titular of Electronic Identity addresses an electronic service, which requires electronic identification.

When the User is not a Titular of Electronic Identity and the RP/ESP does not support user profiles, the scope of the user transaction includes his/her electronic identification, **verification of the established electronic identity** and execution of an active operation (e.g., signing).

When the User is a Titular of Electronic Identity, 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-Titular is registered in the REI/REIC of the QTSP BORICA;
- The RP/ESP supports a user profile, and the electronic identity (electronic identifier and certificate) of the User-Titular is registered in the REI/REIC of the RP/ESP.

The electronic identity verification (strict authentication) at the RP/ESP follows the steps below.

8.2.3.1 Electronic identity (electronic identifier and certificate) of the User-Titular in the REI/REIC of the QTSP BORICA

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

1. A User–Titular of electronic identity addresses an electronic service of a RP/ESP, which requires electronic identification (verification).
2. The User – Titular sends personal data (Personal Identification Number/Personal Foreigner's Number, Mobile phone number, email) to the electronic service of the RP/ESP.
3. The RP/ESP sends the personal data to the AEI/CEI.
4. The AEI/CEI checks the REI/ REIC in B-Trust CMR for registered eID and Certificate of the User-Titular. If there are none, this User does not have a registered electronic identity – he/ she should be registered.
5. The AEI/CEI extracts current personal data from RegiX.
6. The AEI/CEI checks for validity an official identity document in the Ministry of Interior.
7. The AEI/CEI generates electronic identifier based on the current personal data and an identifier of the AEI/CEI.
8. The AEI/CEI generates a certificate of electronic identity with the personal data (PDF).
9. The AEI/CEI notifies of a document for signing via the B-Trust Mobile application – a consent for provision of personal data to the RP/ESP.
10. The user views the PDF and gives consent by entering the PIN of the CQES.
11. The AEI/CEI signs the PDF (electronic identity certificate with current personal data) with the CQES of the user.
12. The AEI/CEI seals the certificate (indication of its source and integrity).
13. The AEI/CEI compares the generated electronic identifier with that in the REI of B-Trust CMR (BORICA).
14. In case of correspondence - the User-Titular is authenticated before the RP/ESP; he/she gets access to the electronic service. In case of discrepancy, **step 16** follows.
15. The AEI/CEI sends personal data (from the electronic identity 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 Titular of Electronic Identity.
16. If there is no correspondence in step 14, the AEI/CEI invalidates the registered electronic identity of the User-Titular in the REI/REIC of B-Trust CMR (BORICA).

17. The AEI/CEI registers the new current electronic identity of the User in the REI/REIC of B-Trust CMR (BORICA).

8.2.3.2 The electronic identity (electronic identifier and certificate) of the User-Titular in the REI/REIC of the RP/ESP

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

1. A User – Titular of electronic identity, addresses an electronic service of a RP/ESP, which requires electronic identification (verification).
2. The User – titular sends personal data (Personal Identification Number/Personal Foreigner's Number, Mobile phone number, email) to the electronic service of the RP/ESP.
3. The AEI/CEI checks the REI/ REIC for a registered eID and Certificate of the User-Titular. If there is none, **the procedure under section 8.2.3.1 is performed**.
4. The RP/ESP has a registered electronic identity of the User-Titular. It extracts personal data from the registered electronic identity certificate.
5. The RP/ESP sends personal data of the User-Titular to the AEI/CEI.
6. The AEI/CEI extracts current personal data of the User from RegiX.
7. The AEI/CEI checks for validity the official identity document of the User in the Ministry of Interior.
8. The AEI/CEI generates electronic identifier based on the current personal data and an identifier of the AEI/CEI.
9. The AEI/CEI generates a certificate of electronic identity with the personal data (PDF).
10. The AEI/CEI notifies the User of a document for signing via the B-Trust Mobile application – a consent for providing personal data to the RP/ESP.
11. The user views the PDF and gives consent by entering the PIN of the CQES.
12. The AEI/CEI signs the PDF (electronic identity certificate with current personal data) with the CQES of the user.
13. The AEI/CEI seals the certificate (indication of its source and integrity).
14. The AEI/CEI returns a current electronic identity (electronic identifier and certificate) to the RP/ESP.
15. The RP/ESP compares the generated electronic identifier with that in the REI of the RP/ESP; in case of discrepancy, **step 17** follows.
16. In case of correspondence, the User-Titular of electronic identity is authenticated before the RP/ESP; The user gets 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-Titular in the REI/REIC of the RP/ESP.
18. The RP/ESP registers the new current electronic identity of the User in their REI/REIC.

8.2.4 "Electronic Identity Change" Procedure

A registered electronic identity of a Titular of Electronic Identity is permanent in time until a change in the personal data of a valid official identity document of the person. Any change in the data leads to automatic update – a termination of the registered electronic identity and registration of the new electronic identity (with generated eID and certificate of electronic identity based on current personal data) of the person.

8.2.5 "Electronic Identity Cancellation" 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 provided for the workplaces (of operators), used for processing and storing personal recorded data obtained through the "onboarding" process, in order to prevent unauthorized access to these places – the AEI/CEI with "onboarding" process (identification center and data center/register of Users). Only authorized persons related to the activity of implementation of procedures and functions - operators and system administrators have access to them.

In addition, the QTSP BORICA uses redundancy to minimize the impact of disasters. In identification centers, data is not stored permanently.

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" that ensures that the relevant tasks and responsibilities at the AEI/CEI with 'onboarding" process are separated 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 Operators participating through a videoconference call and registration in the "onboarding" process of the electronic identification, 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 in the AEI/CEI (video identification centers). The training documentation is part of the human resources management system. The responsibility for conducting the training lies with the team leader of the AEI/CEI with "onboarding" process (identification center) and the human resources manager.

The QTSP requires from each employee the relevant documents (certificate of no criminal conviction, police permit, CV, conflict of interest, creditworthiness 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 AEI/CEI 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 diary, paper form or other physical mechanism.

All security audit files, both electronic and non-electronic, are stored and provided 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:

- of a qualified electronic seal – to seal each generated electronic identity certificate.
- of website authentication – to authenticate (the provider of) the SERVICE.
- of Qualified CQES, respectively for one-time CQES - the User authorizes access to personal data (from the electronic identity certificate) and for signing electronic documents.

9.7 Management of the cryptographic keys

According to 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, which are used in providing the SERVICE.

9.8 Access management

All components requiring physical and logical protection against critical data and information (servers, communication equipment, keys, repositories archives, etc.) are segregated in rooms and areas with high security protection. The physical and logical control of access to the infrastructure of B-Trust® of the QTSP is according to 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 for exchange and protection of information with Users, with the AEI/CEI and with the means providing external services (analysis of images and access to national registers) to ensure network security of the systems used for electronic identification against external interventions 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

The information security is an integral part of that of the B-Trust infrastructure and is within the scope of the general Information Security Policy of BORICA, approved by the management of the company. This policy establishes the organizational measures and procedures for security management of all systems and information assets, through which BORICA provides all its services. The personnel directly involved in these systems and assets are acquainted with and implement this Policy. Signed/sealed electronic documents with QES/QESeal may contain information considered personal data. In accordance with the regulations regarding this type of data, BORICA as a QTSP, respectively as a provider of the SERVICE, is registered by the Commission for Personal Data Protection as a personal data administrator.

9.12 Continuity

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

9.13 Termination of activity of the QTSP BORICA

According to 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 detected business and technical problems in the delivery, operation and maintenance of the SERVICE, the QTSP BORICA performs risk assessment to identify, analyze and assess the related risks.
The QTSP BORICA documents the security requirements and operational procedures necessary to avoid identified risks in the electronic identification process of the SERVICE provided. Periodically, risk review and assessment are performed in order to overcome the identified risk factors.
Appropriate measures are chosen to avoid identified risks, considering the results of the risk assessment. The measures taken ensure a level of security adequate to the degree of the identified risk.

The results are reported to the Management of BORICA, which approves the results of the risk assessment, the prescribed measures for overcoming identified risk factors and accepts the identified residual risk regarding the SERVICE provided to the RPs/ESPs and to their Users.

11 INSPECTION AND CONTROL OF PROVIDER’S ACTIVITIES

According to 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 strictly complies with the conditions in this document, the requirements of the EDETSA, and the regulations in carrying out the activity of a registered QTSP.

The RPs/ESPs which will use the electronic identification service should inform and/or provide this document to their clients – Users of the SERVICE. The user must strictly follow the conditions and procedures of the "onboarding" process, which are identical to those of 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 use of CQES.

Detailed information regarding the business conditions and legal aspects in the relations of the QTSP BORICA with 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).