Public document

Certificate Policy and Practice for the Provision of Qualified Remote and Physical Identification for the Issuance of Qualified Certificates and the Verification of Specific Attributes

Version 2

Effective from 1 March 2026

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	01.01.2021	Approved	Initial release
1.1	Margarita Boneva	01.07.2021	Approved	Edited
1.2	Margarita Boneva	10.03.2023	Approved	Corrections
2	Margarita Boneva	01.03.2026	Approved	Corrections

CONTENTS

ACRONYMS 5
SPECIFIC TERMS AND DEFINITIONS 7
COMPLIANCE AND USE 8
1 GENERAL PROVISIONS 10
1.1 Certifying Authority of BORICA 10
1.2 Other Certifying Authorities and Relying Parties 11
1.3 Identifiers in this document 11
1.4 Management of the Policy 12
1.5 Other Applicable Documents 12
1.6 USE CASE – Applicable Scenarios 13
2 PARTICIPANTS IN THE "ONBOARDING" PROCESS 14
3 PUBLICATION AND REGISTRATION RESPONSIBILITIES 14
4 IDENTIFICATION AND AUTHENTICATION 15
4.1 Naming 15
4.1.1 Use of names 15
4.1.2 Use of pseudonyms 15
4.1.3 Meaning of names upon registration 16
4.1.4 Rules for name interpretation 16
4.1.5 Uniqueness of names 16
4.2 Initial validation of identity 16
4.2.1 B-Trust Mobile Application - Remote Identification in accordance with Article 24(1a), point (c) 17
4.2.2 Website for identity verification - Remote Identification in accordance with Article 24(1a), point (c) 18
4.2.3 Video Call – Remote Identification in accordance with Article 24(1a), point (c) of Regulation (EU) No 910/2014 19
4.2.4 Identification Based on Physical Presence and Verification of Attributes in accordance with Article 24(1a), point (d) 20
4.2.5 Special Attributes 21
4.2.6 Unverified information 22
4.3 Validation of Identity for Renewal 22
4.4 Validation of Identity for Suspension/Resumption 22
4.5 Validation of Identity for Revocation 22
5 Request for Issuance of Certificate 22
5.1.1 Delivery of application and acceptance of general conditions 23
5.1.2 Validation of e-mail and smart device (mobile phone number) and application protection 23
5.2 Onboarding process and registration (identity validation) 23
5.2.1 Capture of the official identity document and selfie via a Website for identity verification 23
5.2.2 Capture of the official identity document and selfie through the B-Trust Mobile application 24
5.2.3 Verification of the official identity document and selfie 24
5.2.4 Validation of the official identity document 24
5.3 Certificate issuance 25
5.3.1 Functions of Identification and Authentication 25
5.3.2 Identification and authentication with an assistant 26
5.3.3 Confirmation or rejection of the request for issuance 26
5.3.4 Technical request for issuance (PKCS # 10) 26
5.3.5 Operation of the Certification Authority 26
5.3.6 Notification of the User by the Provider 27
5.4 Certificate acceptance and publication 27
5.5 Use 27
5.6 Certificate renewal 27
5.7 Certificate renewal by generation of a new key pair (re-key) 27
5.8 Certificate modification 27
5.9 Certificate suspension/resumption and revocation 27
5.10 Certificate status 28
5.11 Termination of a Contract for Certification Services 28
6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 28
6.1 Physical controls 28
6.2 Procedural controls 28

6.3 Staff qualification and training 28
6.4 Logging procedures 29
6.5 Archiving 29
6.6 Key changeover 29
6.7 Compromise and disaster recovery 29
6.8 Compromise of a Private Key 29
6.9 Provider Termination 29
7 FUNCTIONAL MODEL AND SPECIFICATION 29
7.1 Functional model 29
7.2 Specification 30
7.3 Access management 30
7.4 Operational Security 31
7.5 Network security 31
7.6 Information security 31
7.7 Continuity 31
8 RISK ASSESSMENT 31
9 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES 32
10 BUSINESS AND LEGAL ISSUES 32

ACRONYMS

AD	JSC (Joint-stock company)
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRC	Communications Regulation Commission
CRL	Certificate Revocation List
CQES	Cloud Qualified Electronic Signature
DN	Distinguished Name
EDETSA	Electronic Document and Electronic Trust Services Act
eIDAS	Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183
ES	Electronic Signature
ETSI	European Telecommunications Standards Institute
EU	European Union
HSM	Hardware Security Module
ISO	International Standardization Organization
LRA	Local Registration Authority
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QC	Qualified Certificate
QC QES	Qualified certificate for Qualified Electronic Signature
QCS	Qualified Certification Services
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QSCD	Qualified Electronic Signature Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority
RA-VI	Registration Authority using remote video identification
VI	Video Identification
VIS	Video Identification Server

SPECIFIC 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 – identification of a natural person by a trusted party (in this case, BORICA as a QTSP).

Video Identification Server (VIS)/Video Identification Center – information resource that manages and administers the onboarding process.

Agent Portal (AP) – information resource servicing the process of registration and managing after identity validation of a natural person through the "onboarding" process and providing personal data to the CA for certification in a qualified certificate.

B-Trust Registration Authority for Face-to-face Identification – a body operating integrated information resource servicing Users upon registration for issuance and management of QES/Cloud QES certificates through a process of physical presence (face-to-face) identification with an Operator/Agent.

B-Trust Registration Authority for Remote Video Identification (RA-VI) - a body operating information resource (VIS and AP), servicing Users upon registration for issuance and management of Cloud QES through remote online video identification.

User – a natural person who participates in the "onboarding" process and who will be the Titular of the QC, i.e. B-Trust user.

Operator (of the RA-VI) – a qualified employee of BORICA, participating in the "onboarding" process via the AP.

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

Identity document - a valid document containing data for identification of a natural person (identity card, international passport, foreigner identity card and others, according to the national legislation of the respective country).

"Cloud services" – online services for image analysis for the purposes of the "onboarding" process.

RegiX/Registry Information eXchange system – a national information hub for access to national databases (registers) with primary data.

COMPLIANCE AND USE

This Document:

- has been prepared by "BORICA" AD (hereinafter, BORICA), a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- is effective from **01.03.2026;**
- is entitled "**Policy and Practice for the Provision of Qualified Remote and Physical Identification for the Issuance of Qualified Certificates and the Verification of Specific Attributes**.
- is associated with the published current versions of the documents „Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)", and "Policy on the Provision of Qualified Certificates for Qualified Electronic Signature, Cloud Qualified Electronic Signature, Qualified Electronic Seal, and Cloud Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal/CQESeal)",which contain the general conditions and requirements for the procedures of authentication, QC issuance and maintenance, and the security level requirements for generating and storing the private key for these certificates;
- has been drawn up in compliance with the formal requirements for content, structure and scope, as set out in international guideline RFC 3647, and the international specifications ETSI EN 319-401 and EN319 411-1/2 including the sections that are specific and applicable to the "onboarding" process, and QC for Cloud QES and QC for Cloud QESeal;
- addresses only the Registration Authority for remote video identification (RA-VI), but includes texts, explanations and references that prove that the RA-VI meets the requirements for RA of a QTSP according to the above international recommendations and specifications;
- serves as General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These conditions are part of the Contract for certification services, which is concluded between the Provider and Users on the grounds of art. 23 of the EDETSA. The contract may contain special conditions that take precedence over the general conditions in this document;
- is a public document with the purpose to establish the conformity of the activity of the Provider BORICA, and in particular of the RA-VI with the EDETSA and the legal framework;
- is publicly available on the Provider's website: https://www.b-trust.bg/documents;
- may be changed by the QTSP, and each new version shall be published on the Provider's website.

This document has been prepared in compliance with:

- Electronic Document and Electronic Trusted Services Act (EDETSA);
- Ordinance on Liability and Termination of Trust Service Providers;
- 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;
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024
- 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 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

- Article 42 of the Regulation for the Implementation of the Measures Against Money Laundering Act (Republic of Bulgaria).
- Article 55(2) of the Measures Against Money Laundering Act (Republic of Bulgaria).

The content and structure of this document is in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183 and refer to the information contained in the following ratified international guidelines, specifications and standards:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

The ETSI standards and specifications referenced above require that the identity of the applicant be established through a process ensuring an appropriate level of reliability, depending on the applicable identification context. This may be achieved either through identification in a physical presence context or through remote identification, provided that suitable means and procedures are applied to ensure the required level of identity proofing. This document also constitutes the practice statement of the identity proofing service component within the trust services provided by BORICA AD and has been developed in accordance with ETSI TS 119 461 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects”.

This document applies in connection with Article 24(1a) and, where applicable, Article 24(1b) of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, as well as with Commission Implementing Regulation (EU) 2025/1566 concerning reference standards for the verification of the identity and attributes of a person to whom a qualified certificate or a qualified electronic attestation of attributes is to be issued.

For the purposes of ETSI TS 119 461, this document serves as the practice statement describing the physical and remote identification processes applied by BORICA AD and defines the applicable use cases, the level of identity proofing (LoIP), the identity evidence used, the methods for validation and binding of the applicant to the presented evidence, as well as the outcome of the identification process.

The RA-VI registration authority addressed in this document uses "onboarding" process for remote online video identification, providing a level of security equivalent to a physical presence.

Further information relating to this document can be obtained from the Provider at:

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

1 GENERAL PROVISIONS

This document describes the specific conditions and requirements that the QTSP BORICA fulfills through the "onboarding" process (physical and remote video identification) of the registration authority RA-VI to verify the identity of natural persons involved in the process of issuing qualified certificates. The natural person participates in the "onboarding" process through at a BORICA AD office, a website via a browser or through a smart device (smartphone or tablet) with a mobile application on it. The online video identification process is certified for equivalent assurance as the physical presence (face-to-face) of the persons for whom the Provider collects, verifies and validates personal data in order to certify them in issued for them QCs. Identification of natural persons through "onboarding" by the Provider has been confirmed by a Conformity Assessment Body pursuant **to Article 24(1a), points (c) and (d) of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183.**

The document contains a description of the participants in the "onboarding" process in B-Trust in identifying natural persons (Titulars/Creators of QCs), as well as describes the general operating procedures in this process:

- verification of the actual existence of the natural person in real life
- verification that the identity document belongs to that person
- proof that the current person is the same as stated before
- verification of the legal validity of the identity document

The issuance, publication, delivery and acceptance of the issued QCs by applying the "onboarding" process as well as the measures and technical procedures followed by the Provider and the natural person, which ensure the security and reliability of the provided QCs are also part of the document in accordance with the EDETSA and the regulatory framework.

The QTSP BORICA performs remote video identification of a B-Trust User through the "onboarding" process only if:

- the User and the Subject in the QC (i.e., the Titular) is a natural person.
- the User has requested that the QC shall sign e-documents on his own behalf and not on behalf of a third party.
- the User is a Creator for issuing a qualified certificate to a legal person.

Where necessary, the identification of a legal person and the establishment of the representative power of a natural person regarding a legal person, in the presence of an official public commercial or company register in a Member State, in which the legal person is registered, shall be carried out by reference in the commercial register or in the respective public register on the account of the legal entity and documenting the undertaken identification actions.

It is assumed that a User who uses this document has the knowledge and understanding of public key infrastructure, certificates and concepts for electronic signature. Otherwise, it is recommended that he/she becomes acquainted with these concepts and with the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services (B-Trust CPS-eIDAS)” before using this document.

1.1 Certifying Authority of BORICA

The QTSP BORICA has built and operates the public key infrastructure (PKI) in accordance with the legal framework of Regulation 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. The Provider uses OIDs in the B-Trust PKI Infrastructure, formed on the basis of code 15862, assigned to BORICA by IANA in the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprise) and in compliance

with ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).

The B-Trust CPS-eIDAS document specifies the infrastructure objects with their assigned identifiers (OIDs). The B-Trust Infrastructure Certification Authority has the identifier 1.3.6.1.4.1.15862.1.6.1 (B-Trust Operational Qualified CA). Through it, BORICA issues all qualified certificates specified in the document B-Trust QCP-eIDAS, including QC for CQES.

This Provider Certificate Policy and Certification Practice Statement are applied/implemented through the object with identifier 1.3.6.1.4.1.15862.1.6.10 (B-Trust Remote Video Identification Service) and 1.3.6.1.4.1.15862.1.6.12 (B-Trust Identification with physical presence)

More information about the Registration Authority of the B-Trust infrastructure of BORICA can be obtained from the document B-Trust CPS-eIDAS.

BORICA has informed the CRC about onset of activity as a QTSP in accordance with the EDETSA and current legislation. The Provider shall notify the Users of its accreditation for providing qualified trust services and the respective issued certificates.

The accreditation of BORICA as a QTSP under the Regulation and the EDETSA aims to achieve the highest security level of QCs provided and better synchronization of these activities with related activities provided in other Member States of the European Union.

Concerning relations with Users and third parties, only the version of this document is considered valid, which is effective at the time of using a QC

1.2 Other Certifying Authorities and Relying Parties

Pursuant to this Policy and Practice, within a legal entity (third party), different from the QTSP BORICA, a unit may be established as a Registration Authority RA-VI, to which rights are delegated to carry out activities on the "onboarding" process or of some of them on behalf of this Provider or for internal purposes of the legal entity.

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

The relations of BORICA and an external Provider regarding RA-VI with onboarding process are settled by a contract. This provider guarantees that the activity of the RA-VI complies with this Certificate Policy and Certification Practice Statement. For the purposes of this document, bilateral contact is maintained within the framework of the contract regarding:

- reports of all security incidents to the Provider/Relying Party;
- changes to this document after approval by the Provider/Relying Party;
- control of the operational procedures regarding the activities of RA-VI in accordance with this Policy

1.3 Identifiers in this document

The Certificate Policy and Certification Practice Statement of the QTSP BORICA regarding the “onboarding” process 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 process.

The Provider's practice in providing remote/online video identification is carried out by the object B-Trust Remote Video Identification Service (vRA) identified by the identifier: 1.3.6.1.4.1.15862.1.6.10:

"Onboarding" remote video identification process (B-Trust Remote Video Identification / B-Trust vRA)	Object Identifier
Practice of the Provider of the "onboarding" process	**1.3.6.1.4.1.15862.1.6.10**

In accordance with this document, the Provider's Practice implements Policy on the "onboarding" process with the following identifier:

"Onboarding" remote video identification process (B-Trust Remote Video Identification / B-Trust vRA)	Object Identifier
Policy of the Provider of the "onboarding" process	**1.3.6.1.4.1.15862.1.6.10.1**

The Provider's practice for the provision of physical identification is implemented through the B-Trust Identification with Physical Presence component, identified by Object Identifier (OID): 1.3.6.1.4.1.15862.1.6.12

Onboarding process for physical identification (B-Trust Identification with Physical Presence component)	Object Identifier
Practice of the Provider of the "onboarding" process	**1.3.6.1.4.1.15862.1.6.12**

In accordance with this document, the Provider's Practice implements the Policy for the onboarding process with the following identifier:

Onboarding process for physical identification	Object Identifier
Policy of the Provider of the "onboarding" process	**1.3.6.1.4.1.15862.1.6.12.1**

1.4 Management of the Policy

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.

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.

1.5 Other Applicable Documents

This document only supplements the B-Trust basic documents: "Certification Practice Statement for providing qualified certificates and qualified trust services (B-Trust CPS-eIDAS)", and "Policy on the Provision of Qualified Certificates for Qualified Electronic Signature, Cloud Qualified Electronic Signature and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal)", and follows their structure. In terms of content, it indicates references to the relevant parts of these documents and includes text (comments, short descriptions and references) to prove how the requirements for the RA-VI of the B-Trust infrastructure of the QTSP BORICA are met according to standards ETSI EN 319 411-1/2, and ETSI EN 319 401.

According to this Certificate Policy and Certification Practice Statement, the RA-VI performs the same functions as of RA in the B-Trust infrastructure, but by identifying an individual through an "onboarding" process. All missing parts of the documents: "Certification Practice Statement for providing qualified certificates and qualified trust services (B-Trust CPS-eIDAS)", and "Policy on the Provision of Qualified Certificates for Qualified

Electronic Signature, Cloud Qualified Electronic Signature and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal)" in this document are considered inapplicable in the context of RA-VI. In any case, this document should be used together with the main general documents of B-Trust:

- "Certification Practice Statement for providing qualified certificates and qualified trust services (B-Trust CPS-eIDAS)"
- "Policy on the Provision of Qualified Certificates for Qualified Electronic Signature, Cloud Qualified Electronic Signature and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal)";

The screens of the identification process through a website via a browser and through the mobile application installed on a smart device (smartphone or tablet) of the User for participation in the "onboarding" process of B-Trust can also be helpful when using the document.

1.6 USE CASE – Applicable Scenarios

The identification processes described in this document are organised in such a way as to enable the achievement of the applicable Level of Identity Proofing (LoIP) in accordance with ETSI TS 119 461, depending on the specific scenario, type of service and applicable regulatory context.

In cases where a specific scenario, the identity evidence used, the availability of a trusted source, or the applicable national context do not allow the achievement of Extended LoIP, BORICA AD may apply a scenario providing Baseline LoIP, only insofar as this is permitted for the respective service and the applicable regulatory framework.

In accordance with ETSI TS 119 461, BORICA AD declares the applicability of the following scenarios for the identity proofing of natural persons.

1. **Unattended remote context – hybrid manual and automated operation**

A scenario in which the capture of the identity document and the image of the applicant's face is performed in an automated interactive session, while the validation and/or confirmation of the result is carried out by an operator at a later stage.

The process under this point represents a remote identity proofing scenario within the meaning of ETSI TS 119 461, where the collection of identity evidence is performed in a remote environment via a mobile application, and the validation and binding of the applicant to the presented evidence is performed through a combination of automated means and control by a registration operator.

2. **Attended remote context – hybrid manual and automated operation**

A scenario in which the applicant presents an identity document and their facial image in real time through a mobile application or a web page, and in the event of unsuccessful automated identification, an operator performs a video call for control, review and confirmation.

3. **Identification in a physical presence context – manual operation**

A scenario in which identification is performed through the presentation of a physical identity document at the premises of the provider

Identification process / channel	Classification according to ETSI TS 119 461	Method of execution	Applicability
Identification at a BORICA office	physical presence context – manual operation	In person	Services requiring the highest level of reliability
Identification via the B-Trust mobile application	remote identity proofing	Automated capture and checks with subsequent operator review	Issuance of qualified certificates for Cloud QES and other applicable services
Identification via web page	remote identity proofing	Automated capture and checks with subsequent operator review	One-time Cloud QES and other services where permitted
Video call with an operator	attended remote context – hybrid manual and automated operation	Remote, in real time, with operator participation	In case of difficulties or escalation during the remote identification process

2 PARTICIPANTS IN THE "ONBOARDING" PROCESS

The parties participating in the "onboarding" process of BORICA are:

- *User* - a natural person whose identity should be securely and reliably verified and validated before being successfully registered in the Provider's database. Only those personal data are registered, which should be certified in the QC requested by the User. The User is a Titular ("Subject" attribute) in the issued Certificate and he or she can electronically sign documents only on his/her own behalf.
- *Mobile application* for online video identification - operates on a smart device (smartphone or tablet) of the User. Through it, the User participates in the "onboarding" process of the Provider;
- *Website for identity verification through a browser* - a User accesses a specific Internet address and follows the instructions, going through an identification process, as a result of which he is issued a one-time CQES;
- *Specialized website* – a User activates a QC after delivery by courier.
- *Provider,* who supplies and operates the RA-VI Registration Authority - integrated information resource that is accessed by the User through the mobile application. It supervises and manages the successive steps in the implementation of the "onboarding" process.

3 PUBLICATION AND REGISTRATION RESPONSIBILITIES

See section 2 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

The contract for the delivered QC for CQES through the "onboarding" process with reference to this Policy and Practice, as well as the certified personal data of the User in an issued QC are displayed to the User in a specialized website. He reviews and accepts them, signs the Contract with the issued CQES and they are included in the evidence file in the database of the Provider.

The contract for one-time CQES, and the certified personal data of the User in the issued QC are displayed to the User on a specialized website. The User reviews and accepts them, signs the Contract with the issued one-time CQES and they are included in the evidence file in the database.

The agreement for the qualified certificate on a hardware device, as well as the certified personal data of the User included in the issued qualified certificate, are presented to the User either at the premises of BORICA AD or through a dedicated web page for electronic document exchange.

For services provided through an electronic channel of BORICA, for which contract is not signed between the User and BORICA, the General Terms and Conditions are used, which have the force of a contract.

4 IDENTIFICATION AND AUTHENTICATION

The Provider:

- accept requests for issuance of QC through physical presence, through a website via a browser or via the B-Trust mobile application on a smart device (smartphone or tablet) of a natural person - user;
- perform verification to establish the identity of the User and specific data about him/her through the implementation of "onboarding" process:
    - 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;
- register the request for issuance of QC after successful verification and validation of the person or rejects the request;
- provide to the User the validated personal data, which are certified (requests consent);
- notify the CA to issue a QC.

The Provider shall ensure that the natural persons are properly identified, authenticated, and that the requests for issuing QCs are fully, accurately and duly verified and approved, including full name and evidence for the relation between the certified data and the natural person.

Where the identification is performed for a natural person acting on behalf of a legal entity, in addition to identifying the natural person, data relating to the legal entity are also collected and validated, including the role of the natural person in relation to the legal entity and the source of the representation authority. This relationship is established and/or validated through trusted registers, official documents, certificates, authorisation documents, or other permissible sources that provide a sufficient level of reliability for the applicable context.

4.1 Naming

In the process of remote video identification, the name and other personal data of the User are verified against a copy of his valid legal identity document or passport.

4.1.1 Use of names

See the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services”, which is applicable to QCs of a natural person. The RA-VI, operating on behalf of the Provider, asserts that the names in the requests for certificates comply with the standard X.509.

4.1.2 Use of pseudonyms

Pseudonyms (as well as anonymity) are not accepted by the RA-VI. All names of Users of QC are real names and are checked against evidence in the form of a selfie and a copy of the identity document or passport delivered in the "onboarding" process.

4.1.3 Meaning of names upon registration

See section 3.1.3 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS).

4.1.4 Rules for name interpretation

The Provider includes in the QC personal data from the validated identity of Users, which are successfully verified and confirmed by the RA-VI based on the secure and reliable video identification of the User through the "onboarding" process and the submitted identity documents. In all certificates, the Common Name (CN) field contains the name of the individual with whom he is usually designated in his activity.

4.1.5 Uniqueness of names

See the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), which is applicable to QCs of a natural person.

The "Subject" field in the certificate is formed by the User's data, which is provided remotely, authenticated and validated through the "Onboarding" process.

The minimum set of personal data for a natural person that are collected and verified in order to identify and fill in the field "Subject" are:

- surname(s);
- first name(s);
- father’s name(s)
- national unique identifier, in accordance with the technical specifications for the purposes of cross-border identification: for Bulgarian citizens – Uniform Civil Number/Foreign National's Personal Number, passport number or ID card number; for a foreigner - national personal number, passport number or ID card number; the identifier should be contained in a valid official identity document with photo of the identified person.
- date and place of birth;
- valid email address;
- citizenship;
- country of residence and permanent address.

The set of identification data for a natural person may additionally contain:

- sex;
- phone number;
- email address;
- others (depending on the integration of the RA-VI with a relying party and the different primary registers and secure data sources).

In the DN of the User for QC the name of the RA-VI may be included - a unique feature of the RA-VI in the B-Trust infrastructure, through which the Provider has verified and validated online the identity.

4.2 Initial validation of identity

Only a natural person, who will be the Titular of the certificate apply before the Provider for initial issuance of a a QC for QES, a QC for CQES, a one-time CQES, and a QC for AES. The Provider performs an "onboarding" process, which delivers and validates the necessary information for secure identification of the Titular of the certificate. Additionally, for the purposes of the QC for CQES, the RA-VI collects and verifies identification data for a mobile smart device (smartphone or tablet) with a mobile application for Android or for iOS of the

applicant of the QC for cloud QES. Where electronic identification means (eID) are used within the services of BORICA AD, they are issued only after the successful completion of the identification (onboarding) process. In such cases, the eID means serves as the result of a successfully completed identity proofing process.

4.2.1 B-Trust Mobile Application - Remote Identification in accordance with Article 24(1a), point (c)

The Provider requires the User to participate via the mobile application in the "onboarding" process of the RA-VI. For this purpose, the User has to:

- download and install the mobile application for the respective operating system;
- start the registration process in the mobile application;
- accept the General Terms and Conditions;
- provide and validate his/her email address;
- provide and validate the phone number of the smart device he will work with;
- set a login password for the application (or enable biometric login authentication if the smart device supports one).

In order to issue a QC for CQES, the Provider requires through the RA-VI the User to register a request for initial issuance of the certificate. Registration through the "onboarding" process includes:

- collection of personal identification data of the User;
- secure verification and validation of the User's identity data;
- visualization on the smart device of the validated personal data to the User and request for consent for their certification in the QC for CQES.

Successfully verified and validated data of the User are recorded in the user register of B-Trust of BORICA - a profile of the User of QC for CQES is created. For the purposes of registration and subsequent identification, the User is required to provide a mobile phone number and an email address. These are validated by sending a one-time password (OTP) to verify the User’s access to the declared phone number and email address.

After the mobile number and email address have been validated, the User selects the type of identity document and captures images of the official identity document. Depending on the selected document type, the system requires the capture of one or more pages of the document.

The User’s personal data are entered automatically following the scanning of the identity document. The system performs a quality check of the captured document image, including verification for blurring, glare, or dark spots. The system also verifies the authenticity of the document image, ensuring that it represents a genuine document and not a scanned copy, a photograph of a printed document, a screenshot, or other manipulated representation.

In the next step, the User is required to capture an image of their face, during which a biometric verification is performed.

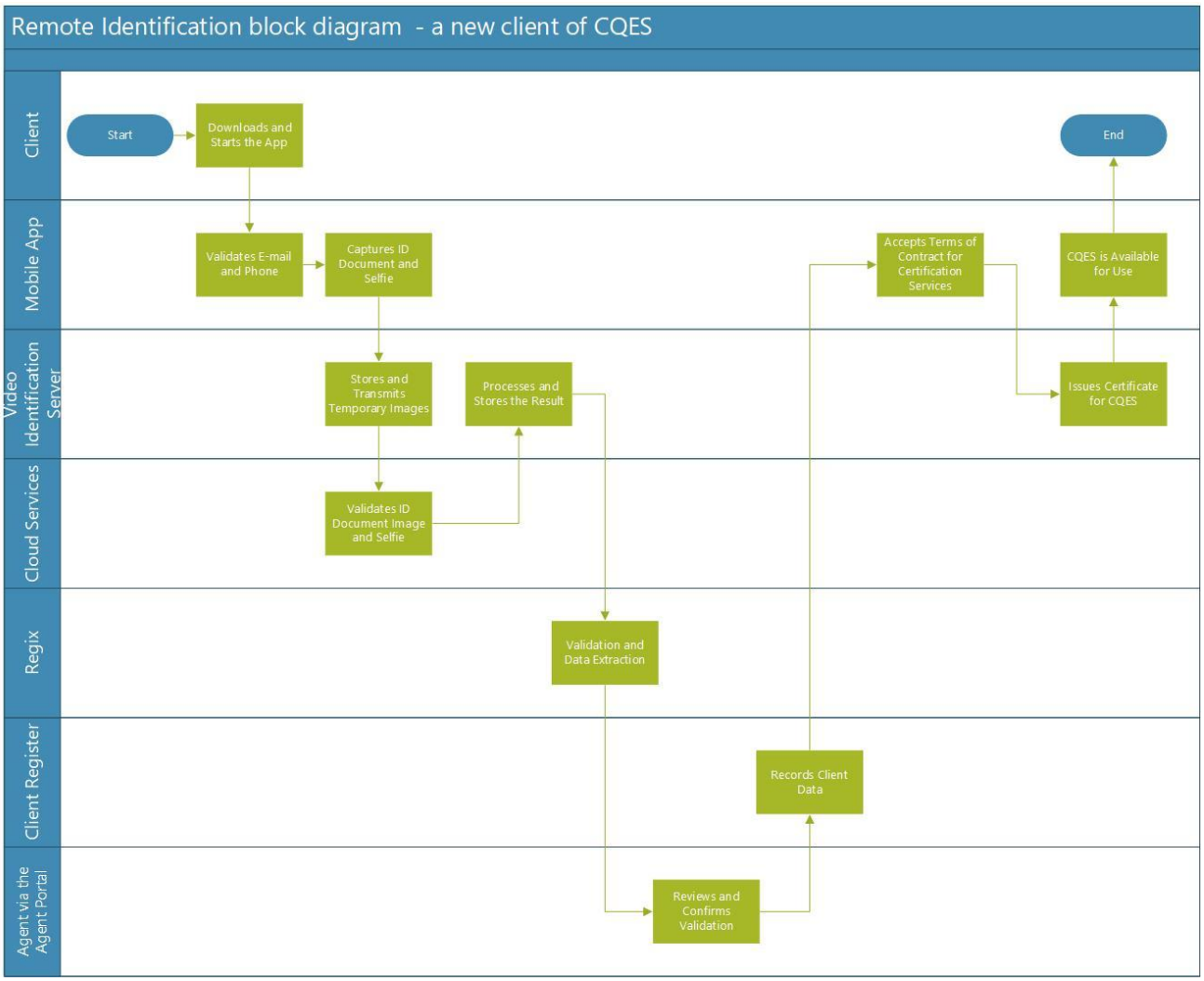
The data extracted from the identity document are automatically validated against a trusted source, where such a source is available, based on integration with national identity document databases or citizenship registers. In Bulgaria, integration with a trusted national source is available, enabling the full automated validation of the data and retrieval of the facial image in high resolution from the national database.

This method is nationally recognised by the competent regulatory authority — the Communications Regulation Commission — as part of a nationally notified electronic identification service included in the Trust List.

Following successful automated identification, the process is subject to mandatory review and verification by an operator of BORICA AD.

The process described in this section represents a remote identity proofing scenario within the meaning of ETSI TS 119 461, where the collection of identity evidence is performed in a remote environment via a mobile application, and the validation and binding of the applicant to the presented evidence are carried out through a combination of automated means and review by a registration operator.

The remote identification of a User proceeds according to the block diagram presented below:



4.2.2 Website for identity verification - Remote Identification in accordance with Article 24(1a), point (c)

A user accesses a specific internet address and follows the instructions by going through an identification process, as a result of which he is issued a one-time CQES, with which to participate and use the electronic identification service of BORICA or a QC for QES, which he or she has requested through an electronic channel of BORICA.

For this purpose, the User has to:

- access a specific internet address;

- start a process of registration;
- accept the General Terms and Conditions;
- provide for this purpose his/her valid mobile phone number and email address which have to be completely under his/her control;
- select the type of document with which he or she will be identified- ID card or passport.

To issue a one-time CQES or a QC for QES, the Provider requires through the RA-VI the User to register an application for initial issuance of the certificate. The registration through the "onboarding" process includes:

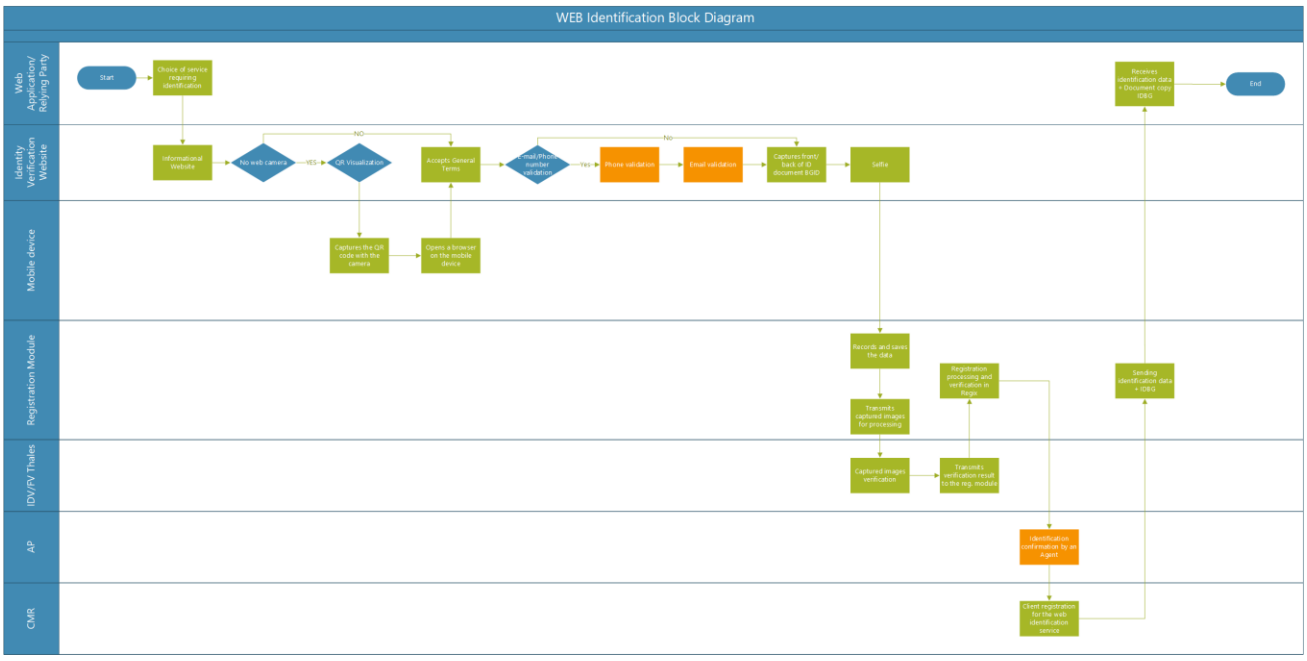
- collection of personal identification data of the User;
- secure verification and validation of the User's identity data;
- visualization of the validated personal data to the User and request for consent for their certification in the QC for CQES

Successfully verified and validated data of the User are recorded in the user register of B-Trust of BORICA.

The checks performed during the remote identification process via the web interface are equivalent to those carried out in the onboarding process described above for the mobile application.

The process described in this section represents remote identification in a web environment and is classified under ETSI TS 119 461 as remote identity proofing, whereby the presentation of identity evidence and the image of the applicant are performed remotely through a browser-based session.

The remote identification of a User for issuance of a one-time QES proceeds according to the block diagram presented below:



4.2.3 Video Call – Remote Identification in accordance with Article 24(1a), point (c) of Regulation (EU) No 910/2014

When natural persons - Users encounter difficulties during the "onboarding" process, they can initiate remote video identification via the mobile application or a website for identity verification, by contacting a qualified

RA-VI operator for a video conference call and verification of a legally valid official identity document (identity card, international passport, identity card of a foreigner and others in accordance with the national legislation of the citizen of the respective country). The RA-VI presents the validated personal identification data by visualizing them to the User on the smart device or on the website with a request for consent for their certification in the QC, i.e. consent to the Provider to issue the qualified certificate.

After successful identification, a profile of the User of QC is created automatically in the Provider's register of users.

If during the videoconferencing the operator has doubts in the course of the process, he rejects and interrupts the identification of the person or contacts him or her. In case of an invalid identity document, the operator interrupts the connection with the person. He/she must re-capture the document and reconnect to the operator via the application.

In case of unsuccessful remote video identification by a video conference call with a qualified operator of the RA-VI via the mobile application on the smart device, the person shall be requested to visit the LRA-office of the CA of the Provider.

The process described in this section corresponds to attended remote identity proofing, as the presentation of the identity document and the visual or biometric binding of the applicant to the identity evidence are performed within a session supervised by a registration operator.

4.2.4 Identification Based on Physical Presence and Verification of Attributes in accordance with Article 24(1a), point (d)

The process described in this section corresponds to identity proofing in a physical presence context within the meaning of ETSI TS 119 461, where the applicant appears in person before an officer of the registration authority and presents a physical identity document.

A person may be identified by visiting a BORICA office. This may occur either at the initiative of the person or in the event of unsuccessful remote video identification performed through a smart device and the mobile application.

In such cases, the person is invited to visit the Provider's office where the physical identification process is carried out.

When visiting a BORICA office, a representative of the Provider performs an initial verification of the identity based on the presented identity document. In addition to visual verification of the data, the representative also checks the validity and authenticity of the document using the technical means available at the offices, where necessary. The person's data are also verified against national registers before proceeding with the service request.

Following the successful registration of the User through the onboarding process, a request for the issuance of a qualified certificate for a qualified electronic signature (QES) is prepared as follows:

- a key pair is generated;
- an authorisation option is selected for the User when signing with the cloud-based QES (association of the smart device with the mobile application).

Verification of possession of the private key by the natural person corresponding to the public key included in the issued certificate for cloud QES is not applicable. Such verification is performed only where the key pair is generated by the User. In the case of cloud QES, the key pair is generated by the Provider (within an RQSCD/HSM).

The issued qualified certificate for a qualified electronic signature on a hardware device is delivered to the User, with the key pair generated in the User's presence on a qualified device. A qualified certificate for cloud QES is not delivered to the User–holder. Instead, the Provider publishes it in the B-Trust Public Certificate Repository, while the generated key pair for the cloud QES is stored within the RQSCD (HSM) of the cloud signature platform.

The certificate and the key pair are associated with the User's account and with the User's mobile device running the mobile application on the smartphone or tablet.

4.2.5 Special Attributes

Where, in addition to the identity of the applicant, specific attributes are required to be verified, such verification shall be carried out using appropriate and reliable data sources depending on the type of attribute, the applicable service and the relevant regulatory context.

The Registration Officer (RO) verifies and confirms that the data and attributes provided by the applicant correspond to the data contained in the relevant national, authentic or authoritative information sources.

The verification of specific attributes is performed in accordance with Article 24(1b) of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, and may be carried out directly by the Provider or through a third party, where permitted under the applicable legal framework.

Depending on the type of attribute, the available information sources and the technological means used, the verification may include one or a combination of the following methods:

1. verification through the European Digital Identity Wallet or through an electronic identification means that has been notified and meets the requirements of Article 8 of Regulation (EU) No 910/2014 for the "high" level of assurance;
2. verification through a qualified electronic signature certificate or a qualified electronic seal certificate, where such certificate is used as evidence of the identity or attributes of the person;
3. verification through a qualified electronic attestation of attributes, where such attestation is available and valid;
4. verification through other methods ensuring a high level of reliability, the conformity of which has been confirmed by a conformity assessment body;
5. verification through access to official registers or other authoritative data sources via secure electronic communication channels;
6. verification of an identity document using technical means for confirming its authenticity, including:

   • verification of the data through a secure connection to a primary register or other authentic information source;
   • verification using NFC technology where the identity document contains an integrated RFID chip (e.g. ICAO ePassport chip);
   • verification of the visual and security features of the document;
   • verification through official documents or other evidence confirming the relevant attribute.

A specific attribute shall be considered verified only where a sufficient link has been established between the identified natural person, the information source, and the attribute to be attested.

Attributes that cannot be confirmed through a reliable source, or for which there are doubts regarding their reliability, shall not be included in the result of the identification process.

4.2.6 Unverified information

See of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), which is applicable to QC for CQES of a natural person. Only verified information used by the RA and RA-VI, is certified in the issued certificate for CQES.

4.3 Validation of Identity for Renewal

See the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), which is applicable to QC for CQES of a natural person, and section 4.2 (Initial validation of identity) of this document.

QCs for CQES and one-time CQES are not renewed. With an existing and valid Cloud QES, the user may at any time request the issuance of a new Cloud QES - after successful authentication with the mobile application.

The one-time CQES is issued for a specific purpose. The certificate is issued with the purpose of signing a specific electronic document. The certificate cannot be used after performing the action for which it has been issued.

Renewal by "re-key" (generation of a new key pair) of an issued QC for CQES by the RA-VI (by means of "onboarding" process) is not supported.

4.4 Validation of Identity for Suspension/Resumption

The request for suspension/resumption of a QC must be made personally by the Titular.

The one-time CQES is issued with the purpose of signing a specific electronic document. The certificate cannot be used after performing the action for which this CQES has been issued.

See “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), which is applicable to QC for CQES of a natural person, and section 4.2 (Initial validation of identity) of this document.

4.5 Validation of Identity for Revocation

The request for revocation of a QC for CQES must be made personally by the Titular.

The one-time CQES is issued only with the purpose of one-time signing a specific document. The certificate cannot be used after performing the action for which this CQES has been issued.

to QC for CQES of a natural person, and section 4.2 (Initial validation of identity) in this document.

5 Request for Issuance of Certificate

The issuance of a QC is preceded by the registration of an application through the RA-VI with "onboarding" process of the Provider. An application for issuance of a certificate can be made only personally by the Applicant, preceded by the installation and initialization of the mobile application in his/her mobile smart device or by access to a website for identity verification for the purpose of issuing a for signing of documents provided by a third party.

In case of unsuccessful "onboarding", the Applicant registers a request for issuance of a certificate online by conducting a videoconference call with a qualified operator in the RA-VI of the Provider, who as an authorized representative of the Provider online registers an application for issuance of QC for CQES or one-time CQES.

5.1.1 Delivery of application and acceptance of general conditions

From an e-shop (App Store or Google Play), depending on the operating system of the smart device, the User downloads, installs and launches the mobile application. In order to participate in the "onboarding" registration process, the User must accept the General Terms and Conditions and the Declaration for the provision of personal data. Before the identification process is initiated, the applicant is provided with clear information regarding the purpose of the identification, the applicable terms and conditions, the actions required from the applicant, the categories of data and attributes to be collected, the identity evidence to be used, the technical means required to participate in the process, as well as the storage and retention of the collected data and evidence.

5.1.2 Validation of e-mail and smart device (mobile phone number) and application protection

The user enters and sends his valid e-mail address to which the RA-VI sends a message with a unique code. The user enters the received code in the mobile application; the RA-VI compares it with the sent one and accepts as valid the delivered e-mail address.

The procedure for delivery and acceptance of a valid mobile number on a smart device of a User by the RA-VI of the Provider is similar by exchanging a one-time unique code sent to the phone number or through another technical service delivered by the Provider, which guarantees at least the same security level.

5.2 Onboarding process and registration (identity validation)

Regarding this document, the User is a natural person, who is the Titular/Creator of the requested QC.

To participate in the "onboarding" process, the User should have:

- a valid official national identity document;
- a smart device with initialized mobile application for issuance of a QC for CQES or a device with a browser for web identity verification for issuance of a QC;
- Internet connection.

The application for issuance through the "onboarding" process of the RA-VI includes all the required information of the User under the EDETSA. The request may also include additional, non-verifiable information, which is not certified, but facilitates the contact of the Provider with the natural person.

The "Onboarding" process enables automatic (without an operator) or through a qualified/trained operator of the RA-VI generation of the pair of cryptographic keys and to include the public key in the request for issuance of the certificate by the CA of the Provider.

5.2.1 Capture of the official identity document and selfie via a Website for identity verification

A User accesses the website for identity verification through a computer or mobile browser and accepts the general terms and conditions for remote identification.

The site prompts the User to display an identity document in front of the camera (face and back, depending on the selected document type).

The user views and confirms the captured images.

The website requires the User to take a selfie, following the instructions to perform "liveness detection".

The captured images of the official identity document and selfie are handed over for temporary storage to the RA-VI of BORICA.

5.2.2 Capture of the official identity document and selfie through the B-Trust Mobile application

The application launches the camera of the smart device (smartphone or tablet) and prompts the User to place the front of the identity document in front of the camera.

The User specifies the type of the captured document and depending on the specified type; the application requires the capture of one or more pages of the document.

The user views and confirms the captured images.

The application requires the User to take a selfie, following the instructions of the application to perform "liveness detection".

The captured images of the official identity document and selfie are handed over for temporary storage to the RA-VI of BORICA.

5.2.3 Verification of the official identity document and selfie

The Provider's **RO-VI (Registration Officer – Video Identification)** at **BORICA AD** accesses cloud services through which analysis of the images of the identity document and the captured facial image is performed. The analysis may be supported by automated means, including machine-learning algorithms that compare the characteristics of the document with the corresponding document model and detect signs of forgery, manipulation or inconsistencies.

Through these services:

- the captured images of the identity document and the selfie are transmitted;
- a quality check of the captured images is performed;
- verification of the validity and usability of the identity document is performed;
- data (OCR) and the facial image are extracted from the identity document;
- a comparison is performed between the facial image from the identity document and the captured selfie.

After processing, the Provider's RO-VI receives a document (status report) from the cloud services used for online video identification.

The information channel used for the exchange between the Provider's RO-VI and the cloud services is secured (HTTPS/TLS protocol).

During **identification with physical presence**, additional tools may be used to verify the security features of the document, including magnification tools and other specialised equipment for verifying the authenticity of the document.

5.2.4 Validation of the official identity document

The RA-VI and RA uses the received document (status report) to check the validity of the identity document:

- for a Bulgarian citizen the verification is through the national Regix system and the database with primary identity documents of the Ministry of the Interior;

- for foreign citizens the received document (status report) is entered in a list of pending validity confirmation by the Operator.

For the identification of natural persons, BORICA AD accepts as official identity documents at least a valid national identity card, an international passport, and other official identity documents permitted under the national legislation of the issuing state, provided that such documents meet the reliability requirements in the applicable context.

For the validation of the data and status of identity documents, BORICA AD uses, where available, national primary registers, PRADO, and other permissible authoritative sources. The use of a specific register or source may be mandatory or supplementary depending on the type of document, the nationality of the person, the type of service and the applicable identification context.

5.2.4.1 Available service to primary registers – natural person Bulgarian citizen

The RA-VI and RA performs automated verification of the data received from national primary registers with those from the official document (status report) received from the service used. After successful verification of the validity of the identity document, the User's data are extracted and recorded in the client register of B-Trust (BORICA).

The RA-VI and RA notify the User of successful identification and registration.

5.2.4.2 Unavailable service to primary registers

If automated verification is not possible, the RA-VI notifies the User. The received document (status report) after verification of the official identity document and selfie is saved by the Operator in a list of pending validity confirmation. A Qualified RA-VI Operator receives a notification to review pending records with identification data.

The Operator accesses the list of pending records and checks the registration status:

- For official identity documents of a natural person-Bulgarian citizen, the Operator takes action to call Regix and follows instructions for qualified verification of the identity document;
- For foreign citizens - performs verification of the validity of the identity document in PRADO (Public Register of Authentic travel and identity Documents Online); conducts a telephone conversation and requires additional information from the User (e.g., invoice for purchased goods/utility bills, etc.
- The establishment of the identity of a legal person (Creator) is carried out by checking the relevant registers according to the provided UIC, BULSTAT number or other identification number of the person.

The Operator confirms the successful identification of the User through the "onboarding" process by an electronic signature.

5.3 Certificate issuance

5.3.1 Functions of Identification and Authentication

The RA and RA-VI through the "onboarding" process validates the identity of the Applicant-natural person, delivers the personal data that the Provider will certify in a QC and registers the User. See section 4.2 (Initial identity validation) of this document.

5.3.2 Identification and authentication with an assistant

Participation of a User with an assistant in the "onboarding" process of the RA-VI of the Provider is performed according to item 4.2.2 in the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services"

5.3.3 Confirmation or rejection of the request for issuance

After successful validation of the User's identity through the "onboarding" process of the RA-VI, his/her identification data are registered (by Operator's approval). The Operator confirms the identification of the User/Creator through the "onboarding" process by an electronic signature.

With the successful registration of the User with the Provider, the request for issuance of a QC.

The validated identification data, which the Provider will certify in the QC, are visualized in the application on the smart device/the website of the User.

The "onboarding" process shall be terminated in case of:

- invalid official identity document of the natural person - Applicant;
- doubts raised in the RA-VI Operator during the execution and review of the videoconference conversation with the Applicant;

If during the review of the video the operator has doubts about details of the process, he rejects and interrupts the identification of the person or contacts him to clarify the procedure.

The RA-VI operator shall immediately notify the Applicant and state the reasons for rejecting the request for issuance of a CA. An applicant with a rejected request for the issuance of a QC may make a request again, through RA-VI "onboarding" process after eliminating the specified reasons for rejection.

The RA-VI duly stores and archives elements of the operation of the "onboarding" process as well as the confirmed electronic request for issuance of a certificate.

The RA-VI controls and approves to the Provider the accuracy and precision of the information included in the QC only at the time of its issuance.

5.3.4 Technical request for issuance (PKCS # 10)

The User should:

- Accept and confirm the Contract/Terms and Conditions and associated Policy and Practice Statement (this document).
- accept the visualized personal data (consent for his national personal identifier).
- choose an option for confirmation when signing with CQES - the login code for the mobile application or a separate PIN, respectively biometrics.

After a response from the User, the RA-VI generates:

- technical request PKCS # 10 for issuance of QC, which is approved by signing it and is sent to the Certifying Authority of the Provider;
- Certification services contract, which is sent to the mobile application/specialized website of the User.

5.3.5 Operation of the Certification Authority

The CA of the Provider electronically authenticates the RA-VI, which has approved the electronic request for issuance of QC for CQES. The CA generates the requested QC, signs it with the electronic signature of the Provider and publishes it immediately in its Public Register.

The contract for certification services is signed with the issued QC for CQES.

5.3.6 Notification of the User by the Provider

The Provider, via the User Notification Service, immediately notifies the User of a certificate issued and published. The Notification Service sends to the User an electronic notification by e-mail or push-notification to the mobile application with information about the issued QC, its serial number and its validity period.

5.4 Certificate acceptance and publication

See section 4.4. of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), which is applicable to QC for CQES of a natural person.

5.5 Use

The benefits of the "onboarding" process include extremely easy and fast identification of the User from any place and at any time. The use of digital online video identification is fully compliant with current legislation. Used by natural persons holding a valid official identity document.

See section 4.5 of the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services” of BORICA AD (B-Trust CPS-eIDAS), and the document “Certificate Policy for providing Qualified Certificates for Qualified Electronic Signature, Cloud Qualified Electronic Signature, Qualified Electronic Seal, and Cloud Qualified Electronic Seal”, applicable to QCs of a natural person.

5.6 Certificate renewal

Renewal of QC for Cloud QES/QESeal, Advanced QES/QESeal is not accepted. At the request of the User, the Provider issues a new QC, performing initial identification and authorizing his/her identity.

Having a valid Cloud QES/QESeal, the user may at any time request the issuance of a new one - after successful authentication with the mobile application.

5.7 Certificate renewal by generation of a new key pair (re-key)

Certificate renewal by generation of a new key pair (re-key) of an issued QC for Cloud QES/QESeal, Advanced QES/QESeal is not supported.

5.8 Certificate modification

The Provider allows changes in the content of information in an issued and published QC only in compliance with the requirements and conditions for registration of a request for issuance of a new certificate to the RA-VI with "onboarding" process.

5.9 Certificate suspension/resumption and revocation

Revocation of a QC is done personally by the Titular/Creator.

See the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services”.

Suspension/resumption of a QC is done personally by the Titular.

See the document “Certification Practice Statement for Providing Qualified Certificates and Trust Services”.

5.10 Certificate status

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

5.11 Termination of a Contract for Certification Services

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

6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

6.1 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 - identification center and data center (client register). Only authorized persons related to the activity of implementation of the "onboarding" process - operators and system administrators have access to them.

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

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

6.2 Procedural controls

The Provider implements a “role concept” that ensures that the relevant tasks of the RA-VI with “onboarding” 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 further 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).

6.3 Staff qualification and training

The Provider guarantees that Operators performing the “onboarding” process via videoconferencing, and the registration, have the necessary qualifications and skills. This is done by conducting training after the appointment of operators and before the implementation of production operations in the video identification centers. The provider provides a detailed training plan listing all initial and periodical training. The training documentation is part of the human resources management system and is stored in a fireproof safe. The responsibility for conducting the training lies with the head of the RA-VI team with "onboarding" process (identification center) and the human resources manager. The responsibility for conducting the training is of the RA-VI (video identification center) team leader with and the human resources manager.

The reliability of each employee is determined by the Provider, requiring all relevant documents (certificate of criminal record, resume, declaration of no conflict of interest, solvency information, etc.) of this employee.

For futher information see section 5.3 of the document “Certification Practice Statement for Providing

Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

6.4 Logging procedures

Audit logs are generated by the RA and RA-VI for all events related to the security of the "onboarding" process and related services. 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 retained and provided during compliance audits.

For further information see section 5.4 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

The collected registration records, logs, video and image materials, extracted data, results of automated checks, results of verification against registers, operator actions and electronic confirmations are retained as evidence of the identity proofing process for the retention periods and under the conditions applicable to the respective trust service and regulatory framework.

6.5 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).

6.6 Key changeover

The Provider may change the RA-VI key corresponding to the issued QC of the Video Identification Center (VIS) only by issuing a new certificate or renewing the current one with "Re-Key".

For further information see section 5.6 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

6.7 Compromise and disaster recovery

See section 5.7 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

6.8 Compromise of a Private Key

See section 5.8 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

6.9 Provider Termination

See Section 5.9 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services" of BORICA AD (B-Trust CPS-eIDAS).

7 FUNCTIONAL MODEL AND SPECIFICATION

7.1 Functional model

The RA-VI with "onboarding" is a functional element of the Registration Authority unit in the PKI of B-Trust infrastructure of BORICA. It performs all standard functions of a RA according to section 1.4.2 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services", but using the

"onboarding" process (online video identification) of an applicant for a QC as an alternative to the standard attendance identification (face-to-face). This functional element automates the procedures for requesting the issuance of a certificate, collection, authentication and validation of personal data in order to register the request for the QC securely. After the successful identification, the RA-VI registers the request as successful, provides to the smart device the data for certification in the QC for CQES/CQESeal and asks for their approval by the User.

The functions performed by the RA-VI with "onboarding" process are:

- accepting requests of a natural person - User for issuance of a QC for CQES/CQESeal from a smart device (smartphone or tablet) or a one-time CQES, QC for QES/AES/AESeal through a website for identity verification through a browser;
- carrying out verification to establish the identity of the User and specific data about him/her by performing an "onboarding" process, namely:
    - verification of the actual existence of the individual;
    - verification of possession of the official identity document by that person;
    - verification that the person is the same as indicated in the document;
    - verification of the legal validity of the official identity document;
    - if necessary, a verification of the actual existence of a legal entity and the relationship between the natural person and the legal entity is carried out.
- registering the application for issuance of a QC after successful verification and validation or rejecting the application;
- presenting to the User the validated personal data, which will be certified by a request for consent;
- notifying the CA to issue a QC.

The functional model of the “onboarding” process of the RA-VI of BORICA follows and is in accordance with section 5 (5.2 - 5.11) of this document.

7.2 Specification

The QTSP BORICA implements remote registration of Users of QCS of the B-Trust infrastructure with the RA-VI component to the unit Registration authority of this infrastructure.

The RA-VI includes the following components:

- Video Identification Server/Video Identification Center (VIS);
- Agent Portal (AP);
- Mobile Application on a smart device (smartphone or tablet);
- Specialized website through an internet browser for certificate activation.

In addition, the RA-VI uses external to the B-Trust infrastructure approved and certified sources of services in order to securely and reliably validate the identity of an individual from a distance - remote identification:

- Certified and validated "cloud services" for image analysis;
- Nationally approved and utilized service for access to public national primary registers.

7.3 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", and is applicable to the RA-VI, as a part of the RA unit in the B-Trust PKI Infrastructure of the Provider.

7.4 Operational Security

The operational security of the platform of the RA-VI 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)

7.5 Network security

The Provider uses advanced technical means for exchange and protection of information of the RA-VI with Users, with the Certification Authority and with the means providing external services (analysis of images and access to national registers) to ensure network security of the systems against external interventions and threats. The information systems and components used to perform identity verification and to determine the decision to accept, reject or escalate the identification process are logically and/or physically separated from non-critical information systems of BORICA AD, including office, administrative and supporting systems.

7.6 Information security

The information security of the components of the B-Trust infrastructure, and of the RA-VI, is part of the common information security policy of BORICA, approved by the management of the company. This policy establishes the organizational measures and procedures for the security management of the systems and information assets, through which BORICA provides all its services. The personnel having direct relations to these systems and assets is acquainted with and implement this Policy.

In accordance with the legislation on such data, BORICA as a QTSP, respectively as Provider of the service, is registered by the Commission for Personal Data Protection as a data controller.

7.7 Continuity

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

8 RISK ASSESSMENT

Considering detected business and technical problems in the delivery, operation and maintenance of the certification services, the Provider performs risk assessment to identify, analyze and assess the related risks.

Appropriate measures to avoid identified risks are chosen considering the results of the risk assessment. The measures ensure a level of security equivalent to the degree of identified risks.

The Provider documents via the Practice Statement and the Policy included as parts of this document the security requirements and operational procedures necessary to avoid identified risks for the "onboarding" process of the RA-VI.

Periodically, risk review and assessment are performed in order to overcome the identified risk factors. 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 applied "onboarding" process for remote video identification of B-Trust Users.

The risk assessment relating to the identification processes is carried out and regularly reviewed by BORICA AD in order to ensure that the procedures, technologies and organisational measures applied provide reliable establishment of the identity of applicants.

The risk assessment is reviewed at least once per year, as well as whenever a significant change occurs in the identification processes, the technological means used, the data sources or the types of identity evidence used in the onboarding process.

As part of this review, potential threats and vulnerabilities that may affect the reliability of the identity proofing process are analysed, including but not limited to:

- attempts to present **false or manipulated identity documents**;
- **presentation attacks**, involving artificially created images or video material;
- attempts to inject **pre-recorded or generated content** into the identification process (**injection attacks**);
- the use of technologies for generating **synthetic or manipulated images**, including **deep fake content**;
- attempts at fraud through **social engineering**, or attempts to mislead the operator or the automated systems;
- other threats that may lead to the incorrect establishment of the applicant's identity or to the compromise of the identification process.

Where new risks are identified or where the level of existing risks changes, BORICA AD takes appropriate technical, organisational and procedural measures to mitigate them. Such measures may include updating identification procedures, improving the technological tools used, introducing additional verification steps, or providing additional training for personnel involved in the identification process.

The results of the risk assessment are documented and presented to the management of BORICA AD, which approves the necessary risk management measures and accepts the residual risk associated with the provision of the identification service.

The risk assessment also takes into account the applicable Level of Identity Proofing (LoIP) that must be achieved for the relevant identification scenarios.

9 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

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

10 BUSINESS AND LEGAL ISSUES

The Provider 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 Provider guarantees that the RA-VI with "onboarding" process performs its functions and obligations in full compliance with the conditions in this document, with the requirements and procedures in the Policy and Practice Statement applicable to QCs, as well as the issued internal operational instructions.

The user must strictly comply with the conditions and procedures of the "onboarding" process according to this document when requesting issuance of a QC through the RA-VI, and according to the respective Policy for this certificate.

Detailed information on the business conditions and legal aspects in the relations of the Provider BORICA with Users of certification services applicable to QCs is contained in section 10 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services".