Public document

BORICA
BANK SERVICES

CERTIFICATE POLICY
AND CERTIFICATION PRACTICE STATEMENT
OF BORICA AD
FOR PROVIDING REMOTE VIDEO IDENTIFICATION
FOR ISSUANCE OF QUALIFIED CERTIFICATES FOR CLOUD QES

(B-Trust Registration Authority for Video Identification)
(B-Trust RA-VI CPS/CP-eIDAS)

Version 1.1

Effective from: 01 July 2021

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

CONTENTS

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
EGN	Uniform civil number assigned to each Bulgarian citizen
eIDAS	electronic Identification, Authentication and trust Services (EU Regulation 910/2014)
ES	Electronic Signature
ETSI	European Telecommunications Standards Institute
EU	European Union
HSM	Hardware Security Module
IP	Internet Protocol
ISO	International Standardization Organization
LRA	Local Registration Authority
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QC	Qualified Certificate
QCP-n-qscd	certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
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 – remote video 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 for CQES.

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 for CQES, 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 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;
- is entitled "Certificate Policy and Certification Practice Statement of BORICA AD for Providing Remote Video Identification for Issuance of Qualified Certificates for Cloud QES (B-Trust RA-VI CPS/CP-eIDAS)";
- 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 and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal)",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 developed in accordance 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;
- 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;
- has the nature of 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 accordance 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) 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).

The content and structure of this document is in accordance with Regulation (EU) № 910/2014 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;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification

Practices Framework.

The ETSI standards cited above state that each User must be identified in person (face-to-face) or indirectly “using means that ensure the equivalent of physical presence”.

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.

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 Web site: www.b-trust.bg

1 GENERAL PROVISIONS

This document describes the specific conditions and requirements that the QTSP BORICA fulfills through the "onboarding" process (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 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 QC for QES. The "equivalent assurance" regarding the identification of 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 document contains a description of the participants in the "onboarding" process in B-Trust in identifying natural persons (Titulars of QC), as well as describes the general operating procedures in this process, namely:

- 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 Certificate Policy and the Certification Practice Statement of the QTSP BORICA according to this document refer only to the QCs for CQES, which BORICA provides to Users according to the general documents of the Provider 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 and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal, Regulation (EU) № 910/2014 and the applicable legislation of the Republic of Bulgaria.

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.

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).

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 QC for CQES.

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**

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 above basic B-Trust general 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.

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 for CQES or one-time CQES 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;
- *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.

4 IDENTIFICATION AND AUTHENTICATION

The Provider, through its RA-VI:

- accepts requests for issuance of QC for CQES through a website via a browser or through the B-Trust mobile application on a smart device (smartphone or tablet) of a natural person - user;
- performs 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;

- registers the request for issuance of QC for CQES after successful verification and validation of the person or rejects the request;
- provides to the User the validated personal data, which are certified (requests consent);
- notifies the CA to issue a QC for CQES.

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.

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 section 3.1.1 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services", which is applicable to QC for CQES of a natural person. The RA-VI, operating on behalf of the Provider, asserts that the names in the requests for certificates for CQES 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 for CQES are real names and are checked against evidence in the form of a selfie and a copy of the identity document or passport 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 section 3.1.5 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.

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 for CQES may be included the name of the RA-VI - 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 RA-VI of the Provider for initial issuance of a QC for CQES or one-time CQES. Through the RA-VI, the Provider performs an "onboarding" process, which remotely requires, delivers and validates the necessary information for secure identification of the Titular of the certificate. Additionally, for the purposes of this process, 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.

4.2.1 B-Trust Mobile Application

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:

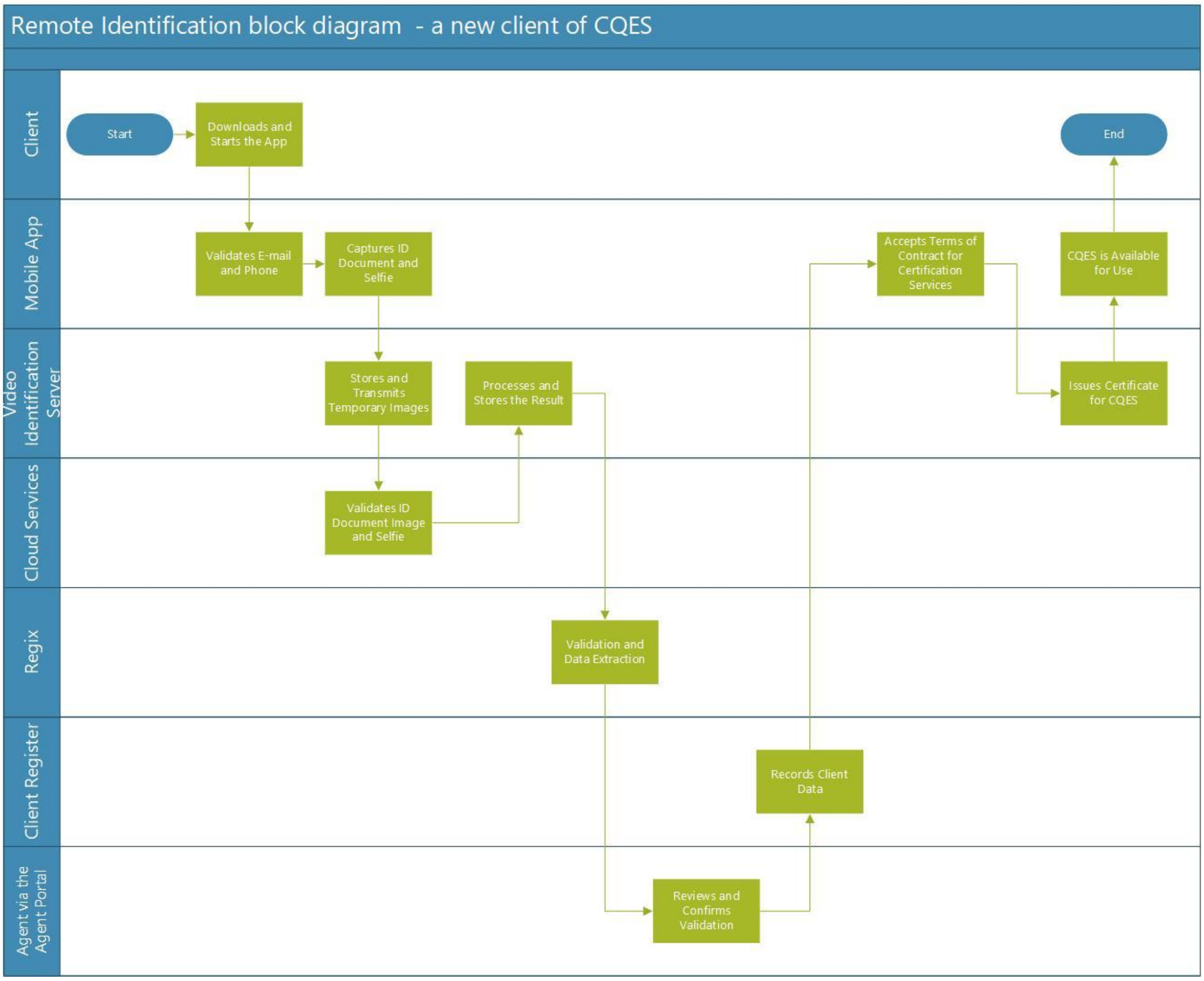
- download and install the mobile application for the respective operating system;
- start the registration process in the mobile application;
- accept the General Terms and Conditions;
- provide and validate his/her email address;
- provide and validate the phone number of the smart device he will work 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.

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


Remote Identification block diagram - a new client of CQES
Client
Mobile App
Video Identification Server
Cloud Services
Regix
Client Register
Agent via the Agent Portal
Start
Downloads and Starts the App
End
Validates E-mail and Phone
Captures ID Document and Selfie
Accepts Terms of Contract for Certification Services
CQES is Available for Use
Stores and Transmits Temporary Images
Processes and Stores the Result
Issues Certificate for CQES
Validates ID Document Image and Selfie
Validation and Data Extraction
Records Client Data
Reviews and Confirms Validation

4.2.2 Website for identity verification

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 the QTSP BORICA.

For this purpose, the User has to:

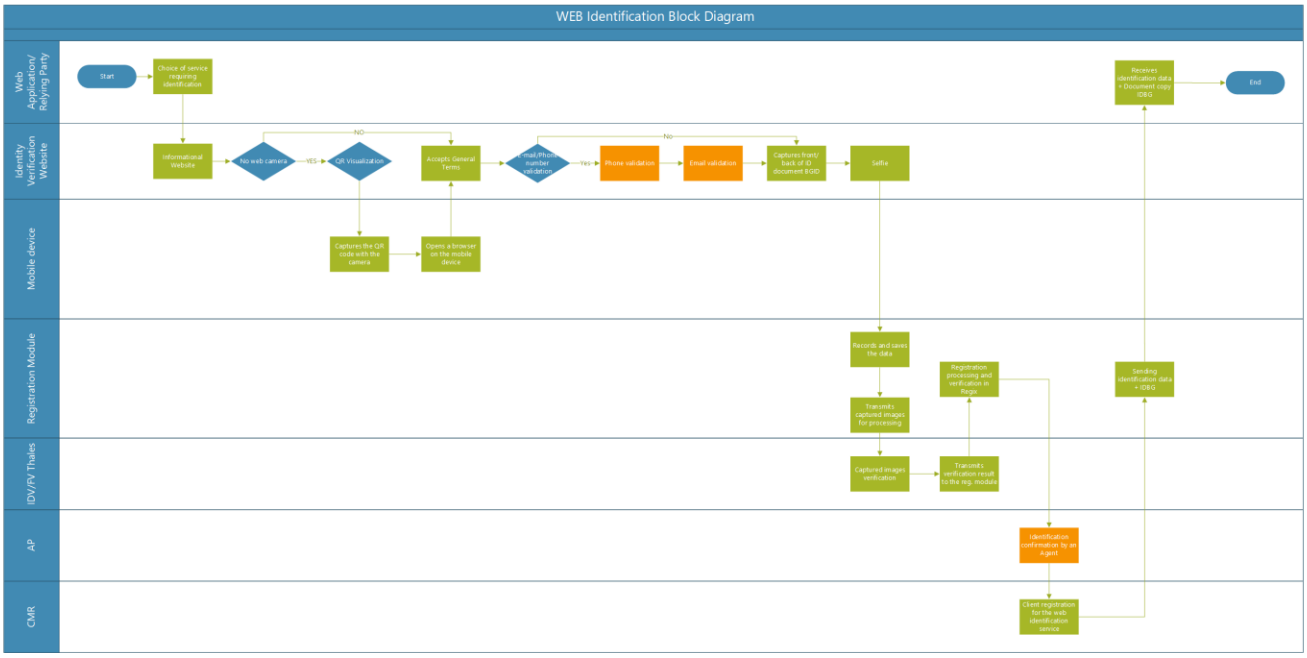
- access a specific internet address;
- start a process of registration;
- accept the General Terms and Conditions;
- provide for this purpose his/her valid mobile phone number and email address which have to be completely under his/her control;
- select the type of document with which he or she will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

To issue a one-time CQES, 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 remote identification of a User proceeds according to the block diagram presented below:


WEB Identification Block Diagram
Web Application/ Relying Party
Identity Verification Website
Mobile device
Registration Module
IDV/FV Thales
AP
CMR
Start
Choice of service requiring identification
Informational Website
No web camera
YES
NO
QR Visualization
Captures the QR code with the camera
Opens a browser on the mobile device
Accepts General Terms
E-mail/Phone number validation
Yes
No
Phone validation
Email validation
Captures front/ back of ID document BGID
Selfie
Records and saves the data
Transmits captured images for processing
Captured images verification
Transmits verification result to the reg. module
Registration processing and verification in Regix
Identification confirmation by an Agent
Client registration for the web identification service
Sending identification data + IDBG
Receives identification data + Document copy IDBG
End

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 for CQES, i.e. consent to the Provider to issue the qualified certificate.

After successful identification, a profile of the User of QC for CQES or one-time CQES 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.

After successful registration of a User through the "onboarding" process, the RA-VI prepares a request for issuance of a QC for CQES by:

- generating a key pair for the QC for CQES;
- selecting an option for authorization (possession of the smart device with the mobile application) of the User when signing with CQES.

Verification for holding the private key by the natural person, corresponding to the issued public key for QC for CQES is not applicable. It can be performed only if the key pair is generated by the User. The CQES key pair is generated by the Provider (in RQSCD/HSM).

An issued QC for QES is not handed over to the User-Titular. The provider publishes it in the B-Trust Public Register of Certificates, and the generated key pair for this cloud QES is stored in the RQSCD (HSM) of the cloud QES platform. The authentication and the key pair are associated with the user account of the Titular and with his mobile device with the mobile application.

4.2.3 Special Attributes

See section 3.2.4. 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.

4.2.4 Unverified information

See section 3.2.5 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-VI, is certified in the issued certificate for CQES.

4.3 Validation of Identity for Renewal

See section 3.3 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, 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 for CQES 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 section 3.4 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, 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.

See section 3.5 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, and section 4.2 (Initial validation of identity) of this document.

5 OPERATIONAL REQUIREMENTS AND PROCEDURES

1. The Provider, through the RA-VI, within the framework of a Contract for QCS, performs the following operating procedures applicable to the QC for CQES:
   - registration of request for issuance via “onboarding” process (validation of identity);
   - issuing;
   - handover of an issued QC;
   - use of key pair and QC;
   - suspension / resumption;
   - revocation;
   - QC status;
   - Provider’s termination.

5.1 Request for Issuance of Certificate

The issuance of a QC for CQES 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 one-time CQES 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.

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 of a smart device of a User by the RA-VI of the Provider is similar by exchanging SMS-messages with a unique code.

The last step in the initialization is protection of the application on the smart device when starting registration, i.e. participation in the "onboarding" process. The application requires and the User sets a password. If the smart device supports biometric authentication, the User can activate it and use it at login.

5.2 Onboarding process and registration (identity validation)

Regarding this document, the User is a natural person, who is the Titular of the requested QC for CQES or one-time CQES.

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 for one-time CQES;
- 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 RA-VI of BORICA accesses cloud services in order to:

- transmit captured images of the identity document and selfie;
- check the quality of the captured images;
- perform a check for validity of the identity document;
- extract the data (OCR) and the image of the person from the identity document;
- check for the matching of the face image in the identity document with the selfie.

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

The information channel of exchange between the RA-VI of the Provider and the cloud services is secure (HTTPS protocol).

5.2.4 Validation of the official identity document

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

5.2.4.1 Available Regix service - natural person-Bulgarian citizen

The RA-VI verifies the data received from Regix with those from the official document (status report) received from the cloud service. After successful verification of the validity of the identity document, the User data are extracted from Regix and recorded in the client register of B-Trust (BORICA).

The mobile application notifies the User of successful identification and registration.

5.2.4.2 Unavailable Regix service - natural person-Bulgarian citizen

If the Regix service is not available, the RA-VI notifies the User and 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 pending list 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 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-VI through the "onboarding" process validates the identity of the Applicant-natural person, delivers the personal data that the Provider will certify in QC for CQES 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"

In all cases, the Provider through the RA-VI with "onboarding" process establishes the identity of the interpreter and the witnesses by the order of item 4.2 of this document. The identity data of the interpreter and the witnesses are recorded in the registration record for the User in the client register of the Provider BORICA.

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 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 for CQES has been accepted.

The validated identification data, which the Provider will certify in the QC, are visualized in the application on the smart device 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 for CQES 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 for CQES only at the time of its issuance.

5.3.4 Technical request for issuance (PKCS # 10)

The User should:

- 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 for CQES, 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 of the User.

The User reviews the contract and the associated Policy and Practice (this document) and accepts / confirms them.

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

According to 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.

According to 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 “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)”, applicable to QC for CQES of a natural person.

5.6 Certificate renewal

QC for CQES is not renewed. Having a valid Cloud QES, the user may at any time request the issuance of a new Cloud QES - 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 CQES 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 the QC for QES is done personally by the Titular.

According section 4.9 (4.9.1-10) 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, and section 4.5 (Validation of Identity for Revocation) of this document.

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

According section 4.9 (4.9.11-16) 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, and section 4.4 (Validation of Identity for Suspension/Resumption) of this document.

5.10 Certificate status

According to section 4.10 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.

5.11 Termination of a Contract for Certification Services

According to section 4.11 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.

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 more 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 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).

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 more 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-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 more 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).

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 more 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

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).

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 QC for CQES or applicant for a one-time CQES 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 at the CA and asks for their approval by the User. The latter confirms the submitted personal data, which the Provider will certify in the QC for CQES or one-time CQES and selects an option to authorize signing with CQES.

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

- accepting requests for issuance of QC for CQES from a smart device (smartphone or tablet) or one-time CQES through a website for identity verification through a browser of a natural person - User;
- 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;
- registering the application for issuance of a QC for CQES after successful verification and validation or rejecting the application;
- registering the application for issuance of a one-time CQES 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 for CQES.

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);
- Website through an internet browser

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) (sections 6.6, 6.7, and 6.8).

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.

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.

9 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).

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 CQES, 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 QC for CQES 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 QC for CQES is contained in section 10 of the document "Certification Practice Statement for Providing Qualified Certificates and Trust Services".