Public document

CERTIFICATE POLICY
AND CERTIFICATION PRACTICE STATEMENT
FOR PROVIDING REMOTE VIDEO IDENTIFICATION SERVICE

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

Version 2.0

Effective from 15 March 2023

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	01.01.2021	Approved	Initial release
2.0	Margarita Boneva	15.03.2023	Approved	Technical corrections

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 TSP).

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.

Customer – 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 as of 15.03.2023;
- is entitled “Certificate Policy and Certification Practice Statement for Providing Remote Video Identification Service (B-Trust RA-VI CPS/CP-eIDAS)”;
- has been drawn up in accordance with the formal requirements for content, structure and scope, and the international specifications ETSI EN 319-401 including the sections that are specific and applicable to the “onboarding” process;
- addresses only Registration Authority using remote video identification (RA-VI), but includes texts, explanations and references regarding the compliance of the RA-VI with the requirements for a 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) 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:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;

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 referred to in this document uses "onboarding" process for remote online video identification, providing a level of security equivalent to physical presence.

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

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. The natural person participates in the "onboarding" process via a website through a browser or via 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.

The document contains a description of the participants in the "onboarding" 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.

Personal data is processed in a way that ensures a high level of security and appropriate technical and organizational measures are applied.

In case of failed identification, the process is redirected to an operator of the RA-VI for video conference call.

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

1.1 Certifying Authority of BORICA

This 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 is available in the document B-Trust CPS-eIDAS.

BORICA has informed the CRC about onset of activity as a QTSP in accordance with the EDETSA and the current legislation. The Provider shall notify the Users of its accreditation when 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 QCSs 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, which is effective at the time of using QC for CQES, is considered valid.

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 TSP, 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 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 the 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 of 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.

2 PARTICIPANTS IN THE "ONBOARDING" PROCESS

To establish identity through a remote video identification system, procedures are applied that ensure a high level of security and reliability of the verified information identifying the users of the TSP. The RA-VI provides a service for verification of only those identification data that are relevant and comply with the requirements for lawful processing of personal data in accordance with the GDPR.

The following parties participate in the "onboarding" process of BORICA:

- *User* - a natural person whose identity should be securely and reliably verified and validated before being successfully registered in the Provider's database.

- *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.
- *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 or through a website via a browser. It supervises and manages the successive steps in the implementation of the "onboarding" process.

3 IDENTIFICATION AND AUTHENTICATION

The Provider, through their RA-VI:

- performs verification to establish the identity of the User and specific data about him/her through the implementation of "onboarding" process including:
  - 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;

The Provider guarantees that individuals are properly identified and duly verified.

3.1 Naming

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

3.1.1 Use of pseudonyms

Pseudonyms (as well as anonymity) are not accepted by the RA-VI. All names of Users 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.

3.2 Remote identity verification of a natural person

A user accesses a specific Internet address or uses a smart device (smartphone or tablet) with the B-Trust mobile application in it. The user is prompted to place the front of the ID document in front of the camera. The user specifies the type of document being captured, and depending on the type specified, one or more pages of the document are required to be captured. The personal data of the User are entered automatically after scanning the identity document. The validity of the identity document is verified through national registers or reliable data sources. The system requires the User to take a photo of himself (selfie), following the instructions for performing liveness detection. A procedure for automated analysis of facial biometrics is performed through a series of controls. The record of the process of identification of the Users of the Provider necessarily pass an inspection by an operator of the RA-VI of BORICA.

The minimum set of personal data for natural person that is collected and verified for identification purposes is:

- surname(s);
- first name(s);
- father's name(s);

- a 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 a 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).

If 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.

3.3 Identity verification of a legal person

Verification of the identity and authenticity of a legal entity has two purposes:

- to prove that the legal entity exists during the inspection of the application;
- to prove that the representative has received permission from the legal entity to represent him.

The establishment of the identity of a legal entity is verified by verification in reliable sources. The minimum set of data for a legal entity may contain the following data:

- legal name (company);
- national unique identifier.

The data set for a legal entity may contain additional specific data:

- company address;
- VAT registration number, when different from the national unique identifier.

The RA-VI shall terminate the identification process if during the inspection it is established that the representative power of the natural person towards the legal entity has been terminated.

3.4 Special Attributes

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

3.5 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 OPERATIONAL REQUIREMENTS AND PROCEDURES

4.1 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 for use of the mobile application.

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

The User enters and sends his/her 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 the User to set a password. If the smart device supports biometric authentication, the User can activate it and use it at login.

4.3 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.

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

A User accesses the identity verification website 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.

4.5 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 receive 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).

4.6 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.

4.6.1 Available service to primary registers – natural person Bulgarian citizen

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

4.6.2 Unavailable service to primary registers – natural person Bulgarian citizen

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 recorded to a list of pending validity confirmation by an Operator. A Qualified RA-VI Operator receives 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 actions 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 signing it electronically.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 Archiving

The Provider records and stores information related to the identity verification process in accordance with applicable legislation and good practices regarding data protection and storage.

5.6 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).

6 FUNCTIONAL MODEL AND SPECIFICATION

6.1 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.

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

- 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;

The functional model of the “onboarding” process of the RA-VI of BORICA follows and is in accordance with Section 4 of this document.

6.2 Specification

The QTSP BORICA implements remote registration of Users with the RA-VI component to the Registration authority unit 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 a natural person 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.

6.3 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.

6.4 Operational Security

The operational security 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).

6.5 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.

6.6 Information security

The information security of the components of the B-Trust infrastructure, including 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. Signed/sealed electronic documents with a QES/QESeal may contain information that can be considered personal data. 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.

6.7 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.

7 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.

8 INSPECTION AND CONTROL OF PROVIDER’S ACTIVITIES

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

9 BUSINESS AND LEGAL ISSUES

The Provider guarantees that the RA-VI with "onboarding" process performs its functions and obligations in full compliance with the conditions in this document, 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.