CERTIFICATION PRACTICE STATEMENT

OF BORICA AD

FOR PROVIDING QUALIFIED CERTIFICATES AND QUALIFIED TRUST SERVICES

(B-Trust CPS-eIDAS)

Version 7.1

Effective from:

01 July 2021

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
3.2	Dimitar Nikolov	13.01.2017	Approved	Amendments to the document related to the implementation of Regulation 910/2014.
4.0	Dimitar Nikolov	01.06.2017	Approved	Dividing the document to a common practice statement in providing qualified trust services and relevant policies. Adding practice statement in providing qualified certificates for qualified electronic seal. Adding practice statement in providing qualified certificates for cloud qualified electronic signature. Adding practice statement in providing qualified certificates for qualified electronic seal. Adding practice statement in providing qualified services for validation of qualified electronic signatures and seals.
5.0	Dimitar Nikolov	01.04.2019	Approved	Added Qualified electronic signatures and seals validation service and Qualified preservation service for qualified electronic signatures and seals
6.0	Dimitar Nikolov	01.03.2020	Approved	Technical corrections
6.1	Dimitar Nikolov	01.10.2020	Approved	Additional requirements for user identification
7.0	Dimitar Nikolov	01.01.2021	Approved	Added process for remote identification
7.1	Margarita Boneva	01.07.2021	Approved	Corrections

CONTENTS

LIST OF TERMS AND ABBREVIATIONS

AES	Advanced Electronic Signature
AESeal	Advanced Electronic Seal
BG	Bulgaria
B-Trust QHSM	Qualified HSM in the cloud-based QES platform with a security profile meeting the EAL 4+ or higher security level according to CC or other specification defining equivalent security levels
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation - International Standard for Information Security (ISO/IEC 15408)
CEN	European Committee for Standardization
CENELEC	European Committee for Electro-technical Standardization
CP	Certificate Policy – Policy on the provision of trust services
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CQES	Cloud Qualified Electronic Signature
CQES_OT	One Time CQES
DSA	Digital Signature Algorithm
DN	Distinguished Name
eIDAS	EU Regulation 910/2014
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and Council relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data
HSM	Hardware Security Module
IEC	International Electro-technical Commission
ISO	International Standardization Organization
IP	Internet Protocol
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QC	Qualified Certificate
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
RA	Registration Authority
RSA	Rivest – Shamir - Adelman
QSCD	Qualified Signature Creation Device - (local) device for secure creation of qualified signature in accordance with EU Regulation 910/2014

QHSM	HSM with security level as QSCD
RA-VI	Registration authority using remote video identification
RQSCD	Remote QSCD – server component with QHSM for secure creation of remote signature
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SAM	Signature Activation Module
SCT	Signature Creation Token (PKCS#12 crypto-file)
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TRM	Tamper Resistant Module
URL	Uniform Resource Locator
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
QCP-l-qscd	Certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
QCP-w	Certificate policy for EU qualified website authentication certificates

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;
- Fully replaces all previous versions of the User Guide and/or "Certificate Policy on issuing qualified certificates for qualified electronic signature and Certification Practice in the provision of qualified trust services by BORICA AD";
- Is effective as of 01.07.2021;
- Contains the conditions under which the Qualified Trust Service Provider (QTSP) BORICA AD (the Provider) provides to Users for payment Qualified Certificates (QCs) and Qualified Trust Services (QTS) for Electronic Signature (ES), for Cloud Electronic Signature, for Electronic Seal (ESeal) and for website authentication, as well as other information, cryptographic and consulting services under the registered trade mark B-Trust, through its administratively independent unit - B-Trust® Certification Authority, in accordance with the requirements of the Electronic Document and Electronic Trust Services Act (EDETSA);
- Constitutes the General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These conditions are part of the Certification Services Contract, which is concluded between the Provider and Users. 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 with the EDETSA and the legal framework;
- Includes a detailed description of the practice of the Provider in providing QCs and related QCSs, and is a public document with the purpose to establish the conformity of the activity of the Provider BORICA with the EDETSA and the legal framework;
- is publicly available at any time 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 is prepared in accordance with:

- Electronic Document and Electronic Trust Services Act (EDETSA);
- Ordinance on the Activities of Trust-Service-Providers;
- Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature;
- 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.

The contents and structure of this document is in accordance with Regulation (EU) № 910/2014 and refers 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;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;

- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1/5: Certificate Profiles;
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles;
- ETSI EN 419 241, part 2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- ETSI EN 419 241, part 3 – Trustworthy Systems Supporting Server Signing – Part 3: Protection profile for Signature Activation Data management and Signature Activation Protocol(PP-SAD+SAP);
- ETSI EN 419 221-5 - Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- ETSI TS 119 312 – ESI Cryptographic Suites;
- ETSI TS 119 495 – ESI Sector Specific Requirements: Qualified Certificates Profiles and TSP Policy Requirements under the PSD2;
- ETSI TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

Additional information relating to this document may be obtained by 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

INTRODUCTION

The Certification Practice Statement for providing Qualified Certificates and Trust Services by BORICA contains a description of the participants in the public key infrastructure of B-Trust® and its components, used by the Provider to issue, maintain, publish and manage QCs for QES/AES, for Cloud QES, for QESeal/AESeal and for website authentication. It describes the general operating procedures in ordering QCs, identification of Applicants, issuing and publishing, delivery and acceptance of QCs, maintenance and management of these certificates, and procedures for granting access for verification of the certificates.

The Practice also includes the measures and technical procedures followed by the Provider to ensure safety and reliability of the QCs and related QCSs provided via the B-Trust® infrastructure, in accordance with the EDETSA and other relevant regulations.

The document has been developed in accordance with the formal requirements for content, structure and scope, as set out in international guideline RFC 3647, as far as this guideline is in line with the management policy of the Provider.

The document also includes additional information with regard to the requirements under the EDETSA.

1 GENERAL TERMS

1.1 Qualified Trust Service Provider

1. BORICA AD is a legal person – trader, operating as a QTSP under the EDETSA and other relevant regulations.
2. The PKI of BORICA is built and managed 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.
3. The Provider uses OIDs in the B-Trust PKI Infrastructure, formed on the basis of code 15862, assigned to BORICA AD 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 ISO / IEC 9834-1: 2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).
4. As a registered QTSP, BORICA AD carries out the following regulated activities:
   - QC issuance:
     - accepting application for initial issuing;
     - identifying and validating User's data;
     - providing services for creating cryptographic key pairs - private and public key
     - signing QC with advanced electronic signature/seal of the QTSP;
     - recording issued QC.
   - QC maintenance and management:
     - renewal of an issued valid QC;
     - changing the status of a valid QC - suspension, resumption and revocation;
     - check of the status of a QC;
     - check of the status of a QC in real time (OCSP status).
   - keeping registers:
     - keeping a Public Register of all QCs issued;
     - publication of QC issued in the Public Register;
     - keeping list of all QCs that have been revoked;
     - immediate publication of a revoked QC on the Certificate Revocation List;
     - providing permanent third-party access to the public register and the Certificate Revocation List.
   - validation of electronic signatures.
   - providing QSCD for (local) generation and storage of cryptographic keys and for creation of QES – smart card/s.
   - providing RQSCD for generation and storage of cryptographic keys at the QTSP and for remote creation of QES (Cloud QES/CQES).
   - issuance of qualified electronic time stamps:
     - of presented content of an electronically signed/sealed document (time of signing/sealing);
     - of digital content before a specified moment and unchangeability of the content after this moment;
     - evidence-based verification of qualified electronic time-stamp tokens issued.
5. The Provider provides the QCSs specified in accordance with the current Practice Statement of the Certification Authority and the Policy specified in the respective certificate.
6. The Provider may provide other qualified certification, cryptographic, information and consultancy services relating to the applicability of the trust services, following generally accepted recommendations, specifications and standards.
7. The Provider may publish separate terms and conditions for these QCSs.

1.2 Regulation and Control

1. The full title of this document is "Certification Practice Statement for the provision of Qualified Certificates and Qualified Trust Services by BORICA AD (B-Trust CPS-eIDAS)".
2. BORICA AD has informed the CRC of the start of operations as a QTSP under the EDETSA and current regulations.
3. The accreditation of BORICA AD as a QTSP under the EDETSA aims to achieve the highest security level for the QCSs provided and better harmonization of these activities with similar activities provided in other Member States of the European Union.
4. The Provider shall notify all Users of this accreditation during the provision of QCSs specified in this document.
5. In relations with Users and third parties, only the version of the document that is current at the time of using the services of BORICA AD is valid.
6. This document is publicly available at https://www.b-trust.bg/documents.
7. The Practice Statement for the provision of Qualified Trust Services is applicable to the following Certificate Policies of the Provider:
   - Certificate Policy on the Provision of Qualified Certificates for Qualified Electronic Signature/Cloud Electronic Signature/Seal (B-Trust CP-eIDAS QES/CQES/QESeal);
   - Certificate Policy on the Provision of Qualified Certificates for Advanced Electronic Signature/Seal (B-Trust CP-eIDAS AES/AESeal);
   - Certificate Policy on the Provision of Qualified Certificates for Website Authentication (B-Trust QCP-eIDAS QWAC);
   - Certificate Policy on the Provision of Qualified Certificates for Electronic Seal and Website Authentication to Payment Service Providers (B-Trust QCP-PDS2 QSealC and QWebC).

   These policies meet the specific certification policy requirements set out in ETSI EN 319 411-2: QCP-n; QCP-l-qscd, QCP-l, QCP-l-qscd, and QCP-w based on the general requirements in the relevant NCP and NCP+ policies specified in ETSI EN 319 411-1.
   The Provider's Certificate Policies for the specific types of Qualified Certificates are published in separate documents and are publicly available at https://www.b-trust.bg/documents.

1.3 Identifiers in the Document

8. The objects in the B-Trust infrastructure of BORICA AD for issuing and maintaining qualified certificates are identified by Object Identifiers (OID).
9. The qualified certificates for signature, seal and website authentication as objects of the infrastructure are identified by the identifiers of the respective certificate policy that can be checked in the Certificate Policies attribute.
10. The B-Trust object identifiers are listed in the following table:

Object	Identifier (OID)
BORICA AD	1.3.6.1.4.1.15862
B-Trust	1.3.6.1.4.1.15862.1
B-Trust Root Qualified CA	**1.3.6.1.4.1.15862.1.6**
B-Trust Operational Qualified CA	**1.3.6.1.4.1.15862.1.6.1**
B-Trust Personal qualified certificate QES	1.3.6.1.4.1.15862.1.6.1.1
B-Trust Professional qualified certificate QES	1.3.6.1.4.1.15862.1.6.1.2
B-Trust Organization qualified certificate QESeal	1.3.6.1.4.1.15862.1.6.1.3
B-Trust PDS	1.3.6.1.4.1.15862.1.6.2
B-Trust Qualified Time Stamp Authority	1.3.6.1.4.1.15862.1.6.3
B-Trust Qualified Time Stamp Authority PDS	1.3.6.1.4.1.15862.1.6.4
B-Trust Root Qualified OCSP Authority	1.3.6.1.4.1.15862.1.6.5
B-Trust Qualified OCSP Authority	1.3.6.1.4.1.15862.1.6.5.1
B-Trust Qualified Validation Service	1.3.6.1.4.1.15862.1.6.6
B-Trust Qualified Long-Term Preservation Service	1.3.6.1.4.1.15862.1.6.7
B-Trust Remote QSCD (RQSCD)/Server Signing Service Component	1.3.6.1.4.1.15862.1.6.8

B-Trust Remote Signature Creation Service Component	1.3.6.1.4.1.15862.1.6.9
B-Trust Remote Video Identification Service Component	1.3.6.1.4.1.15862.1.6.10
B-Trust Root Advanced CA	**1.3.6.1.4.1.15862.1.7**
B-Trust Operational Advanced CA	**1.3.6.1.4.1.15862.1.7.1**
B-Trust Personal qualified certificate AES	1.3.6.1.4.1.15862.1.7.1.1
B-Trust Professional qualified certificate AES	1.3.6.1.4.1.15862.1.7.1.2
B-Trust Organization qualified certificate AESeal	1.3.6.1.4.1.15862.1.7.1.3
B-Trust Application qualified certificate	1.3.6.1.4.1.15862.1.7.1.4
B-Trust Domain Validation SSL qualified certificate (B-Trust DVC SSL)	1.3.6.1.4.1.15862.1.7.1.5
B-Trust Organization Validation SSL qualified certificate (B-Trust OVC SSL)	1.3.6.1.4.1.15862.1.7.1.6
B-Trust Organization qualified certificate AESeal PSD2	1.3.6.1.4.1.15862.1.7.1.7
B-Trust Organization Validation SSL qualified certificate PSD2	1.3.6.1.4.1.15862.1.7.1.8
B-Trust PSD2 PDS	1.3.6.1.4.1.15862.1.7.1.9
B-Trust Root Advanced OCSP Authority	1.3.6.1.4.1.15862.1.7.2
B-Trust Advanced OCSP Authority	1.3.6.1.4.1.15862.1.7.2.1

11. The Provider's Practice Statement for issuing and maintaining QCs is implemented through the following operational CAs:

Operational CA	**Identifier (OID)**
B-Trust Operational Qualified CA	1.3.6.1.4.1.15862.1.6.1
B-Trust Operational Advanced CA	1.3.6.1.4.1.15862.1.7.1

OB

12. The Certificate Policies of the Provider regarding the types of QCs and related QCSs are identified in the issued QCs by the following identifiers:

Qualified Certificate	**Certificate Policy**	**Policy OID**
B-Trust Personal qualified certificate for QES B-Trust Personal Qualified certificate for CQES	B-Trust Personal qualified certificates Policy (QCP-n-qscd)	1.3.6.1.4.1.15862.1.6.1.1 (0.4.0.1456.1.1) (0.4.0.194112.1.2)
B-Trust Professional qualified certificate for QES B-Trust Professional qualified certificate for CQES	B-Trust Professional qualified certificates Policy (QCP-n-qscd)	1.3.6.1.4.1.15862.1.6.1.2 (0.4.0.1456.1.1) (0.4.0.194112.1.2)
B-Trust Organization qualified certificate for QESeal	B-Trust Organization qualified certificates Policy (QCP-l-qscd)	1.3.6.1.4.1.15862.1.6.1.3 (0.4.0.194112.1.3)
B-Trust Personal qualified certificate for AES	B-Trust Personal qualified certificates Policy (QCP-n)	1.3.6.1.4.1.15862.1.7.1.1 (0.4.0.1456.1.2) (0.4.0.194112.1.0)
B-Trust Professional qualified certificate for AES	B-Trust Professional qualified certificates Policy (QCP-n)	1.3.6.1.4.1.15862.1.7.1.2 (0.4.0.1456.1.2) (0.4.0.194112.1.0)
B-Trust Organization qualified certificate for AESeal	B-Trust Organization qualified certificates Policy (QCP-l)	1.3.6.1.4.1.15862.1.7.1.3 (0.4.0.1456.1.2) (0.4.0.194112.1.1)
B-Trust Domain Validation SSL qualified certificate (B-Trust DVC SSL)	B-Trust certificate for Domain Validation Certificate Policy (DVCP)	1.3.6.1.4.1.15862.1.7.1.5 (0.4.0.2042.1.6)
B-Trust SSL Organization Validation qualified certificate (B-Trust OVC SSL)	B-Trust certificate for Organization Validation Certificate Policy (OVCP)	1.3.6.1.4.1.15862.1.7.1.6 (0.4.0.2042.1.7)
B-Trust Organization qualified certificate AESeal PSD2 (B-Trust QSeal PSD2)	B-Trust PSD2 Organization qualified certificates Policy (QCP-l)	1.3.6.1.4.1.15862.1.7.1.7 (0.4.0.1456.1.2) (0.4.0.194112.1.1)
B-Trust SSL Organization Validation	B-Trust certificate for PSD2	1.3.6.1.4.1.15862.1.7.1.8

qualified certificate PSD2 (QWebC PSD2)	Organization Validation Certificate Policy (OVCP)	(0.4.0.2042.1.7)

1.4 Participants in the B-Trust® Infrastructure

1.4.1 Certification Authority

1. The B-Trust® "Certification Authority" of the QTSP "BORICA" AD is a separate organizational unit, which operates activities on issuance, provision and maintenance of QCs and QCSs for them. The CA has no legal personality and all operations and activities of its employees are performed in their capacity of employees of the Provider, within the powers granted to them.
2. The B-Trust® infrastructure has a two-tier hierarchy of the CA for issuing and maintaining QCQES and QCQESeal, as follows:
   - ***"B-Trust Root Qualified CA"*** - issuing certificates to subordinate operational certification authorities of the Provider and those of other Providers;
   - ***„B-Trust Operational Qualified CA"*** - issuing QCQES and QCQESeal under the policies for provision of these QCs;
3. The B-Trust® infrastructure has a two-tier hierarchy of the CA for issuing and maintaining QC for QES and QC for QESeal, as follows:
   - ***"B-Trust Root Qualified CA"*** - issuing certificates to subordinate operational certification authorities of the Provider and those of other Providers;
   - ***„B-Trust Operational Qualified CA"*** - issuing QCAES and QCAESeal under the policies for provision of these QCs.
4. The QTSP reserves the right to expand the B-Trust® infrastructure with further hierarchy of CA.

1.4.2 Registration Authority

1. "Registration Authority" is a unit performing activities of the Provider, as follows:
   - accepts, verifies, approves or rejects applications for the issuance of QCs;
   - registers applications submitted to the CA for issuance and makes changes to the status of QCs;
   - performs appropriate checks to verify the identity of the natural persons and the legal persons, as well as specific details about them by the eligible means;
   - notifies the CA to issue a QC after successful identification and service paid;
   - delivers to the User or an authorized person the QC issued, corresponding to a generated key pair;
   - accepts or rejects registered requests for maintenance and management of QCs;
   - concludes contracts for the provision of certification and other cryptographic, information and consultancy services with the Users on behalf of the Provider.
2. The Registration Authority carries out the above activities:
   - at the Authority's office requiring the physical presence of the applicant for QC (attendance identification, registration and QC issuance);
   - via remote online video identification of the applicant (nonattendance identification, registration and QC for CQES issuance).
3. The Policy and the Practice of a RA performing the activities under item 1 at the Authority's office are an integral part of this document.
4. The Policy and the Practice of a RA performing the activities under item 1 via remote online video identification are in a separate document – "Certificate Policy and Certification Practice Statement for Providing Remote Video Identification for Issuance of Qualified Certificates for Cloud QES by BORICA AD (B-Trust RA-VI CPS/CP-eIDAS)"
5. The Provider's Registration Authority may provide certification services to Users at an office

(attendance) through Local Registration Authorities (LRA).
6. The Registration Authority may be a separate unit within a legal entity other than Provider, with delegated rights to perform these activities or part of them on behalf of the Provider.
7. The Provider's Registration Authority (RA) may provide trust services to Users via the Local Registration Authorities (LRA).
8. When the RA/LRA is a separate legal person, the power to carry out this activity may be limited by territory, term, trust services, or for a particular category of Users. The power is certified to all Applicants and third parties with a written or electronic certificate of the RA/LRA.
9. In cases where the RA is a separate legal person, LRAs to this body may be opened only after the explicit approval of the Provider.
10. The relations between the Provider and the RA /LRA are regulated by a contract.
11. The Provider guarantees that the activities of the RA/LRA follow the terms of this Document.

1.4.3 Qualified Electronic Time Stamp Authority

1. The "Qualified Electronic Time Stamp Authority" is a separate and indivisible unit to the Certification Authority, which executes the following activities of the Provider:
   - accepts requests for issuing qualified electronic time stamp tokens of the content of an electronic document presented by a User or a Relying Party;
   - prepares qualified electronic time stamp token of the presented hash value of the electronic document;
   - allows for subsequent verification (after the period of validity of the QC) to the accepting party, the fact of signing/sealing a statement or an electronic document.
2. The "B-Trust Qualified Time Stamp Authority" is the Provider's authority issuing qualified electronic time stamp tokens.
3. The electronic signature of the Provider on the qualified electronic time stamp has the status of a qualified electronic time stamp token.
4. Qualified electronic time stamp tokens can be integrated in the process of creation or approval of signatures/seals to electronic documents and electronic transactions, in the archiving of electronic data, to electronic notaries, etc.
5. The Provider shall develop and publish a separate Policy of the Qualified Electronic Time Stamp Authority.

1.4.4 Qualified Service for Validation of Qualified Electronic Signature/Seal

1. The Qualified Service for Validation of Qualified Electronic Signatures/Seals (B-Trust QSVS) is a separate and indivisible unit of the Provider, which performs the following activities:
   - accepts signed/sealed files/e-documents with certain formats and profiles of signature/seal for validation;
   - validates the signed/sealed files/e-documents in accordance with Regulation 910/2014 (Articles 32, 33 and 40);
   - Prepares and provides status(es) and report, sealed by the Provider, on validation of e-signature(s)/e-seal(s) in accepted files/e-documents;
   - Enables printing (PDF format) of the Authorized report of validation of signature(s)/seal(s).
2. The service authorizes the status and the report on validation by a qualified electronic seal issued by the Provider.
3. The validation statuses of qualified e-signatures/e-seals can be integrated in processes of acceptance of signatures/seals to electronic documents and electronic transactions, etc.
4. The Provider shall develop and publish a separate Policy and Practice Statement of Qualified Service for validation of QES/ QESeals.

1.4.5 Qualified Service for Preservation of Qualified Electronic Signature/Seal

1. The 1.4.5 Qualified Service for Preservation of Qualified Electronic Signatures/Seals (B-Trust QSPS) is a separate and indivisible unit of the Provider, which performs the following activities:

- accepts e-signatures/e-seals (signed/sealed files/e-documents) with certain formats and profiles of signature/seal for preservation;
- securely preserves signed/sealed files/e-documents in accordance with Regulation 910/2014 (Articles 34 and 40);
- Prepares and provides evidence records of preservation, sealed by the Provider, of e-signature(s)/e-seal(s) in accepted files/e-documents;
- Prepares notifications upon request after successful preservation of signed/sealed files/e-documents;
- Enables authorized access, reading, modification and deletion of preserved signed/sealed files/e-documents.

2. The service authorizes the evidence records and notifications by a qualified electronic seal issued by the Provider.
3. The Provider shall develop and publish a separate Policy and Practice Statement of Qualified Service for preservation of QES/ QESeals.

1.4.6 Cloud QES Platform

1. The Cloud QES Platform consists of two parts:
   - Remote server component RQSCD (software and HSM) at the Provider;
   - Mobile application (B-Trust Mobile) on a User's smartphone.
2. RQSCD is a detached and integral component of the B-Trust infrastructure of the Provider, which performs the following activities:
   - Generates key-pair for cloud QES in HSM at the Provider, at the request of a certified User
   - Stores securely the generated key-pair at the Provider
   - Activates remote generation of digital signature (PKCS#1)
   - Generates digital signature of a Signatory in the HSM at the Provider (Cloud QES)
   - Provides the generated signature and the corresponding certificate for verification of the signature to the Signatory
3. RQSCD receives the requests for issuance of cloud QES through the RA/LRA of the Provider after successfully verified Applicant and registered mobile device (smartphone) of the Applicant.
4. RQSCD uses B-Trust Operational CA of the Provider to issue a qualified certificate corresponding to the generated remote signature.
5. The B-Trust Mobile application on the smartphone of the Signatory serves to activate generation of a digital signature for cloud QES in the HSM of the RQSCD only after sole control assurance of the private key of the signature through strict authentication of the Signatory and entered PIN (activation code) through the mobile device (smartphone).
6. The provided by the Platform digital signature and corresponding qualified certificate of the Cloud QES can be integrated in the container of signed documents with Cloud QES by a signing service operated by the Provider or by an external one (at the Signatory/Relying party).

   The Cloud QES Platform "relocates"/virtualizes the physical smart card (local QSCD) for QES of the Signatory to the HSM of the RQSCD at the QSTP. A "virtual slot" is allocated in the RQSCD as remote resource of the Signatory with equivalent cryptographic parameters and characteristics of the smart card (local QSCD).

1.4.7 OCSP server

1. "OCSP server" is a separate and indivisible unit of the CA, which executes the following activities of the Provider:
   - accepts requests from Users or Relying Parties for real-time check of the status of a certificate issued by the Provider;

- prepares automatically in real time an electronically signed response on the status of a certificate.

2. The OCSP servers are „B-Trust Root Qualified OCSP Authority" and „B-Trust Qualified OCSP Authority", and respectively „B-Trust Root Advanced OCSP Authority" and „B-Trust Advanced OCSP Authority".
3. Each Relying Party, when accepting a QC, may apply for a real-time check of the certificate status.
4. The real- time status check of a QC is not mandatory for Relying Parties, but the Provider recommends using this service and its integration in the process of creation or acceptance of electronically signed/sealed and for website authentication in electronic transactions.

1.4.8 User

1. The Users are natural or legal persons who have submitted request and after successful completion of the procedure, they have been issued a qualified certificate. Before verification and issuance of qualified certificate, the User is only an Applicant for the Qualified Services of B-Trust
2. The relations between BORICA AD as a QTSP and the User are legalized by a written contract.

1.4.8.1 Signatory

1. The Signatory is a natural person – User of QC for QES/AES or a QC for CQES, who creates the electronic signature.
2. The Signatory carries out electronic statements on his own behalf, or on behalf of other person, represented by him, and signs them electronically in accordance with his representative authority.
3. In the QC for QES/AES or QC for CQES the person represented by the Holder can also be specified.
4. Only the Signatory of the QC for QES/AES or QC for CQES is entitled to access the private key for signing electronic statements.

1.4.8.2 Creator

1. The Creator is a legal person – User, who creates an electronic seal, the data of which is certified in the QC used for verification of the electronic seal. The creator may only be a legal person.
2. "Legal persons" within the meaning of the Treaty on the Functioning of the European Union (TFEU) means all entities constituted or regulated under the law of a Member State, regardless of their legal form.
3. Electronic Seal is not a signature of the legal person and serves only to certify the source and integrity of a sealed electronic document or statement.
4. When a legal person uses an electronic seal, it is recommended that an internal control mechanism be established for the legal person allowing only an individual authorized by that legal person (Creator) to create the seal (for example, press a button for “(automatic) creation of electronic stamps”).
5. In the QC for QESeal the natural person, representing the Creator can also be specified.
6. Only this physical person is entitled to access the private key for generating the seal.
7. When a transaction requires a qualified electronic seal by a legal person, the qualified electronic signature of the authorized representative of the legal person is equivalently accepted.

1.4.9 Relying Parties

1. Relying Parties are the recipients of signed/sealed electronic statements and documents by Users, who have QCs issued by the Provider or end clients, who address websites with certificates issued by the Provider.
2. The Relying Parties should have the knowledge and competences to use QCs and trust circumstances certified therein only in terms of the applicable Policy, especially regarding the security level when verifying the Users of these certificates.
3. The Relying Parties have permanent access to the registers of the Provider to check the validity of QCs, to verify the Users or other circumstances and data contained in the certificates or

recorded in these registers.

1.5 Certificates and their Use

1.5.1 Definition

1. "Qualified Public Key Certificate" is an electronic document signed by the Provider, containing certain requisites certifying the relation between the User and his public key in the QC corresponding to the private key of the User and it is used for verification of the signature/seal in electronic documents and objects or for website authentication.
2. QCs can be used for activities that require electronic documents signing, User or website authentication and for data encryption in electronic transactions that require a significant or the highest level of security.
3. Only certificates with Certificate Policies listed in this document, issued by the Provider, have the character of QCs.

1.5.2 Certificates of the Provider

Root certificate

1. The Root Certificate of the Provider is a certificate that is self-issued and electronically self-signed with the private key of the Provider QC for his root public key. The root private key is used by the Provider to sign electronically the certificates for public keys of its operational CAs, and Certificates of other (sub-) providers of trust services in the infrastructure of B-Trust.
2. In accordance with the EDETSA and the hierarchy of CA in the infrastructure of the B-Trust, the Provider provides the valid certificate of the root CA to the CRC. The main requisites of the root certificate of the Provider's B-Trust Root Qualified CA are as follows:

B-Trust Root Qualified CA

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	01
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-25T18:28:43Z
Validity to	-	2037-04-25T18:28:43Z
Subject	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path Length Constraint =	CA None
Certificate Policies	-	[1] Certificate Policy: Policy Identifier=All issuance policies [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name:

		Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	c0 4d 7a 42 7f 5a 82 b1 2d a6 f0 94 88 11 66 8e 1a 67 0a f6
Thumbprint (Sha256)	-	d3 38 95 e1 d5 11 23 f9 48 c8 c9 99 f7 26 40 fa 05 05 fb d1 5a b0 93 e8 98 db 27 dd 29 14 e8

B-Trust Root Advanced CA

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	01
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-24T18:55:40Z
Validity to	-	2037-04-24T18:55:40Z
Subject	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path Length Constraint =	CA None
Certificate Policies	-	[1] Certificate Policy: Policy Identifier=All issuance polices [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootACA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access

		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	ba 11 d6 ad 94 b2 4f c9 16 11 3a f6 82 cd 76 2a b3 bf d7 75
Thumbprint (Sha256)	-	fb 2c 73 6f 3c f1 ad 7c 89 ec 36 e8 60 c9 0c d6 be 87 f7 0d 66 09 8e 0a cc d5 4a 49 ea fa 2c a9

3. Electronic seals of the Provider that are accompanied by the root certificate are qualified.
4. The Provider may install and maintain other root certificates in the infrastructure of B-Trust.

Operational certificates of the Provider

1. The Certificate of Provider's operational CA is the qualified certificate for the public key of the operational CA electronically sealed with the root private key of the Provider. The Operational CA shall seal electronically the QCs issued by the Provider to Users using the private key corresponding to the certified public key.
2. Main requisites of the operational certificate of the Provider's CA "B-Trust Operational Qualified CA" are:

B-Trust Operational Qualified CA

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	69 0e 4f b7 9a ed 13 94
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2018-06-01T16:44:50Z
Validity to	-	2033-05-31T16:44:50Z
Subject	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path length Constraint =	CA 0
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.2 [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3

CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	ad 4c 92 43 9a 5b 83 28 13 1e b8 45 65 d1 46 2b f0 3d 3d 55
Thumbprint (Sha256)	-	49 9a 9c a8 b4 7e e8 44 37 f9 0b 96 fb 40 41 3e a2 93 f9 b3 94 2a 16 08 37 a0 c6 7b 0e c5 ba 0c

B-Trust Operational Advanced CA

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	55 6c c1 9f 35 f1 95 ca
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	O =	BORICA AD
	C =	BG
Validity from	-	2018-06-01T16:29:34Z
Validity to	-	2033-05-31T16:29:34Z
Subject	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path length Constraint =	CA 0
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.1 [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.2 [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.3

		[5]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.4 [6]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.5 [7]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6 8]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.7 [9]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.8
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustRootACA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	2d 11 f1 fb 79 b9 46 0a d5 e7 04 bf 36 18 8d a6 b6 e8 d8 c4
Thumbprint (Sha256)	-	e7 42 69 82 c0 26 4b 78 6b 94 25 ce 45 f3 63 58 7f 34 83 4f a3 4a 6a 7f fd d5 05 67 41 76 ad 0d

3. Electronic seals of the Provider that are accompanied by these operational certificates are qualified.
4. The Provider may install and maintain other operational certificates in the infrastructure of B-Trust.

Certificates of OCSP servers of the Provider

B-Trust Root Qualified OCSP Authority

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	03
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:27:48Z
Validity to	-	2022-04-26T14:27:48Z
Subject	CN =	B-Trust Root Qualified OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	34 31 84 22 65 34 41 46 e0 0d 03 2a 9f a1 0a 29 4a 93 7b 5c
Authority Key Identifier	KeyID =	f2 84 ee 2e 35 fe f0 fa d8 50 50 b0 9c 48 89 ea 5a 2f d9 ab
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootQCA.crl
Authority Information Access		[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		64 ed 90 7c af 37 a0 f2 62 39 3a ce 7e 90 e1 a7 bd 45 af a1
Thumbprint (Sha256)		91 18 ce 2d 4b c0 dc d2 c0 b4 32 fc cb f7 04 4e 94 c0 53 e2 8e 92 93 21 88 5c d3 43 6b e2 69 d5

B-Trust Qualified OCSP Authority

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	23 C3 46 00
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T15:26:25Z
Validity to	-	2022-04-26T14:35:30Z
Subject	CN =	B-Trust Qualified OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	be e5 83 42 fa 25 a5 58 4a 39 a5 0f 42 ea ef f4 42 05 95 2e
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access		[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		53 a1 58 0e db 15 6c c0 1f f6 f4 a1 99 43 8d 5d 59 42 63 90
Thumbprint (Sha256)		c7 5f 3b 30 0c 54 62 ba 78 80 e9 ea 4b e3 96 35 e3 50 df 1a 92 e8 f4 53 5b 07 4a 6d 4a 02 d8 81

B-Trust Root Advanced OCSP Authority

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	03
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:31:30Z
Validity to	-	2022-04-26T14:31:30Z
Subject	CN =	B-Trust Root Advanced OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	0a fe c2 5d 35 50 0a e1 00 2a c9 a7 09 2a 0a 4c f0 c5 cf 41
Authority Key Identifier	KeyID =	88 db 42 ed 89 05 32 0c 72 27 0c 46 1b e1 c6 09 5e ec c9 21
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootACA.crl
Authority Information Access		[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootACAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		34 0a 07 e7 9a 27 88 3f 55 a6 0a 84 85 02 a7 62 98 96 c2 6a
Thumbprint (Sha256)		01 86 c1 46 66 50 68 b5 17 81 62 c5 c8 55 9b ab 67 06 6c c0 17 ca 12 5f 00 1e f4 38 f6 90 0b f3

B-Trust Advanced OCSP Authority

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	29 B9 27 00
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Advanced CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2017-04-26T14:36:08Z
Validity to	-	2022-04-26T14:36:08Z
Subject	CN =	B-Trust Advanced OCSP Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	30 9c f5 49 43 6c af 46 3d 6f eb 5e ad 2e 55 06 de f6 30 de
Authority Key Identifier	KeyID =	07 dc aa 30 76 98 b7 85 4b 6d 03 18 c8 e3 cd a7 7b 36 82 ef
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustRootACA.crl
Authority Information Access		[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustRootACAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		0c 88 77 18 0e 60 d2 a9 37 f5 45 28 35 b2 cf 2f 30 d1 99 01
Thumbprint (Sha256)		0d 0b 59 a0 6b 13 8d ca b2 bc 11 d7 b9 e4 09 1e 95 52 01 26 6e c8 33 a4 7e 0e b0 c7 9a f9 e2 4f

1. B-Trust Root Qualified OCSP Authority Certificate of the Provider is a QC for his public key sealed with the private key of B-Trust Root Qualified CA of the Provider. The private key of the key pair of the OCSP server "B-Trust Root Qualified OCSP Authority" is used by the Provider to seal the result/response of the real-time verification of the status of submitted QCs, issued by B-Trust Root Qualified CA.
2. B-Trust Qualified OCSP Authority Certificate of the Provider is a QC for his public key sealed with the private key of B-Trust Operational Qualified CA of the Provider. The private key of the key pair

of the OCSP server "B-Trust Qualified OCSP Authority" is used by the Provider to seal the result/response of the real-time verification of the status of submitted QCs, issued by B-Trust Operational Qualified CA.

3. B-Trust Root Advanced OCSP Authority Certificate of the Provider is a QC for his public key sealed with the private key of B-Trust Root Advanced CA of the Provider. The private key of the key pair of the OCSP server "B-Trust Root Advanced OCSP Authority" is used by the Provider to seal the result/response of the real-time verification of the status of submitted QCs, issued by B-Trust Root Advanced CA.
4. B-Trust Advanced OCSP Authority Certificate of the Provider is a QC for his public key sealed with the private key of B-Trust Operational Advanced CA of the Provider. The private key of the key pair of the OCSP server "B-Trust Advanced OCSP Authority“ is used by the Provider to seal the result/response of the real-time verification of the status of submitted QCs, issued by B-Trust Operational Advanced CA.
5. The electronic seals of the Provider accompanied by the operational certificates of the OCSP servers of the Provider are qualified.

1.5.3 Certificates of Other Operational Authorities

1. The Provider may issue operational QCs to other CAs in the infrastructure of the B-Trust, and to other providers when they:
   - perform activities outside those legally stipulated in the EDETSA, in order to function as providers;
   - mutually certify the public operational keys to enhance the credibility of trust services provided (cross-certification);
   - perform legally regulated activity of a QTSP under the EDETSA.
2. The issuance of these certificates is based on a specific agreement with the respective providers.
3. The B-Trust Qualified Time-Stamping Authority certificate is provided in a separate document entitled “Certificate Policy and Certification Practice Statement on the Provision of Qualified Services by BORICA AD in Issuing Qualified Time-Stamp Tokens of the B-Trust® Qualified Time-Stamping Authority”.

1.5.4 User Qualified Certificates

1.5.4.1 Qualified certificates for qualified electronic signature

1. The Provider issues QCs for QES and QCs for CQES depending on Users, scope and purpose of the electronic signature, as follows:
   - B-Trust Personal Qualified Certificate for QES;
   - B-Trust Personal Qualified Certificate for CQES;
   - B-Trust Professional Qualified Certificate for QES;
   - B-Trust Professional Qualified Certificate for CQES.
2. The Practice Statement and the Certificate Policy for these QCs determine the procedures, format and security requirements applicable to the issue and use of the B-Trust Personal Qualified Certificate for QES and the B-Trust Personal Qualified Certificate for CQES. The Certificate Policies and the profiles of B-Trust Personal Qualified Certificate for QES and B-Trust Personal Qualified Certificate for CQES are the same.
3. The Provider issues B-Trust Personal Qualified Certificate for QES and B-Trust Personal Qualified Certificate for CQES only to Users – natural persons.
4. B-Trust Personal Qualified Certificate for QES and the B-Trust Personal Qualified Certificate for CQES are issued personally to an individual – Signatory.
5. B-Trust Professional Qualified Certificate for QES and B-Trust Professional Qualified Certificate for CQES are issued to a natural person (Signatory) representing a legal person by virtue of law or authorization.
6. The request for registration and issuance of these QCs is submitted remotely (by electronic

means) or locally (on site) at a RA/LRA, and the User identification procedure requires personal presence or explicit authorization by the User-Signatory. The identity of the represented person, respectively of the authorized natural person (if any) is also checked. The identification procedure and the procedures for generating the key pair when issuing and delivering Professional Qualified Certificate for QES and B-Trust Professional Qualified Certificate for CQES to the User ensure the highest level of security of the certified data in the certificate and their relation with the public key.

7. B-Trust Personal Qualified Certificate for QES and B-Trust Professional Qualified Certificate QES with their corresponding private keys are generated, stored and submitted to the User-Signatory on a B-Trust QSCD.
8. B-Trust Personal Qualified Certificate for CQES and B-Trust Professional Qualified Certificate for CQES with their corresponding private keys are generated, stored and submitted to the User-Signatory on an HSM in the RQSCD on the Cloud QES platform of the Provider.
9. The term of validity of the QC for QES and QC for cloud QES is 1 (one) or 3 (three) years from the date of issue and is defined in the contract for the QCS.

1.5.4.2 Qualified certificates for advanced electronic signature

1. The Provider issues two types of QC for AES depending on the Users, scope and purpose of the electronic signature as follows:
   - B-Trust Personal Qualified Certificate for AES;
   - B-Trust Professional Qualified Certificate for AES.
2. The Practice Statement and the Certificate Policy for these QCs determine the procedures, format and security requirements applicable to the issue and use of the QC for AES.
3. The Provider issues QC for AES only to Users – natural persons.
4. B-Trust Personal Qualified Certificate AES is issued personally to an individual (Signatory).
5. B-Trust Professional Qualified Certificate AES is issued to an individual (Signatory) representing a legal person by virtue of law or authorization.
6. The request for registration and issuance of these QCs for AES is submitted remotely (by electronic means) or locally (on site) at a RA/LRA, and the User identification procedure requires personal presence or explicit authorization by the User-Signatory. The identity of the represented person, respectively of the authorized natural person (if any) is also checked. The identification procedure and the procedures for generating the key pair when issuing and delivering QCs for AES to the User ensure a significant level of security of the certified data in the certificate and their relationship with the public key.
7. B-Trust Personal Qualified Certificate for AES and B-Trust Professional Qualified Certificate for AES with their corresponding private keys are generated through a specialized and approved by the Provider software, and are stored and submitted to the User-Signatory on a software token B-Trust SCT (PKCS#12 crypto file).
8. The term of validity of the QC for AES is 1 (one) year from the date of issue.

1.5.4.3 Qualified certificate for electronic seal

1. The Provider issues two types of QC for ESeal depending on the scope and purpose of the electronic seal, as follows:
   - B-Trust Organization Qualified Certificate for Qualified Electronic Seal (QCQESeal);
   - B-Trust Organization Qualified Certificate for Advanced Electronic Seal (QCAESeal);
2. The Practice Statement and the Certificate Policy for these QCs determine the procedures, format and security requirements applicable to the issue and use of the QC for ESeal.
3. The Provider issues QC for ESeal only to a User – legal person (Creator).
4. The request for registration and issuance of these QCs for ESeal is submitted remotely (by electronic means) or locally (on site) at a RA/LRA, and the User identification procedure requires personal presence or explicit authorization by the User-Signatory. The identity of the legal person,

respectively of the authorized natural person (if any) is also checked. The identification procedure and the procedures for generating the key pair when issuing and delivering QCs for ESeal to the User ensure the highest level of security of the certified data in the certificate and their relationship with the public key.

5. The procedure for generating the key pair for C uses the B-Trust QSCD and guarantees the highest level of security. The private key is stored and submitted to the Creator mandatorily on a B-Trust QSCD.
6. The procedure for generating the key pair for QC for ESeal uses specialized software and ensures a significant level of security. The private key is stored and submitted to the Creator on a B-Trust SCT (PKCS#12 crypto file).
7. The QC for ESeal has no meaning of an electronic signature and is used only to authenticate the source and integrity of the electronic document or statement.
8. QC for ESeal can also be used in secure and encrypted electronic messaging and secure and encrypted communications, access to information and online transactions requiring the highest or a significant level of security.
9. The term of validity of the QC for QESeal is 1 (one) or 3 (three) years from the date of issue and is defined in the contract for the QCS.
10. The term of validity of the QC for AESeal is 1 (one) year from the date of issue and is defined in the contract for the QCS.
11. In accordance with EU Regulation 910/2014, the QC for ESeal should not be used and applied as an electronic signature of a legal person. Where a qualified electronic seal is required for a transaction by a legal person, the qualified electronic signature of the authorized representative of the legal person shall be treated as equivalent.

1.5.4.4 Qualified certificates for website authentication

1. The Provider issues qualified certificates for website authentication as follows:
   - B-Trust Domain Validation SSL Certificate (B-Trust DVC SSL);
   - B-Trust Organization Validation SSL Certificate (B-Trust OVC SSL).
2. The Provider's Certificate Policy for these QCs determine the procedure, format and security requirements applicable to the issue and use of the authentication certificates.
3. The Provider issues certificates for website authentication to a natural person or a legal person.
4. The request for registration and issuance of these certificates is submitted remotely (by electronic means) or locally (on site) at a RA/LRA, and the procedure for identification of the natural or legal person requires personal presence or explicit authorization by the User. The identity of the legal person, respectively of the authorized natural person (if any) is also checked and verification is performed of the submitted domain name, required address details and registration number (in public registers). The identification procedure when issuing and delivering a certificate for website authentication ensures the highest or a significant level of security of the certified data in the certificate and their relationship with the public key.
7. The procedure for generating the key pair for QCs for B-Trust DVC SSL and B-Trust OVC SSL uses specialized software approved by the Provider and ensures a significant level of security. The private key is stored and submitted to the Creator on a portable software token (PKCS#12 crypto file).
8. The term of validity of the QCs for B-Trust DVC SSL and B-Trust OVC SSL is 1 (one) or 825 days from the date of issue and is defined in the contract for the certificates.
9. B-Trust DVC SSL certificate serves to identify the domain holder hosting the website by ensuring a significant level of security for the client with the browser. This certificate may contain a wildcard (*) for the hostname (for example, * .b-trust.bg). It is issued in accordance with the DVCP policy in ETSI EN 319 411-1.
10. B-Trust OVC SSL certificate serves to identify the domain owner and the organization accreditation, ensuring a significant level of security for the client with the browser that site he accesses belongs to the organization identified in the certificate. This certificate may contain a

wildcard (*) for the hostname (for example, * .b-trust.com). It is issued in accordance with the OVCP policy in ETSI EN 319 411-1.

1.5.4.5 Qualified certificates for Payment Service Providers

1. The Provider issues qualified certificates to Payment Service Providers under PSD2, as follows:
   - QSealC PSD2 – Qualified Certificate for Electronic Seal (issued to a payment institution) under PSD2;
   - QWebC PSD2 – Qualified Certificate for Website authentication (issued to a payment institution) under PSD2.

   These certificates have the status of qualified certificates within the meaning of Regulation 910/2014.
2. The Provider's Policy regarding these certificates defines the procedure, format and the security requirements applicable to the issuance and use of certificates by Payment Service Providers.
3. The Provider issues these qualified certificates only to Users – legal persons that are Payment Service Providers under PSD2.
4. The issuance of these certificates requires the personal presence of the physical person authorized by the Payment Service Provider at the B-Trust RA/LRA of BORICA for verification of the identity of the legal entity and the identity of its authorized person.
5. The identification procedure includes submission of proof and verification of the identity and the authorization of the Payment Service Provider, and of the identity of the authorized person.
6. A Payment Service Provider may itself generate the key pair for the respective certificate using approved by BORICA or other licensed software with equivalent security level and compatible with the B-Trust infrastructure.
7. When the key pair is generated at BORICA, the certificates issued to the Payment Service Provider, certifying the public keys corresponding to the private keys, are recorded on portable cryptographic software tokens (PKCS#12) together with the service certificates of the QTSP and are provided to the Payment Service Provider.
8. The period of validity of the qualified certificates issued to Payment Service Providers under PSD2 corresponds to the period of validity of the relevant standard qualified certificates for seal and website authentication.

1.5.5 Certificate Applicability

1. The QCs issued by the Provider to Users are used are used as intended in accordance with the relevant Certificate Policies for these certificates. The provider has a common (the same) Policy for QC for QES and QC for Cloud QES.
2. Each QC contains as a requisite, a filed for the purpose of the certificate. The requisite is identified as "Key Usage" in accordance with RFC 5280 and can be used with one or with several of the following purposes:
   - DigitalSignature - to enable digital signing/sealing of an electronic statement or content and its verification;
   - to authenticate the User as the Signatory or to authenticate the Source (Creator) and the integrity of the sealed data and the statement;
   - nonRepudiation - to enable subsequent proof to the User of the fact of signing/sealing an electronic statement or content and the impossibility of repudiating the electronic signature/seal;
   - keyEncipherment - to encrypt and/or decrypt keys used in data encryption;
   - dataEncipherment - to encrypt and/or decrypt data.
3. Through the „Extended Key Usage" requisite, in accordance to RFC 5280, which may also be contained in the QC issued by the Provider, the applicability of the certificate in terms of its purpose is specified.

4. The qualified certificates issued to Payment Service Providers contain attributes with specific data, required by PSD2 („QCStatement“ and „organizationIdentifier“ attributes are used).
5. QC for QES and QC for Cloud QES have the effect of a handwritten signature to everyone within the meaning of Regulation 910/2014, and identify the User as the QES Signatory. The QC for QES and QC for Cloud QES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring the highest level of security.
6. QC for AES has not the effect of a handwritten signature to everyone within the meaning of Regulation 910/2014, but identifies the User as the Signatory of the AES.
7. QC for AES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring a significant level of security.
8. According to Regulation 910/2014, a QC for ESeal should not be used and applied as an electronic signature of a legal person. The QC for ESeal serves only to authenticate the source (the Creator) and integrity of sealed electronic documents/statements.
9. In addition to the authentication of documents issued by a legal person, electronic seals may be used to authenticate the digital assets of a legal person such as software code or servers.
10. The QC for website authentication provides possibility for verification of website authenticity by associating it with the natural or legal person, to whom the QTSP has issued the certificate in accordance with the requirements of Regulation (EU) No 910/2014.
11. The qualified certificates issued to Payment Service Providers have field of application corresponding to the field of application of the respective general-purpose qualified certificates.
12. The appropriate use of the QCs issued by the Provider is as follows:

Qualified Certificate	Appropriate use
„B-Trust Personal Qualified Certificate QES" „B-Trust Personal Qualified Certificate CQES"	Personal identity of the User as Signatory of QES/cloud QES in applications requiring the highest level of security - Web-based e-commerce applications, electronic signing of documents, electronic signing of contracts, banking transactions, correspondence and making statements from and to state authorities and local government bodies within the meaning of the EDETSA.
„B-Trust Professional Qualified Certificate QES" „B-Trust Professional Qualified Certificate CQES"	Professional identity of the User as Signatory of QES/cloud QES in applications requiring the highest level of security - Web-based e-commerce applications, electronic signing of documents, electronic signing of contracts, banking transactions, correspondence and making statements from and to state authorities and local government bodies within the meaning of the EDETSA.
„B-Trust Personal Qualified Certificate AES“	Personal identity of the User as Signatory of AES in applications requiring significant level of security - Web-based e-commerce applications, electronic signing of documents, electronic signing of contracts, banking transactions, correspondence and making statements from and to state authorities and local government bodies within the meaning of the EDETSA.
„B-Trust Professional Qualified Certificate AES"	Professional identity of the User as Signatory of AES in applications requiring significant level of security - Web-based e-commerce applications, electronic signing of documents, electronic signing of contracts, banking transactions, correspondence and making statements from and to state authorities and local government bodies within the meaning of the EDETSA.
„B-Trust Organization Qualified Certificate QESeal”	Electronic authentication of the source and the integrity of electronic documents and statements in public and business electronic transactions (in the sense of an "e-office" of legal entities) requiring the highest level of security. Except when authenticating a document issued by a legal entity, electronic seals can be used to authenticate the digital assets of a legal entity such as software code or servers. Where a transaction requires a qualified electronic signature of a legal person, the qualified electronic signature of the authorized representative of the legal person shall be treated as equivalent.
„B-Trust Organization Qualified Certificate AESeal”	Electronic authentication of the source and the integrity of electronic documents and statements in public and business electronic transactions (in the sense of an "e-office" of legal entities) requiring a significant level of security. Except when authenticating a document issued by a legal entity, electronic seals can be used to authenticate the digital assets of a legal entity such as software code or servers. Where a transaction requires a qualified electronic signature of a legal person, the qualified electronic signature of the authorized representative of the legal person shall be treated as equivalent.
“B-Trust Domain Validation qualified certificate”	Identifies the domain owner hosting the website, ensuring a significant level of security for the client with the browser.
“B-Trust Organization Validation qualified certificate”	Identifies the domain owner and the organization's accreditation, ensuring a significant level of security for the client with the browser that the site he/she accessed belongs to the organization identified in the certificate. Encryption of communication between the client and the website (TSL/SSL protocol).

1.5.5.1 Limitation of the authentication action

1. If a QC is issued with a limitation of the authentication action, the Practice Statement of the Provider allows the certificate to contain a limitation on the purposes and / or value of transactions between Users and Relying parties using electronic signature.
2. The Provider must use the “Qualified Statements” requisite in the QC.
3. The limitation of the QCs on value of transactions that Users conclude by an electronic signature is agreed between them and Relying Parties, and is outside the scope of this document.
4. In accordance with EU Regulation 910/2014, the QC for AESeal should not be used and applied as an electronic signature of a legal entity. The QC for AESeal serves only to authenticate the source and integrity of automatically sealed electronic documents / statements ("electronic" office /organization).

1.5.5.2 Use of certificates outside the scope and restrictions

1. When a User or a Relying party uses or trust a QC for website authentication other than those specified in the "Key Usage", "Extended Key Usage," "Certificate Policy," or "Qualified Statements" the responsibility is entirely theirs and does not engage the Provider in any way.

1.6 Management of the Provider Policy

2. The Certification Practice Statement of the Provider (this document) is subject to administrative management and control by the Board of Directors of BORICA AD.
3. Changes, modifications and additions are acceptable, which do not affect the rights and obligations arising from this document and the standard contract between the Provider and the Users after approval and validation by the Board of Directors.
4. Each approved new or edited version of this document shall be immediately published on the Provider's website. Any comments, queries and explanations regarding this document may be made to:
    - e-mail address of the Certification Authority: info@b-trust.org;
    - e-mail address of the Provider: info@borica.bg;
    - Telephone: 0700 199 10.

2 PUBLICATION AND REGISTRATION RESPONSIBILITIES

2.1 Public Register

1. The Provider keeps an electronic Public Register to publish all QCs issued to Users and up-to-date Certificate Revocation List (CRL), and its own Service Certificates.
2. The Public Register of all certificates issued and the current CRLs are permanently available, except in the case of events beyond the control of the Provider or force majeure.
3. A Holder of a QC issued by the Provider is required to verify the accuracy and completeness of information contained in this certificate, despite it being formally accepted.
4. The Provider shall provide to any third party upon request the information concerning the status of a QC issued. The Provider shall provide the information contained in the issued certificate in the presence of a statutory obligation to provide it and at the due request of an Authorized Body or Person.
5. The current CRL contains information about all revoked and suspended QCs until its publication to the Register. A suspended certificate is maintained at the CRL for a period stipulated by the EDETSA and specified in this document. If the certificate is reactivated or the suspension period expires, it is removed and the updated CRL is published without it.

2.2 Public Repository

1. The Provider publishes and maintains electronic repository with current and previous versions of the following:
   - Public Disclosure Statements of the Provider (PDS);
   - Practice statement for providing QCs and QCS;
   - Certificate Policies on the provision of QCs and related QCS;
   - QCS Contract;
   - Tariff of the QCS provided;
   - Rules for issuing QC;
   - Terms and Conditions for use of QCs, including the requirements for storing the private key;
   - Documents required for initial issuance of QC, for renewal and suspension/revocation of QC;
   - Other documents required by the EDETSA and the regulatory framework.

2.3 Publication of Certificate Information

1. The Provider shall publish an issued valid certificate at the Register immediately following its issuance by an operational CA.
2. The Provider shall publish the CRL signed by an operational CA upon revocation/suspension of each valid certificate. The up-to-date CRL shall include the revoked/suspended certificate.
3. The effective period of validity of the published CRL is 30 days, unless it is updated within this period.

2.4 Frequency of Publication

1. The Public Registered of issued certificates is updated automatically and immediately following the issuance of each new valid certificate.
2. The CRL is updated automatically in no more than 3 (three) hours or immediately following revocation or suspension/reactivation of a valid certificate. In each CRL the QTSP states the time for next CRL issue.
3. A new edition or version of the Certificate Policies, the CPS, and of other additional documents under the EDETSA shall be published immediately.

2.5 Access to the Register and Repository

1. Provider keeps a Public Register of certificates issued, which is publicly available online.
2. Provider cannot restrict access to the Public Register. To protect the privacy of Users, third party access to download the published certificates is limited, unless the User has explicitly requested such access to be free.

3. There is no limit in access to the Certificate Policies, the CPS and the conditions contained therein. Any interested person is entitled to access to published documents.
4. There is no restriction on search access for any certificate published, or for the purpose of its status verification. Any interested person may search a certificate issued (valid or expired) by using certain attributes.
5. Any interested person is entitled to free access to the CRL for electronic reading or download.
6. Any interested person is entitled to free access to the service certificates of the Provider.
7. The Provider shall provide free access to all root and operational certificates of their active Certification Authorities, and free access to all certificates of their non-active Certification Authorities for a period of not less than two (2) years after the expiration of validity of these certificates.

3 IDENTIFICATION AND AUTHENTICATION

1. The Provider, through its RA /LRA:
   - accepts requests for issuance of QC;
   - carries out checks to identify the User, and specific data about him/her by eligible means;
   - approves registered requests upon successful verification, or rejects them;
   - notifies the CA to issue the requested certificate.
2. The RA/LRA collects and receives the necessary information for identification and authentication of the User.
3. Authentication/identification of the User after registration and before the QC issuance requires him/her to be present in person, or the presence of an authorized representative of the Applicant at the RA/LRA.
4. The Provider shall ensure that the natural and legal persons are properly identified, authenticated and that requests for issuing QC are fully, accurately and duly verified and approved, including: full name and legal status of the relevant natural/legal person; evidence for the connection between the certified data and the natural/legal person.

3.1 Naming

3.1.1 Use of names

1. QCs are in a format corresponding to the X.509 standard. A RA/LRA working on behalf of the Provider shall confirm that names specified in the applications for certificates comply with the X.509 standard.
2. The "Subject" field in the certificate electronically identifies the User related to the public key in the QC.
3. Name and other individualizing characteristics of the User in the relevant fields for each type of certificate are in accordance with the DN (Distinguished Name), formed according to X.500 and X.520 standards.
4. The service certificates of the Provider contain a DN attribute in the "Subject" and "Issuer" fields, forming its unique name.
5. Detailed specification of the QCs issued by the Provider is contained in the relevant documents of Certificate Policies of the Provider.

3.1.2 Use of pseudonyms

1. The Provider may issue a QC using a pseudonym to name the User only after the RA /LRA has collected the necessary information about his/her identity and has successfully identified him/her.
2. The use of pseudonym in a QC for electronic seal to name the Creator of the seal is not allowed.

3.1.3 Meaning of names upon registration

1. Certificates of the Provider’s CA contain unique names with a commonly understood semantics, allowing identification of the Provider that is the subject of such certificate.
2. The QCs include names matching the authenticated identification names of the Users, who are the subjects of these certificates.
3. For convenient electronic communication with the User, the Provider requests and certifies in the QCs the User’s email address. In the event that the latter has no such address, the Provider may provide to him/her an email address in the B-Trust domain.

3.1.4 Rules for name interpretation

1. The Provider shall include in the QC information for electronic identification of the User that has been successfully verified and validated by the RA/LRA, based on submitted identity documents.
2. In all certificates where the User is entered, the field for the common name (CN) shall contain the name of the natural or legal person, with which he/she is normally, identified in his/her activity.
3. In a professional certificate, the distinguished name (DN) attribute shall contain information about the identity of the person represented by the User.

4. In a certificate of a legal person, the distinguished name (DN) attribute shall contain information also about the identity of the authorized representative of the legal person.

3.1.5 Uniqueness of names

1. The electronic identification of the User of a QC issued by the Provider is based on DN.
2. The "Subject" field in the certificate is based on the information about the User, to be provided online or on paper by the Applicant or by an authorized representative upon registration of the initial application for a certificate and is to be checked by the RA/LRA based of submitted documents.
3. Provider guarantees a unique DN of the User in the B-Trust domain by adding a requisite to ensure this uniqueness.
4. A User with a unique DN in the B-Trust domain can have more than one valid QC issued.
5. Each certificate issued has a unique serial number in the domain of the respective CA of the Provider. The combination of the "Issuer", "SerialNumber" and "Validity from" fields ensures the uniqueness of the issued certificate in the public domain.

3.1.6 Recognition, authentication and role of trademarks

1. A User is not allowed to request certificate issuing using names that infringe upon the property or non-property rights of others.
2. Holders of such rights shall certify these with an official document before the RA/LRA when applying for a certificate.
3. The Provider shall not be held liable when names used in certificates violate the rights of others on a trade name, trademark, domain names, copyrights, etc.
4. In the event of any dispute regarding the names used, the Provider reserves the right not to issue a certificate, or if a certificate has been issued, to revoke it.
5. The Provider does not include trademarks, logos or other graphic material in the certificates.

3.2 Initial identification and identity verification

1. For the purposes of initial identification of the User of a QC, the Provider requires a registered application for initial issuance of the certificate.
2. An applicant/user of a QC for cloud QES must have a mobile device with downloaded B-Trust Mobile app for Android or iOS.
3. The request for initial issuance of a certificate at the RA/LRA of the Provider is a procedure by which the Provider requires, collects and receives information necessary to identify the User of the certificate, and identification data of the mobile device/application.
4. The registration procedure includes:
   - filling in a registration form for QC issuance;
   - generating a key pair;
   - preparing an electronic request containing the public key, for which the certificate is issued;
   - submitting the required documents to the RA/LRA, in accordance with the Policy on the issuance of the QC;
   - option to request other services related to the issued certificate.
5. The identity verification of a User is performed after registration and before issuance of the requested QC through:
   - remote video identification with the RA-VI;
   - personal presence of the User or of his/her authorized representative at the RA/LRA.

In view of preventing unauthorized use of the services, and to enable the verification of the authenticity of the data provided by the User, it is in the interest of both the User and the Provider to achieve the maximum level of security by making a copy of the User's identity document and keeping it on paper or electronically. A consent for making and keeping a copy of the User's identity document may be included in the Trust Services Contract concluded between the parties. If consent is not obtained for making and keeping a copy of an identity document, the Provider may refuse to provide the qualified trust service, considering the impossibility of guaranteeing the unimpeded and full acceptance of the qualified certificate by the relying parties, for whom achieving maximum level of security is a priority,

including payment service providers who are obligated under the applicable anti-money laundering legislation to collect and keep a copy of the customers' identity document as part of the identification process.

6. The initial identification and identity verification include:
   - possession of the private key corresponding to the public key the User or the person explicitly authorized by the User and its submitting to the Provider for issuing of the certificate;
   - possession of the mobile device/mobile application by the applicant/user or by an explicitly authorized person
   - verification and confirmation of the identity of the User of the certificate to be issued.
7. Upon successful verification of the identity of the User, the authorized operator at the RA/LRA:
   - offers a contract for QCS signed on behalf of the Provider and store all documents submitted to the contract;
   - confirms the application and sends an electronic request for issuing a certificate to the operational CA of the Provider;
   - may record the certificate issued (for QES/QESeal) on a QSCD and deliver it to the User, or the authorized person;
   - may record the certificate issued (for AES/AESeal) on a B-Trust STC (PKCS#12 crypto file) using software approved by the Provider (CSP/Crypto Service Provider).
8. QC for Cloud QES issued is not provided to the User - Signatory. The Provider publishes it in the B-Trust Public Register of Certificates and stores it in the RQSCD of the cloud QES platform by associating it in the user account of the Signatory with his mobile device/mobile application and with the generated key pair in the HSM for this Cloud QES.

3.2.1 Method to prove possession of private key

1. The RA/LRA verifies the compliance of the submitted public key, which is certified in the certificate issued by the Provider with the private key of the User.
2. The electronic request with the public key that is generated by the Applicant for issuing QC should be signed with the private key that corresponds to the public key in the request. The electronic request must be in a format that allows the Provider - via the RA/LRA - to verify the possession of the private key.
3. The Applicant should sign online applications for the administration of certificates with the private key corresponding to the public key in the certificate subject of the application. The Provider - via the RA/LRA – shall verify the electronic signature.
4. RA/LRA shall take further steps to authenticate the holder of the private key and the fact of possessing the key, depending on the type of certificate requested and following the applicable Policy.
5. The authentication of the holder of the private key for QC for Cloud QES includes also a TOTP scheme based on the mobile application in a mobile device and the associated user account for which the pair of keys is generated.
6. The key pair for QES and QESeal corresponding to the QC issued by the Provider must be generated on a QSCD or using software that is approved by the Provider (Crypto Service Provider/CSP) for AES/AESeal.
7. The key pair corresponding to the QC for Cloud QES issued by the Provider must be generated in the HSM (CC EAL 4+) on the RQSCD of the Cloud QES Platform and stored at the Provider on the basis of approved internal cryptosystems for personal control in accordance with SAD/SAP/SAM (Signature Activation Data / Signature Activation Protocol/Signature Activation Module) of ETSI EN 419 241 (part 2/3) and Protective Profile (PP) according to EN 419 221-5.
8. The access as well as the remote access to the private key is under the sole control of the QES or Cloud QES Signatory.

3.2.2 Authentication of legal person identity

1. Authentication of legal person identity has two purposes:
   - to prove that the legal person exists at the time of the review of the request;

- to prove that the representing person applying for the certificate has been authorized by the legal person.

2. Authentication and verification of legal person or sole proprietor identity is performed by the RA/LRA of the Provider under the respective Policy for issuing the certificate and other internal documents of the Provider.
3. Authentication and verification of legal person or sole proprietor identity whose data is entered in the QC, requires that an authorized representative of the person appear and present the required documents proving his/ her legal status.
4. The identity of a Bulgarian legal person shall be established by the RA/LRA of the Provider by verification in the relevant registers with the UIC provided, respectively BULSTAT under the procedure of the Electronic Government Act (EGA). An officer of the RA/LRA can check the registration through all available public services under the Bulgarian law.
5. For Bulgarian non-traders, as well as for foreign legal persons, for which an online (or automated) inspection cannot be performed, the following shall be presented:
   - Judgment or other document certifying the establishment of the legal entity;
   - Certificate of good standing;
   - Unique national identifier.
6. A list of required documents is published on the B-Trust website of the QTSP. After copying all required documents, with the consent of the person making the request, the copies shall remain in the archive of the Provider.
7. When instead of a legal person is his authorized representative, the authentication of the information contained in the documents submitted is via:
   - "True to Original" endorsement and handwritten signature on the documents before an employee of the RA/LRA;
   - Notary certified documents;
   - Signing of the attached electronic formats of the documents with a valid certificate for qualified electronic signature.

3.2.3 Authentication of natural person identity

1. Identifying and verifying the identity of the individual as a User of a QC or as a representative of another person as well as his/her authorization is carried out by the RA/LRA of the Provider following the procedural rules and steps specified in the respective Policy and other internal documents of the Provider.
2. The identification requires a natural person as a User or as an authorized representative of another natural or legal person to submit to the RA/LRA the following documents:

QC	Documents required
"B-Trust Personal Qualified Certificate QES" "B-Trust Personal Qualified Certificate CQES"	Documents proving the identity of the User - at personal appearance. Documents proving the identity of the authorized person and a power of attorney - upon the appearance of an authorized person. Approved by the Provider mobile app on a mobile device (for cloud QES).
"B-Trust Professional Qualified Certificate QES" "B-Trust Professional Qualified Certificate CQES"	Documents proving the identity of the User, the identity of the legal entity and the representative power of the User in respect to the legal entity. Approved by the Provider mobile app on a mobile device (for cloud QES).
"B-Trust Personal Advanced Certificate AES"	Documents proving the identity of the User - at personal appearance. Documents proving the identity of the authorized person and a power of attorney - upon the appearance of an authorized person
"B-Trust Professional Advanced Certificate AES"	Documents proving the identity of the User, the identity of the legal entity and the representative power of the User in respect to the legal entity

"B-Trust Organization Qualified Certificate QESeal"	Documents proving the identity of the User, the identity of the legal entity and the representative power of the User in respect to the legal entity
"B-Trust Organization Qualified Certificate AESeal"	Documents proving the identity of the User, the identity of the legal entity and the representative power of the User in respect to the legal entity.
"B-Trust Web authentication Qualified Certificate"	Documents proving the identity of the User - at personal appearance. Documents proving the identity of the authorized person and a power of attorney - upon the appearance of an authorized person. Documents proving the ownership of the website (domain) to the User.

3.2.4 Special Attributes

1. The Provider may include in the certificate to be issued specific attributes associated with the User, if the certificate is issued for a specific purpose under the respective Policy.
2. This information is subject to verification by the RA/LRA.

3.2.5 Non-verified Information

1. Non-verified information is any information beyond the scope of the mandatory information subject to verification that may be included in the certificate.
2. The Provider may include non-verified information about the User in the certificate to be issued, that is not subject to verification by the RA/LRA.
3. The Provider is not responsible for the non-verified information included in the certificate.

3.3 Identification and authentication for certificate renewal

1. The Provider may renew a valid QC for QES, QC for cloud QES or a QC for QESeal, which is not revoked within its validity period, in two ways:
   - by keeping the key pair generated for the current certificate (Renew);
   - by generating a new key pair (Re-key).
2. Renewal of QC for AES and QC for AESeal is not allowed. At the request of the User, the Performer issues a new QC for AES or QC for AESeal by performing initial identification and authentication of his/her identity.
3. A certificate is renewed for the same pair of asymmetric keys (Renew) of the current QC if the information contained in the certificate renewed, is identical to that in the current certificate. Only the period of validity in the renewed certificate is different from that in the current certificate.
4. Provider allows multiple renewal of a QC by keeping the current key pair (Renew), but recommends this practice to be limited in order to reduce the risk of compromising the private key.
5. The Provider will renew a current QC with a new key pair (Re-key), only if the User requests and declares that no change of information contained in the current certificate has occurred. The renewed certificate has a different public key, a new period of validity and a serial number, and the verified information is preserved.
6. After renewal, the current certificate is not terminated and shall remain valid for its validity period.
7. The identification and authentication of the identity of the User of the certificate renewed does not require him/her to be present in person before the RA/LRA of the Provider.
8. Upon changes in the information about the User of the QC, the current certificate is not renewed. The Provider shall issue a new QC, following the initial identification and authentication of the User, and shall immediately revoke the current certificate.
9. Renewal of certificate of a CA of the Provider BORICA AD is not allowed. In any event that requires replacement of the certificate, a new certificate of the CA must be issued.
10. The Provider shall observe the following time limits and requirements for identification when renewing a QC:

Time interval	Renewal	Requirement
Up to 30 days before the expiration	- Renew	1. There should be no change in the "DN" of the certificate

of the validity of a certificate that has not been revoked and which has no change in the information certified in it	- Re-key	2. The certificate has been issued on QSCD 3. The renewal request may be submitted remotely
Up to 30 days before the expiration of the validity of a certificate that has not been revoked and which has no change in the information certified in it	- Renew - Re-key	1. There should be no change in the "DN" of the certificate 2. The certificate has been issued on QSCD 3. The application for renewal must be submitted in person at the RA/LRA
More than 30 days after the expiry of the term of validity of the certificate	not renewed	

3.4 Identification and authentication for suspension

1. The Provider is obliged, through the RA/LRA, to suspend a valid certificate upon request, but for not more than 24 hours.
2. The Provider, through the RA/LRA shall not perform identification and authentication of the Applicant and shall immediately suspend the certificate.
3. The Provider, through the RA/LRA shall resume activity of a suspended certificate in accordance with art. 26, para. 6 of the EDETSA.

3.5 Identification and authentication for revocation

1. The Provider, through the RA/LRA, shall revoke a valid certificate upon request in accordance with art. 27 of the EDETSA.
2. The Provider, through the RA/LRA shall immediately suspend the certificate and perform subsequent identification and authentication of the Applicant.
3. The Provider, through the RA/LRA shall perform identification and authentication of the Applicant within the admissible time limit for suspension of the certificate, which is 24 hours.
4. The Provider, through the RA/LRA shall revoke the certificate only after successful identification and authentication of the Applicant and verified reason for revocation. Otherwise, the certificate shall be reactivated.

3.6 Identification and authentication after revocation

1. Renewal of a certificate via "Renew" or "Re-key" after its revocation is not allowed.
2. A User of a revoked certificate may request new certificate issuance.
3. The Provider, through the RA/LRA, shall perform initial identification and authentication of the User, if he/she requests a new certificate.

4 OPERATIONAL REQUIREMENTS AND PROCEDURES

1. The Provider, through the RA/LRA, within a contract for QCS, provides the following operational procedures for QCS applicable to QC:
   - registration of application for issuance;
   - processing application for issuance;
   - issuance;
   - delivery;
   - use of the key pair and QC;
   - renewal via “Renew”;
   - renewal via “Re-key”;
   - suspension/reactivation;
   - revocation;
   - status of a QC.
2. The Provider, through the RA/LRA, allows a User to terminate the Certification Services Contract between them.

4.1 Application for Certificate

1. The certificate issuance is preceded by a registration of request by the Applicant before the RA/LRA of the Provider.
2. A certificate application may be submitted in person by the User or by an authorized person.
3. The certificate application for QC for Cloud QES is preceded by the installation and initialization/activation of the Cloud QES Mobile App on the Applicant/User Mobile Device.
4. The applicant shall register the certificate application online or through an operator at the RA/LRA of the Provider.
5. An operator of the RA/LRA as an authorized representative of the Provider may act as an Applicant, by registering online an application for issuing of a certificate in the presence of the Applicant.

4.1.1 Application process

1. The Certificate Application shall include all information, about the User and the type of certificate to be issued. The application may include additional, noncertified information, part of which is certified, and other part is used to facilitate contact of the Provider with the person.
2. The request process application allows the operator of the RA/LRA or the User to generate the pair of cryptographic keys and to include the public key in the information for issuing the certificate.
3. The pair of cryptographic keys for issuing a QC for QES and QC for QESeal must be generated in a QSCD that conforms to the security level required for creation of the signature/seal.
4. The pair of cryptographic keys for issuing a QC for cloud QES must be generated by the Provider in HSM in the RQSCD on the Cloud QES platform.
5. The pair of cryptographic keys for issuing a QC for AES and QC for AESeal is generated using software approved by the Provider (Crypto Service Provider/CSP), meeting the requirements for adequate level of security/ safety for creating an advanced signature/seal.
6. The electronic format of the application for issuing of a certificate with information to be included in the certificate is structure that is to be signed with the private key of the generated key pair.
7. If necessary, the RA/LRA shall provide the User or an authorized person with protected information/access code to the private key.
8. If the applicant does not have a QSCD, when submitting an application for issuance of a certificate before the RA/LRA of the Provider, he/she needs to only enter information required to identify the User, and other information, without generating a cryptographic key pair for the requested certificate. The cryptographic key pair is generated at the RA/LRA of the Provider.
9. Communications between Users and protected Internet websites of the Provider are based on the HTTPS protocol.
10. The approved requests for QC issuance and management shall are signed by the Provider.

4.2 Issuance Procedure

4.2.1 Functions of Identification and Authentication

1. The RA/LRA performs identification and authentication of the Applicant for a certificate – User or an authorized person.
2. After initial identification and following established internal procedures of the Provider, based on request for issuance of certificate and other documents submitted, the RA/LRA verifies and confirms before the Provider:
   - the identity of the User or the authorized person;
   - representative power of the individual to the legal person and of the authorized person;
   - verification of the authorization;
   - the possession of the private key corresponding to the public key (when the key pair is generated at the User);
   - (for cloud QES) successful initiation/activation of the mobile application on the mobile device and registration (i.e. associating it with the user account by scanned QR code) by the Provider;
   - (for cloud QES) ownership/possession of the mobile device with the mobile application for cloud QES by the Applicant/User via TOTP mechanism/scheme;
   - additional information submitted for including in the certificate, and admissible non-verified information;
   - signed contract for certification services and consent with the terms of this document.
3. If the key pair is generated by the User, the RA/LRA should check the electronic application and requirements for the security level of the key pair.

4.2.2 Identification and authentication with an assistant

1. If the Applicant/User is literate but is mute, deaf or deaf-mute, the deaf person must read aloud the documents he / she signs, and declare whether he / she agrees with their contents, and the mute or deaf-mute must after reading the document to write in it that he/she has read it and agrees with its contents.
2. If the Applicant/User is illiterate, he/she should provide a literate person (interpreter) who will provide him/her with the contents of the documents to be signed. Signing documents by an illiterate person is done by placing a fingerprint of his right thumb. If fingerprinting is not possible with the right thumb, the reason for that shall be stated in the document, as well as the finger with which the fingerprint is done.
3. If the Applicant/User is blind, the Applicant shall provide two literate witnesses to inform him/her of the contents of the documents for signing and sign them.
4. The RA/LRA shall establish the identity of the interpreter and witnesses in accordance with section 3.2.3. of this document. The identity of the interpreter and the witnesses shall be recorded in the signed documents.

4.2.3 Confirmation or Rejection of Certificate Application

1. After successful checks, and payment by the Applicant/User, an authorized operator of the RA/LRA validates the request for a certificate before the Provider.
2. The RA/LRA shall reject the application for certificate if the validation fails or no payment has been made within 5 days of the request for the issuance of QC for cloud QES.
3. The RA/LRA shall immediately notify the Applicant and specify the reasons for rejection.
4. Rejected Applicant may file another application after having removed the reasons for rejection.
5. The RA/LRA properly stores and archives documents submitted and the validated electronic application for a certificate PO/MPC.
6. The RA/LRA controls and validates before the Provider the correctness and accuracy of the information included in the certificate only at the time of issue.
7. The User of a QC shall immediately inform the Provider of any changes to validated information occurred after issuance.

4.2.4 Time Limit for Processing Certificate

1. The RA/LRA of the Provider shall immediately perform all verification operations in the presence of the Applicant/User or authorized person, after the Applicant has submitted the necessary documents, and validates the information submitted with the application for the issuing of certificate.
2. A 5-day period is allowed for processing a QC request for Cloud QES through which the User can pay for the requested certificate online. After this period, the mobile application blocks the use of the cloud QES. If this period has not expired or the request is validated (upon payment) by the RA/LRA, the mobile application requires the user to enter the PIN code for the cloud QES.
3. CA of the Provider shall issue the certificate immediately after validation by the RA/LRA of the electronic certificate request.

4.3 Certificate issuance

4.3.1 Operation of the Certification Authority

1. The CA of the Provider shall identify by electronic means the RA/LRA that has validated the electronic application for issuing QC.
2. The CA generates the QC in accordance with the selected profile, signs it with the Provider's electronic signature and immediately publishes it in its Public Register.

4.3.2 Notification to User by the Provider

1. The Provider, via the Office for Notification of Users of QCS, shall immediately notify the User of a certificate issued and published.
2. The Office for Notification shall send to the User an e-mail or push-notification to the mobile application with information about the QC issued, the unique serial number of the certificate and its validity period, except in cases where no email address has been specified.
3. The Provider shall deliver the certificate issued to the User or, respectively, to the authorized person, via the RA /LRA.
4. An authorized operator of the RA/LRA shall record the certificate on the B-Trust QSCD or a B-Trust SCT (PKCS#12 crypto file) depending where the cryptographic key pair for this certificate has been generated, when possible.
5. The Provider via the RA/LRA delivers the issued certificate to the User, to the authorized person respectively.
6. In the case when a User has generated the key pair and the private key is on his/her computer, he/she has to deliver/load the issued QC on that computer from the specified URL in the email.
7. Generating a secure portable software token (PKCS # 12 file) is the responsibility of the User or Authorized Person after delivering the QC issued and the certificates to the Provider.

4.4 Certificate acceptance and Publication

1. The Provider, via the operational CA, shall immediately publish the certificate issued in the Public Register of certificates issued.
2. The User may object before the Provider, if the certificate issued contains errors or omissions, within 3 (three) days of its publication in the Public Register. These shall be immediately corrected by the Provider through issuing of a new certificate without charge, unless they have been made due to incorrect data provided.
3. In the absence of objection by the User in the above period, it shall be deemed that the certificate is accepted.

4.5 Key pair and certificate usage

4.5.1 User key pair and certificate usage

1. Only the User controls the private key corresponding to the certified public key. Responsibility for using the private key lies with the User.
2. The User shall use the certificate and corresponding key pair, as follows:

- in accordance with the Policy indicated in the certificate "Certificate Policy", and according to the attributes "keyUsage" and "extendedKeyUsage;
- for qualified electronic signature or electronic seal within the validity period of the certificate;
- for verification of qualified electronic signature or electronic seal;
- until the certificate is revoked;
- when the certificate is suspended, shall not use the private key, particularly for creating a qualified electronic signature or electronic seal;
- in accordance with the Contract for certification services with the Provider.

4.5.2 Relying party key pair and certificate usage

1. The public key in the QC corresponding to the private key held by the User is publicly available to everyone.
2. Each Relying Party, including an operator at the RA/LRA should use the public key and the QC of the User, as follows:
   - in accordance with the Policy indicated in the certificate "Certificate Policy" and according to the attributes "keyUsage" and "extendedKeyUsage";
   - only after verification of the status of the certificate and verification of the Provider's advanced electronic seal;
   - until the certificate is revoked;
   - when the certificate is suspended, the public key must not be used.

4.6 Certificate Renewal

1. Renewal of a QC shall retain information of the current certificate; the period of validity in the renewed certificate shall be changed.
2. QC for AES, QC for AESeal, and QC for Cloud QES are not renewed. The User may request the issuance of a new QC for signature, seal or Cloud QES.
3. The renewal of the QC is preceded by the registration of a request for renewal before the RA/LRA.
4. Renewal of a QC that has not been revoked during its period of validity can be accomplished in two ways:
   - the generated key pair of the current certificate is retained (Renew);
   - A new pair of keys is generated (Re-key).
5. The request for renewal of a certificate is registered online when the User has a valid QC for QES, which has to be renewed.
6. When the certificate is expired and the renewal request is in accordance with the specified time limits and the renewal identification requirements, the User or a person authorized by him/her shall personally visit the RA/LRA of the Provider.
7. A user or a person authorized by him/her may renew his/her QC repeatedly subject to the renewal conditions specified below.
8. The Provider does not allow the use of a key pair for a period longer than 3 (three) years.
9. The provider does not recommend multiple renewal of the QC via "Renew" in order to reduce the risk of compromising the private key.
10. The Provider recommends the User to renew his/her certificate via "Re-key".

4.6.1 Conditions for certificate renewal

1. RA /LRA will renew a QC via the "Renew" function, subject to the following conditions:
   - the certificate is not revoked during its period of validity;
   - the User or his/her authorized representative should declare that there no change has occurred in the information contained in the current certificate;
   - an application for renewal has been submitted within 30 days before or after the period of validity of the certificate;
   - strictly performs identification and authorization of the Applicant and the specified time limits for renewal.
2. RA/LRA will renew a QC via "Re-key", subject to the following conditions:

- the certificate is not revoked during its period of validity;
- the User or his/her authorized representative should declare that there no change has occurred in the information contained in the current certificate;
- an application for renewal has been submitted within 30 days before or after the period of validity of the certificate;
- strictly performs identification and authorization of the Applicant and the specified time limits for renewal;

3. In all cases where a change in the information about the User of the current certificate has occurred, the certificate shall not be renewed, and the Provider shall issue a new certificate.

4.6.2 Who may request renewal

1. A User or his/her authorized representative request a renewal of the certificate subject to the time limitations, requirements and conditions for renewal.

4.6.3 Certificate renewal procedure

1. Renewal of a QC is preceded by the registration of an application for renewal before the RA/LRA of the Provider.
2. The request for certificate renewal by electronic application shall be certified by a QES. If the certificate being renewed has expired, the User or his/her representative must personally visit the RA/LRA of the Provider. The RA/LRA strictly follows the requirements for identification and authentication of the Applicant and the conditions for renewal.
3. Upon successful identification and verification of the conditions for renewal, the RA/LRA confirms the application for renewal before the operational CA of the Provider.
4. Upon successful electronic authentication by the RA/LRA via the authorized operator, the operational CA shall accomplish the confirmed request for renewal of the certificate.
5. Upon unsuccessful identification and verification of the conditions for renewal, the RA/LRA shall reject the application for renewal of the certificate and shall immediately notify the Applicant for the reasons.
6. A rejected Applicant for renewal may apply for a new QC.

4.6.4 Notification of certificate renewal to User

1. The Provider, via the Office for Notification of Users of trust services, shall immediately notify the User of the renewed and published certificate.
2. Office for Notification sends to the User an email notification containing information about the issued QC, unique serial number and validity period of the renewed certificate and the address (URL) which can be used to receive the renewed certificate.
3. When the Applicant for renewal of a certificate visits the RA/LRA, the User receives the renewed certificate from the authorized operator who, if necessary, records it on the QSCD where the pair of cryptographic keys for the certificate has been generated.
4. The renewed QC for cloud QES is not delivered to the User; it is only recorded in the user account corresponding to the associated mobile application/mobile device.

4.6.5 Publication of the renewal certificate

1. The Provider, via the operational CA, immediately publishes a renewed certificate in the Public Register.

4.7 Certificate re-key

1. The Provider allows replacement of cryptographic key pair in the QC via "Re-key", only in compliance with the requirements and conditions for renewal of a certificate, or by issuing a new certificate.

4.8 Certificate modification

1. The Provider allows changes in the content of information in an issued and published QC only subject to the requirements and conditions for issuing a new certificate.

2. The Provider does not allow a change in the profile of QC, specified in the Certificate policy for this certificate.
3. Provider does not support "Certificate Modification"

4.9 Certificate revocation and suspension

1. Only valid certificates shall be subject to revocation, i.e. certificates whose validity has not expired.
2. Upon revocation of the certificate of an operational CA for issuing and maintaining QC, all certificates issued by this Authority that are still valid shall be revoked.
3. Only the operational CA that has issued the certificate may revoke it.
4. If revocation is the result of operator's error or the result of compromise of an operational private key of the Provider, which has led to the revocation of the certificate of the operational CA, the Provider shall issue an equivalent certificate at its own expense.
5. Services related to the management of certificate revocation and suspension are available 24/7, 7 days a week. For urgent suspension of the certificate (in case of lost or stolen QSCD device), it is necessary to call: 0700 199 10.
6. In case of system failure, services or other factors that are beyond the control of the CA, the QTSP shall take all the efforts to ensure that the service will not be unavailable for a period longer than the maximum period of time, which in this case is 3 (three) hours.
7. Time in systems related to suspension and revocation of certificates is synchronized to the UTC at least once every 24 hours.

4.9.1 Conditions for revocation

1. The Provider shall revoke a QC issued by them upon:
   - death or disablement of a User with termination of a legal person of the User;
   - termination of the representative power of the User with respect to the legal person he/she represents;
   - incorrect data provided upon issuing the certificate;
   - certified information that has subsequently become untrue;
   - change in already certified information of the User;
   - compromising the private key;
   - loss of a B-Trust QSCD or a mobile device with an initialized/activated mobile application or a deletion of the mobile application on the mobile device;
   - delay in payment of outstanding remuneration;
   - request for revocation, after verifying the User's identity and representative power.
2. The Provider shall immediately revoke the QC in each of the above circumstances.
3. The Provider shall revoke all certificates they have issued, in case of terminating their activity without transferring it to another provider.
4. The Provider may suspend and revoke a certificate of a CA from their infrastructure upon reasonable suspicions that the private key of this authority has been compromised.

4.9.2 Certificate revocation procedure

1. Revocation of the certificate is preceded by registration of an application for revocation before the RA/LRA of the Provider.
2. The application for revocation of a certificate may be registered electronically only when the User has (another) certificate valid and accessible for use. Otherwise, the application shall be submitted to an authorized operator of the LRA.
3. Revocation of certificate by electronic application shall be certified by QES corresponding to a valid certificate of the User.
4. The authorized operator at a RA/LRA shall immediately suspend the certificate, without identifying the Applicant, for not more than 24 hours.
5. In all cases, the User or his/her representative must personally visit the RA/LRA of the Provider for verification of the identity.
6. The RA/LRA strictly follows the requirements for identification and authentication of the User and

the reasons for revocation.

7. Upon successful electronic authentication by the RA/LRA via an authorized operator, the operational CA shall revoke the certificate.
8. Upon unsuccessful identification and verification of the conditions for revocation, the RA/LRA shall reject the application for revocation of the certificate and shall immediately notify the User of the reasons.
9. A User with rejected request for revocation of certificate may submit a new request for revocation of the certificate after he/she has removed the reasons for refusal.
10. After revocation of the certificate, the Provider, via its operational CA, shall immediately publish the revoked certificate in the CRL, and shall issue a new CRL.
11. After revocation of the certificate, the Provider, via the Office for Notification, shall immediately inform via email or push-notification on the mobile device/mobile application the User of the terminated certificate.
12. A revoked certificate of a User is not subject to reactivation or renewal.
13. Authorized persons from the personnel of the Provider have access to the application for revocation and the reports from the execution of the termination of a certificate.

4.9.3 Grace period before revocation

1. Prior to terminating a valid QC, the Provider through its RA/LRA shall suspend the certificate for not more than 24 hours.
2. During this grace period, the Provider through its RA/LRA shall carry out all checks to establish the identity of the User and the reasons for revocation.
3. Upon unsuccessful verification, or after the end of the grace period, the Provider shall resume the certificate.
4. The Provider shall reactivate the certificate upon request of the User or his/her representative before the expiry of the grace period.

4.9.4 Time within which CA must process the revocation request

1. The Provider shall execute a request for revocation of a certificate within a timeframe not greater than the grace period specified, and only upon successful completion of verification of the conditions and reasons for revocation.

4.9.5 Revocation checking requirement for relying parties

1. Each Relying Party shall accept a QC issued by the Provider only after successful verification of the status of the certificate using the current CRL, or by checking the status of the certificate in real time via the OCSP server of the Provider.
2. The Provider shall not be held liable for any damages and consequences upon non-performance of these requirements.

4.9.6 CRL issuance frequency

1. The Provider, through its operational CA, shall immediately publish a new updated CRL, every time a valid QC issued by that authority is terminated.
2. Provider, through its operational CA, shall periodically publish a new CRL with validity period of 1 month.
3. Validity period of 1 month applies for each new and updated CRL of the operational CA published.

4.9.7 CRL issuance after revocation

1. The Provider shall immediately publish an updated CRL after automatically recording a suspended or revoked certificate.
2. Publication of the current CRL is automatic.

4.9.8 On-line revocation/status checking availability

1. The Provider supports real-time online verification of the status of QCs, by using the OCSP protocol.

4.9.9 Requirements for Using the OCSP

1. Real time checks of the status of a QC (using the OCSP protocol) require using the necessary techniques and technologies, as well as online access via the Internet to the OCSP server of the Provider.
2. Real time checks of the status of a QC (using the OCSP protocol) can be made also via the Provider's website.

4.9.10 Consistency of status information in CRL and OCSP

1. Since the Provider maintains two methods for verifying certificate status (OCSP and CRL), there are procedures to maintain the status information consistency.
2. Certificate status information is first updated on the OCSP, and then the associated CRL is also synchronized. The difference in the certificate status information has an alignment period, depending on the Certification Authority issuing the respective CRL, as follows:
   - For B-Trust Root Qualified CA and B-Trust Root Advanced CA - up to 2 hours;
   - For B-Trust Operational Qualified CA and B-Trust Operational Advanced CA - up to 2 minutes.

4.9.11 Circumstances for suspension of a certificate

1. The Provider, through its operational CA, shall suspend a valid QC under certain conditions and for a period of up to 24 hours.
2. The Provider shall take immediate actions on a request for suspension of a certificate.
3. For the time during which the certificate is suspended, it shall be deemed invalid and any digital signatures verified using this certificate should be void (invalid).

4.9.12 Who may request suspension

1. The Provider shall suspend a validly issued certificate, upon:
   - application of the User or his/her representative, without being obliged to verify his/her identity, or representative authority;
   - request of a person who, under the circumstances, could be aware of any breaches of the private key as a representative, partner, employee, etc.;
   - request by the CRC;
   - decision of the Chairman of the CRC, where there is imminent danger to the interests of third parties or sufficient evidence of breach of the EDETSA.

4.9.13 Certificate suspension procedure

1. Suspension of the certificate is preceded by registration of a request for suspension before the RA/LRA.
2. The request for suspension of a certificate may be registered electronically or before an authorized operator at LRA of the Provider.
3. Suspension of a certificate by electronic request shall be certified by QES (AES) or cloud QES.
4. The authorized operator at a RA/LRA shall immediately suspend the certificate, without identifying the User. Suspension of the certificate shall be performed by its temporary inclusion in the Certificate Revocation List, as per Art. 26, Para. 5 of the EDETSA.
5. Upon successful electronic authentication by the RA/LRA via an authorized operator, the operational CA shall execute the request for suspension of the certificate.
6. RA/LRA cannot refuse to suspend a certificate.
7. Upon suspension of the certificate, the Provider, via its operational CA, shall immediately publish the suspended certificate in the CRL, and shall issue a new CRL.
8. Upon suspension of the certificate, the Provider, via its Office for Notification, shall immediately inform the User of the suspended certificate via email or push-notification on the mobile device.

4.9.14 Limits on suspension period

1. The Provider shall suspend a QC for up to 24 hours of receiving the request for suspension.
2. Provider shall suspend the certificate for 24 hours before its revocation.

4.9.15 Certificate reactivation

1. The Provider shall reactivate a suspended QC:
   - up to 24 hours after its suspension;
   - after the end of the period of suspension (24 hours), if no request for revocation has been submitted;
   - after elimination of the reasons for suspension, before expiry of the period of suspension;
   - at the request of the User, after the Provider, respectively the CRC, ensures that the former was made aware of the reason for suspension and that the request for renewal is made as a consequence of this.
2. After reactivation of a certificate, it shall be deemed valid.

4.9.16 Certificate reactivation procedure

1. RA/LRA shall resume a suspended QC after receiving request for reactivation by the User and upon successful verification.
2. RA/LRA shall reactivate a suspended certificate after receiving a written order of the CRC, or the Chairman of the CRC, to reactivate the certificate.
3. RA/LRA shall immediately resume a suspended certificate at the end of the suspension period (24 hours).
4. In all cases, the procedure for resuming a certificate shall result in removing the certificate from the current CRL, and a new CRL shall be published.

4.10 Certificate status

1. All valid QCs issued by the Provider shall be published in the Public Register.
2. Each certificate published in the Register shall have:
   - a "valid" status - the period of validity specified in the certificate has not expired at the time of status verification;
   - an "invalid" status - the period of validity specified in the certificate has expired at the time of status verification.
3. All revoked certificates shall be included in the CRL, which is published periodically or immediately after a change of status of a certificate.
4. CRL entry corresponding to the suspended/terminated certificate contains an attribute that specifies the reason for the revocation of the certificate ("CRL Reason").
5. A suspended certificate shall be included in the CRL until it is resumed and the attribute "CRL Reason" in the corresponding list entry shall have the value of "certificate Hold".
6. The status of a certificate being checked by a CRL mechanism (through the Certificate Revocation List) is determined by the value of the "CRL Reason" attribute.
7. The status of a certificate checked by an OCSP mechanism (via the OCSP protocol) is determined by the value "response Status" in the response received by the OCSP server, as follows:
   - „good"- the certificate is not suspended/terminated, but does not assert that the time of response is within the period of validity of this certificate;
   - „revoked"- the certificate has been terminated or suspended (on hold);
   - „unknown"- the OCSP server has no information about this certificate (most likely the certificate was issued by another provider).

4.11 Termination of certification services contract

1. A contract for trust services between the Provider and the User shall be terminated after the expiry of the term of validity of the last certificate issued, revocation of all valid certificates under this contract, or as otherwise specified in such contract.

4.12 Key recovery

1. The Provider does not support Key Escrow and Key Recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

1. The Provider shall ensure the physical protection and access control to the premises where critical components of B-Trust infrastructure are installed.
2. Critical components of the Provider's B-Trust Infrastructure are:
   - „B-Trust Root Qualified CA";
   - „B-Trust Root Advanced CA";
   - „B-Trust Operational Qualified CA";
   - „B-Trust Operational Advanced CA"
   - Registration Authority;
   - Public Register;
   - „B-Trust Qualified Time Stamp Authority";
   - RQSCD on the Cloud QES platform
   - OCSP server „B-Trust Root Qualified OCSP Authority";
   - „B-Trust Qualified OCSP Authority";
   - „B-Trust Root Advanced OCSP Authority";
   - „B-Trust Advanced OCSP Authority".
3. The Provider's B-Trust infrastructure is physically and logically separate and not used in other activities operated by "BORICA" AD.

5.1.1 Site location and construction

1. The Provider has a dedicated room with specific design and equipment, provided with electromagnetic protection and the highest level of physical access control, which houses the CA of the Provider and all central components of the infrastructure - "B-Trust Root Qualified CA", "B-Trust Operational Qualified CA".

5.1.2 Physical access

1. Physical access to the specialized premises is controlled by access control systems, video surveillance, alarm systems, etc.
2. Physical access control systems are periodically inspected, and all necessary logs are kept.
3. Authorized staff of the Provider strictly observe and follow internal procedures for access to various areas of the premises with restricted physical access.
4. All members of the Provider's staff are personified in the access control systems for the premises and strict verification is required.

5.1.3 Power and air conditioning

1. Power supply to all critical components of the B-Trust infrastructure of the Provider is protected against disruption of power supply. Power supply of the premises has a high level of protection and is shielded against external intervention.
2. The ventilation system is specifically designed for premises of this class, preventing any compromise of the physical and electromagnetic protection of the premises, and ensuring normal operation of installed computer components.

5.1.4 Water exposures

1. Special measures have been taken to prevent flooding of the premises.

5.1.5 Fire prevention and protection

1. The Provider complies with all regulations and standardization requirements for the fire protection of premises of this class.

5.1.6 Media storage

1. The premises shall contain safe boxes with varying degrees of physical protection against opening,

where confidential information is stored.

5.1.7 Service Life of Technical Components

1. The service life of physical elements in the composition of all critical components of the B-Trust infrastructure is observed and after its end, they are removed from use.

5.1.8 Duplication of Technical Components

1. All critical components in B-Trust infrastructure of the Provider are duplicated.
2. Infrastructure components that provide real-time online services related to certificates issued have been implemented under a scheme for continuity of services.

5.2 Procedural controls

1. Operational procedures described in this document relating to B-Trust infrastructure, are implemented in full compliance with the internal rules, guidelines and Security Policy of the Provider.

5.2.1 Trusted roles

1. The Provider maintains qualified staff with roles to perform duties at any time related to the issue, maintenance and management of QC, in accordance with applicable regulations.
2. The Provider operates using their own staff.
3. For certain activities, the Provider may hire external stuff.

5.2.2 Number of persons required per task

1. For each activity specified in the regulations, the Provider maintains at least one person to perform assigned tasks.

5.2.3 Identification for each role

1. The Provider has developed job descriptions for each of the positions of personnel performing the activities.
2. The roles of Provider's personnel include at least the following:
   - generating and maintaining the infrastructure of the public key of the Trust Service Provider;
   - administration of systems and ensuring their security;
   - creating and managing QC, including creation of a key pair - public and private key for a QC;
   - data storage and archiving.

5.2.4 Roles requiring separation of duties

1. The activities of the Provider’s personnel are performed by different individuals.

5.3 Staff qualification and training

1. The Provider’s staff has the necessary qualifications, expertise and experience in the following areas: security technologies, cryptography, PKI-technology, technical standards for assessing security, information systems, communications, etc.
2. Personnel of the Provider undergo initial and further qualification training in the operation of the components of B-Trust infrastructure.
3. Requirements for additional training, refresher and other events are described in internal documents of the Provider.
4. The Provider prepares and updates internal instructions for operation, and shall provide these to staff for the purpose of self-study and training at work.

5.4 Logging procedures

5.4.1 Records of Important Events

1. The Provider keeps logs created by the computer operating systems in B-Trust infrastructure, as follows:
   - For installation of a new and/or additional software;

- shutting down and launching of systems and their applications (date, time);
- for successful and unsuccessful attempts to start and access to hardware and software PKI-components of systems;
- in cases of software and hardware failures of systems and other failures in the platforms.

2. The Provider keeps logs generated by the components (hardware and software) of the B-Trust infrastructure, on:
   - generation and management of key pairs and certificates for CA and components in the infrastructure of B-Trust;
   - management of HSM of "B-Trust Root Qualified CA" and "B-Trust Operational Qualified CA"";
   - management of HSM of „B-Trust Root Advanced CA" and „B-Trust Operational Advanced CA";
   - contents of certificates issued;
   - generation and management of key pairs and certificates of Users;
   - successful or unsuccessful processing of applications for issuing and/or maintaining of certificates;
   - generation of CRL;
   - publication of valid certificates issued in the Public Register;
   - configuration of certificate profiles;
   - real time certificate status checks;
   - issuing qualified electronic time stamp token of provided content.
3. Access to information contained in logs is restricted only to authorized staff, responsible for systems support.
4. The Provider keeps records that are created in the RA/LRA on:
   - submitted documents for registration to establish identity and applications for issuing, renewal, suspension/resumption and revocation of certificates;
   - internal procedures for identification and registration.
5. Records are stored that are created by communication components of the infrastructure.
6. Records are stored in a documentary archive - old and current versions of the Certification Practice Statement, application forms, operating instructions, etc.

5.4.2 Frequency of Logging

1. Information for electronic Logs is generated automatically.
2. Records and logs are periodically analyzed by authorized employees of the Provider.

5.4.3 Retention period for records

1. Records are kept for a period of 7 (seven) years.

5.4.4 Protection of records

1. Information from records in the logs is periodically recorded on physical media that are stored in a special safe located in premises with a high degree of physical security and access control.
2. Only qualified persons authorized by the Provider have access and use these records and logs.

5.4.5 Backup procedures

1. Backup copies of entries in systems logs are maintained and securely stored.

5.4.6 Notification following an analysis of log entries

1. Log entries are periodically analyzed for vulnerability and reliability of systems and the competent authorities of the Provider are notified to take measures for security management, if necessary.

5.5 Archiving

1. Information about significant events is periodically archived in electronic form.
2. All information relating to the application for issuance, renewal, suspension/revocation and renewal of certificates and the full document flow between the Provider and the Users is archived on paper or on electronic media.

3. The Provider keeps records in a format allowing for reproduction and recovery.

5.5.1 Types of archives

1. The Provider maintains paper and electronic records.

5.5.2 Retention period for archive

1. All archived data shall be kept for a period of 10 (ten) years.

5.5.3 Protection of archive

1. Security of records is ensured, as follows:
   - backup files in electronic form are signed electronically;
   - specific events and data that are recorded in the archive are defined and documented by the Provider;
   - stored on reliable electronic media that cannot be easily destroyed or deleted during the storage of the archive;
   - the CA sign electronically all certificates and lists of revoked and suspended certificates;
   - only authorized system maintenance personnel work with the protected archived information;
   - electronic communications between local components of infrastructure are protected in conformity with the PKIX standard;
   - remote electronic communications are protected and based on the PKIX standard;
2. The Provider ensures the appropriateness of use of postal and courier services and fax communications with Users.

5.5.4 Recovery of Archival Information

1. If necessary, the provider shall recover information from the archive.

5.5.5 Requirements for time-stamping of records

1. Separate archives shall be stamped with the exact time of signing.

5.5.6 Archive collection

1. Internal (logged) and external (documentary) information is properly stored in a special safe in a room with high level of physical protection.

5.5.7 Procedures to obtain and verify archive information

1. Public archive information of the Provider is published and is available in the Public Registry, the CRL and the register of documents. Other information that is collected upon application for issuance or management of certificate is only available to Applicants, or to persons duly authorized by the latter.
2. This CPS, Policies and the Certification Services Contract are publicly available in the Provider's register of documents and may be obtained and downloaded from the website of the Provider.
3. The Provider has ensured that information on public archives is in readable form.

5.6 Key changeover

1. The Provider may change the key corresponding to an issued QC only by issuing a new certificate, or by renewing a current certificate with the "Re-Key" function.
2. Change of a key corresponding to QC foe AES, QC for cloud QES and QC for AESeal is performed only by issuing a new certificate

5.7 Compromise and disaster recovery

1. The Provider takes due care to maintain continuity and integrity of the trust services related to all certificates issued, maintained and managed by the Provider.
2. The Provider takes greatest care, within his capabilities and resources, to minimize the risk of compromising the keys of the CA as a result of natural disasters or accidents.
3. In case of failures in computer resources, software or information, the Provider shall notify the Users, restore the infrastructure components and resume access to the Public Register and CRL.

4. In case of compromise of a cryptographic algorithm used, the Provider shall inform the Users and the Relying Parties by a notification on the Provider's official website.

5.8 Compromise of a Private Key

5.8.1 Of Certification Authority private key

1. The Provider shall take the following actions upon compromise of the private key an operational CA:
   - immediately revoke the certificate of this operational authority;
   - issue and publish a new CRL of the root authority;
   - inform Users and Relying Parties;
   - suspend the operational CA;
   - inform the CRC;
   - perform instant analysis and report on the cause of compromise;
   - initiate a procedure to generate a new pair of operating keys;
   - issue a new certificate to the authority by the root authority.
2. The Provider shall take the following actions upon compromise of the private key of the root CA:
   - immediately terminate the certificate of the root authority;
   - follow all the steps in the preceding paragraph;
   - inform the CRC and accredit/register new CA.

5.8.2 Of User private key

1. Upon compromise of the private key of a User, he/she shall immediately notify the Provider to initiate the revocation of the certificate.

5.9 Provider Termination

1. Activities of the Provider shall be terminated under Ordinance on Liability and Termination of Trust Service Providers.
2. Upon termination of activities, the Provider shall:
   - notify the CRC of his/her intention not later than 4 months before the date of termination;
   - notwithstanding the requirement under the preceding item, the Provider shall notify the CRC in the event of a claim to declare the company bankrupt, invalid, or upon other application for termination or commencement of liquidation proceedings;
   - make every effort and take care to continue the operation of issued certificates;
   - notify the CRC and Users in writing whether the Provider's activity shall be succeeded by another registered provider, and of their name, not later than the time of termination of activities. A notice shall also be published on the website of the Provide;
   - inform Users about the conditions of maintenance of certificates transferred to the successor Provider;
   - The QTSP changes the status of their certificates and duly submits all documentation relating to their operation to the successor Provider, together with all records and all certificates issued (valid, revoked and suspended);
   - perform the necessary actions to transfer the obligations for maintenance of the information to the successor Provider, including the event logs for changing the status of the certificates issued for the relevant period. This information shall be provided to the successor Provider under the same conditions as those described in this policy;
   - the successor Provider shall take the management of already issued certificates for end clients;
   - if the Provider fails to transfer their activities to another registered provider, they shall terminate all issued certificates and submit the whole documentation to the CRC;
   - the CRC maintains a register with CRL.

6 TECHNICAL SECURITY CONTROL AND MANAGEMENT

6.1 Key Pair Generation and Installation

1. Cryptographic key pairs for official certificates of the Provider are generated and installed according to instructions and procedures contained in this document.
2. The Provider shall use their private keys only for the purpose of their activities, as follows:
   - to sign official certificates issued to operating authorities of their infrastructure;
   - to sign the CRL issued and published;
   - to sign all QC issued and published to Users.
3. The cryptographic (RSA) key pairs of QCs issued in the infrastructure of the Provider are generated, as follows:
   - by the User - using hardware and software approved and under the control of the Provider (Crypto Service Provider/CSP);
   - by the RA/LRA of the Provider - using hardware and software that is approved and under the control of operator of the Provider.
4. The cryptographic (RSA) key pairs of QCs for cloud QES are generated in the HSM in the RQSCD on the cloud QES platform of the Provider with the required level of security (CC EAL 4+ or higher).
5. The Provider may, based on a contractual relationship, provide Users with technical resources approved by the Provider that meet the requirements for level of security.
6. Only electronic signatures created with the private key of a key pair generated in the QSCD and RQSCD on the cloud QES platform have the character of QC for QES, QESeal and cloud QES.
7. The User is obliged to use only licensed software for operation with QC or licensed software for operation with QCs and with associated (relevant) token (QSCD or SCT/PKCS#12 file).

6.2 Generation Procedure

6.2.1 Provider CA key pair generation

1. The Provider generates pairs of cryptographic (RSA) keys to the root and operational CA by using HSM with level of security FIPS 140-2 Level 3 or higher, respectively CC EAL 4+ or higher.
2. Authorized personnel of the Provider shall perform the steps of generating, installing and storing key pairs of the root and operational CA, respectively, "B-Trust Root Qualified CA", "B-Trust Operational Qualified CA", „B-Trust Root Advanced CA", and „B-Trust Operational Advanced CA", according to a documented internal procedure agreed and approved by the management of the Provider.
3. The procedure is performed in the presence of a member of the management of “BORICA"AD and a Notary.
4. A key pair of a CA of the Provider is generated only after the initialization of the respective slot in the hardware cryptosystem serving that Authority.
5. Upon initialization of each slot, prepared codes for access control to the private key of the Authority are inserted in this slot.
6. Access codes to the private key are shared independently between at least two authorized members of the Provider’s personnel, to ensure that activation of access to the corresponding private key by a single person is impossible.
7. Private keys of CA are stored separately on individual QSCDs, each of which is under the control of more than one authorized member of the Provider’s personnel.
8. Separate storage of private keys and individual access control to parts of private keys of CA stored in different QSCDs does not allow compromise and/or unregulated reproduction without authorization of the Provider.

6.2.2 User cryptographic keys generation

1. The key pair of a User is generated by the use of specialized software that is entirely under his/her control.
2. When the key pair of a User is generated by the Provider, it is done by the use of specialized

licensed software verified for successful operation through the interfaces of the B-Trust infrastructure.

3. The key pair of a User is generated in a QSCD approved by the Provider with verified security level (Crypto Service Provider/CSP). When the key pair is generated at the Provider, B-Trust QSCD is always used. The private key of the generated key pair cannot be taken out from the QSCD.
4. The key pair of a User of cloud QES is always generated in in the HSM of the RQSCD on the cloud QES platform of the Provider and is stored at the Provider using an approved crypto-scheme, and is accessed remotely guaranteeing sole control of the private key in accordance with SAD/SAP/SAM security profile according to ETSI EN 419 241-2/3.
5. The private key is controlled by an access code and the length of the RSA key is at least 2048 bits. The Titular shall use the private key to create the signature by entering the access code.
6. When a key pair is generated with the User, the Provider recommends the latter to use an approved solution in the B-Trust infrastructure, or equivalent.
7. For the purposes of applying QC for QES/QESeal, the Provider recommends the User to use a B-Trust QSCD or other QSCD compatible with the B-Trust infrastructure.
8. For the purposes of applying QC for cloud QES, the Provider delivers a mobile smartphone application that the User has to install, initialize/register and use for profile activation.
9. For the purposes of applying QC for AES/AESeal, the Provider recommends the User to use a B-Trust SCT (PKCS#12 file) or other SCD compatible with the B-Trust infrastructure.

6.2.3 Private Key delivery

1. When the key pair for QES/QESeal is generated with the Provider, the User or explicitly authorized person shall receive the private key and the certificate issued on a QSCD from the RA/LRA of the Provider.
2. When the key pair for AES/AESeal is generated with the Provider, the User or explicitly authorized person shall receive the private key and the certificate issued using B-Trust STC (PKCS#12 crypto file) from the RA/LRA of the Provider.
3. When issuing QC for QES/QESeal the private key and the issued certificate is provided on B-Trust QSCD, where the private key is generated. QSCD ensures the highest level of security and protection of the private key and is provided together with an initial access code.
4. When issuing QC for cloud QES the private key corresponding to a certified public key in the certificate is stored in the HSM of the RQSCD on the cloud QES platform at the Provider via an established crypto-scheme that guarantees sole control of the private key; the access to the key is in accordance with the SAD/SAP security profile according to ETSI EN 419 241-2/3.
5. The User is obliged to change the initial access code and enter his/her own code.
6. When User generates the key pair by himself/herself, he/she has the full responsibility for guaranteeing the possession of the private key.
7. When User generates the key pair by himself/herself, he/she declares to the Provider that the key pair fully meets the requirements for electronic signature sealing in accordance with the Regulation.

6.2.4 Public key delivery at the Provider

1. This is performed only by the User who generates his/her own key pair and who should deliver the public key to the Provider for the needs of the process of issuing the certificate.
2. The User delivers through the RA/LRA of the Provider the public key of the generated key pair.
3. The Titular may submit the request stored on electronic media in person at the RA/LRA, along with other documents in accordance with the Provider's Certificate Policies, through the website of the Provider or in any other appropriate manner.
4. The RA/LRA of the Provider verifies the possession of the private key by the User.

6.2.5 Provider public key delivery to relying parties

1. Provider's public keys shall be publicly accessible on the Provider's webpage, where their service certificates are published.

2. Each Relying Party builds trust towards the Provider, by accepting and loading service certificates of the Provider into systems under its control.

6.2.6 Key sizes

1. The length of the root RSA-key of the Provider is 4096 bits.
2. The length of the RSA-key pair of "B-Trust Operational Qualified CA" and “B-Trust Operational Advanced CA" is 4096 bits.
3. The length of the RSA-key pair of the operational authorities "B-Trust Root Qualified OCSP Authority", "B-Trust Qualified OCSP Authority" and “B-Trust Root Advanced OCSP Authority", „B-Trust Advanced OCSP Authority" is not less than 2048 bits.
4. The length of the key pair (RSA) for QES/QESeal of a User generated by infrastructure of the Provider is at least 2048 bits.
5. The length of the key pair (RSA) for QES/QESeal of a User generated outside the Provider's infrastructure is at least 2048 bits.
6. Regardless of where the key pair for issuing a QC is generated, the key must have a length of at least 1024 bits for RSA algorithms.

6.2.7 Public key parameters

1. The public key parameters are specified and verified in the certificate that the Provider issues for that public key corresponding to the private.

6.2.8 Key usage

1. The parameters for using the key pair, respectively the private key, are contained in the certificate issued by the Provider through the attributes "keyUsage" and "extended keyUsage".

6.3 Private Key Protection and Cryptographic Module Controls

6.3.1 Standards

1. The key components in the B-Trust infrastructure „B-Trust Root Qualified CA", „B-Trust Operational Qualified CA", „B-Trust Root Advanced CA", „B-Trust Operational Advanced CA", RQSCD on the Cloud QES platform and OCSP servers use HSM with verified security level FIPS 140-2 Level 3 (respectively CC EAL 4+ or higher), which meet the regulatory requirements.
2. B-Trust QSCD, respectively the HSM in the RQSCD on the platform, where the private key of the User is generated and stored, has a security level of CC EAL 4+ /FIPS 140-1 Level 2, respectively Level 3.
3. The software for generating key pair (Crypto Service Provider/CSP) has been approved by the Provider and verified for operation in the B-Trust infrastructure.
4. All QSCDs outside the infrastructure of B-Trust that a User could use to generate the key pair and store the private key for QES must be certified for an equivalent level of security to CC EAL 4 or higher.

6.3.2 Private Key control and storage

1. Private keys of the CA of the Provider are used in HSM only and are available via access codes divided into several parts, which are known to the authorized personnel of the Provider.
2. Along with the procedure of generating the key pair of a CA, the procedure for storing the private key is performed, in accordance with established internal procedure.
3. The private key of QES/QESeal of a User is used only in B-Trust QSCD or in QSCD with equivalent security level, and is accessible via a personal access code. Along with generating the key pair, the private key is stored in the QSCD.
4. The private key of cloud QES of a User is used only in the HSM of RQSCD on the Cloud QES platform and is available through a SAD/SAP/SAM scheme and personal access code in accordance with ETSI EN 419 241-2/3. In this case, simultaneously with the generation of a key pair, the private key is stored based on an approved crypto-scheme by the Provider providing protection and personal control of the key.
5. The private key of AES/AESeal of a User is used only with licensed software via B-Trust SCT

(PKCS # 12 crypto file) and is accessible through a personal access code.

6.3.3 Private Key storing and archival

1. Private keys of the CA are stored separately on separate QSCDs with protection profile CC EAL 4+ or higher, and access to each QSCD is controlled by an access code held by an authorized person of the Provider's staff.
2. The access code to each QSCD is personal to each authorized person of the Provider's staff.
3. Separate storage of private keys of CA on several QSCDs and personal control of access to these QSCDs does not allow for keys to be compromised or for unauthorized reproduction outside the Provider.
4. Reproduction of private keys of the Provider on a backup HSM upon failure of the operational HSM system is made only in the presence of at least two authorized persons, each of whom controls access to their own QSCD.
5. The private key of QES/QESeal of a User is stored only on QSCD and cannot be replicated on another QSCD. Upon defecting the QSCD, the User should replace it and request issuing a new certificate.
6. The private key of a cloud QES of a User is stored only in the HSM of the RQSCD on the cloud QES platform and cannot be replicated on another such platform. The B-Trust cloud QES platform is reserved for the critical components in it, including the HSM module.
7. The private key of AESeal of a User is stored is stored by software and can be reproduced on another system only under the control of the User. Upon defecting the private key, the user must request a new certificate.
8. The Provider does not in any way store or archive a private key of QC for QES/QESeal of a User, regardless of where and how the pair of keys is generated.
9. The Provider stores a private key of cloud QES only based on validated cryptograms for protection and guaranteed personal control of the key by the User.

6.3.4 Private Key transfer into or from a cryptographic module

1. Transfer of a private key of a Certification Authority of the Provider from HSM for the purposes of preservation and restoration is performed under the exclusive control and only with the Provider, in accordance with documented and approved internal procedures for generation, storage and recovery of keys of Certification Authorities.
2. Transfer of a private key of a User to and from the Provider for the purposes of storage and recovery in another QSCD/HSM or software is supported.
3. The private key of QES/QESeal of a User is stored only on a QSCD in which the pair of keys is generated and cannot be transferred/reproduced elsewhere.
4. The private key of AES/AESeal of a User is stored software and can be reproduced on another system only under the control of the User.

6.3.5 Method of activating private key

1. A private key of the Provider is activated via a shared system code for access, individual parts of which are known to more than one authorized person of the Provider's staff.
2. Only in the presence of such persons, after entering all parts of the access code, the access to the slot in the HSM is permitted and the private key is activated.
3. A private key of a User is activated by entering the user access code where the key is stored securely, or other means of identification is used.
4. A private key of cloud QES of a User in the RQSCD on the platform is activated by running a TOTP-Smartphone authentication scheme and entering the user access code (PIN) for cloud QES in accordance with the SAD/SAP/SAM of ETSI EN 419 241-2/3. The private key for a cloud QES is activated only if there is a signed Request for issuing of Cloud QES and a Certification Services Contract issued by the User. The signing of these documents can be done after a cloud QES certificate has been issued.

6.3.6 Method of deactivation of the private key

1. A private key of the Provider in the cryptosystem of the CA is deactivated (terminate the possibility to use/access the private key) by terminating the logical access to the appropriate key contained therein.
2. A private key of a User is deactivated (the possibility to use/access the private key is terminated) by terminating the logical access to the location where the key is stored.

6.3.7 Destroying private key

1. A private key of the Provider in the cryptosystem of the CA is destroyed by deletion of the key or the relevant slot. If necessary, recovery media stored in the archive shall be deleted as well.
2. A private key of QES/QESeal of a User is destroyed by its deletion from the QSCD or by the overall deletion of QSCD.
3. A private key of cloud QES of a User is destroyed by its deletion (its cryptogram) from the user account for cloud QES.
4. A private key of AES/AESeal of a User is destroyed by its deletion from the location where the key is stored securely.

6.4 Other Aspects of Key Pair Management

6.4.1 Public key archival

1. Public keys of CA are contained in the service certificates of the Provider and stored in an internal register. These are publicly available through publication of certificates of the Provider.
2. Public keys of CA are archived and stored for 10 years after the expiry of validity or termination of the respective certificates.
3. Public keys of Users are contained in certificates issued to them, which are published in the Public Register and stored in an internal register.
4. Public keys of Users are stored and archived by periodical archiving of the internal register.

6.4.2 Certificate Validity Period and Use of Key Pair

1. QC have the following validity periods:
   - of „B-Trust Root Qualified CA" and „B-Trust Root Advanced CA" – 20 (twenty) years;
   - of „B-Trust Operational Qualified CA" and „B-Trust Operational Advanced CA" - 15 (fifteen) years;
   - of the OCSP servers – 5 (five) years;
   - of a User – according to the contract between the Provider and the User, but not more than 3 (three) years.
2. When the key is used for signing/sealing after expired validity period of the certificate, the signature/seal is invalid, and the respective signed/sealed statement or object should be considered void.
3. Six months prior to expiration of validity of the CA, the Provider generates a new key pair and applies all the necessary actions for safeguarding the operation of the Relying Parties who rely on the old key pair. The new key pair of the CA is be generated and its public part is distributed according to the policy of this document.

6.5 Activation Data

6.5.1 Generating and Installing Activation Data

1. When generating a key pair by a User, he/she creates and manages the activation data.
2. When generating a key pair of a User by the Provider, the latter hands over, together with the private key, the control of the activation data to the User.
3. Upon initial issuance of a certificate on a B-Trust QSCD, before generating a key pair, the B-Trust QSCD is initialized and the following access/activation codes are created: User ("User") and Administrative ("SO"), and respectively for access to the personal private key in QSCD and for unblocking the QSCD.

4. Initial User and Administrative access code and code to unblock the B-Trust QSCD are provided to the User or his/her authorized representative in a sealed, non-transparent paper envelope.
5. The User must change the initial User access code through the software that comes with the B-Trust QSCD.
6. The Provider recommends that the User periodically change his/her user code for access to the QSCD.
7. The User must use the Administrative access code to unblock a blocked B-Trust QSCD.

6.5.2 Generating and Installing Activation Data for Cloud QES

1. The key pair for cloud QES is generated in the HSM of the RQSCD on the B-Trust cloud QES platform and the private key is securely stored by the Provider.
2. Upon initial issuance of a QC for cloud QES before generating a key pair the user has to load and initialize/activate the mobile cloud application on the smartphone.
3. The initialization/activation of the mobile application is performed autonomously in the smartphone, and registration of the mobile application is performed jointly with the cloud QES platform of the Provider and include the following:
   - Creating a password;
   - Registration (association) of the application/mobile device in the cloud QES platform (creating user account, exchange of shared key for TOTP-scheme for authentication, PIN protection key);
   - Secure storage of the two keys in the mobile device/application - one used for TOTP authentication (ownership of the mobile device by the User), the other - for protection of the PIN for access to the private key;
   - Generating a key-pair after entering the PIN through the mobile application by the User; the private key is protected by an established crypto scheme that guarantees personal control to the private key and is stored;
4. Data for activation of the cloud QES (shared key for TOTP-authentication, key for PIN protection) are under the control of the User.
5. TOTP-authentication mechanism and the crypto scheme for protection of private key of a cloud QES bring guaranteed personal control of the User to the protected private key of the cloud QES.

6.5.3 Protection of Activation Data

1. The User must store and keep from compromising the access codes to the place where the private key is stored securely.

6.5.4 Other aspects of Activation Data

1. After a number of unsuccessful attempts to enter the correct code to access the private key of a User, the B-Trust QSCD is blocked.
2. After a number of unsuccessful attempts to enter the correct code to access the private key of a Cloud QES of a User, the cryptogram with the private key in the user account is blocked.
3. The User has to use the Administrative access code to unblock a blocked B-Trust QSCD.
4. The User of Cloud QES has to use an additional (administrative) code to unblock the cryptogram with the private key.

6.6 Security of Computer Systems

6.6.1 Security Requirements

1. The computer platforms on which all critical components of the B-Trust infrastructure are operating are equipped and configured with means for local protection of access to software and information.
2. The Provider provides methods and procedures to administer and manage the security of the entire infrastructure of B-Trust, in accordance with standards for information security management that are generally accepted in international practice.
3. The reliability of systems, and technical and cryptographic security of the processes they perform, is ensured by tests and checks of technical equipment and technology according to a methodology

for security assessment.
4. Inspections and tests are carried out periodically, and after each change that affects the security infrastructure.

6.6.2 Security level

1. The security level of systems used in the infrastructure of B-Trust meets the legal requirements for implementing the activities of the Provider and is determined by the document Security Policy of the Provider.

6.7 Development and Operation (Life Cycle)

6.7.1 Development

1. The development of products and trust services related to certificates issued and maintained by the Provider is performed on separate systems, completely independent of those in regular operation.
2. Products, software and services offered by the Provider are initially tested on development systems, before being implemented into operation.
3. New products and trust services offered by the Provider are accompanied by operational procedures and instructions for use.

6.7.2 Operation

1. Trust services and products implemented in operation by the Provider are maintained by dedicated separate operating computer systems.
2. The Provider provides all trust services through its operational systems.
3. Products and services of the Provider are tested in real working conditions.

6.8 Additional Tests

1. The Provider provides an opportunity for performance testing of the issued Qualified Certificates on its official website.

6.9 Network Security

1. The Provider uses innovative technical means for the exchange and protection of information in the infrastructure of B-Trust, in order to ensure network security of systems against external threats and interventions.

6.10 Timestamp

1. The Provider has published in a separate document the Certificate Policy and Certification Practice Statement of the Qualified Electronic Time-Stamping Authority.

7 RISK ASSESSMENT

1. Considering established business and technical problems in the delivery, operation and maintenance of trust services, the TSP carries out a risk assessment to identify, analyze and assess the associated risks.
2. Appropriate measures are selected to avoid identified risks considering the results of the risk assessment. The measures adopted ensure a level of security commensurate with the degree of risks identified.
3. The Provider documents through the Practice and the relevant Trust Services Policies the security requirements and the operational procedures necessary to avoid identified risks.
4. Periodic review and risk assessment are performed to address identified risk factors.
5. The Management of the Provider approves the results of the risk assessment, the prescribed measures to overcome identified risk factors and accepts the residual risks identified.

8 PROFILES OF QUALIFIED CERTIFICATES, CRL AND OCSP

8.1 Qualified Certificate Profile

1. The full content (profile) of QCs is contained in the published documents of the respective Certificate Policies.

8.1.1 Version number

1. The Provider issues QC in a X.509, v3 format.
2. The version number is included in the issued QC.

8.1.2 Extensions in the certificate format

1. „Subject Key Identifier" attribute - formed by the public key certified in the certificate as a hash value of the public key.
2. „Authority Key Identifier" attribute - formed as a hash value of the public key of the operational CA of the Provider.
3. „Issuer Alternative Name" attribute - contains the URL-string as an alternative name of the Provider.
4. „Basic Constrains" attribute - specifies the type of certificate and has the value "End entity" in the User certificate.
5. „Certificate Policy" attribute - determines the identifier of the QC policy.
6. „Key Usage" attribute - attribute that determines the use and limitations on the use of the certificate.
7. „Enhanced Key Usage" attribute - supplements the meaning of "Key Usage" attribute and indicates additional and specific applications of the certificate.
8. „CRL Distribution Point" attribute - contains a link to the current CRL of the operational CA of the Provider.
9. „Authority Information Access" attribute - contains the URL-address of the OCSP server for validation of the certificate.
10. „Qualified Statements" attribute - the attribute contains an indication that the certificate is qualified and whether the private key is generated and stored on QSCD.

8.1.3 Identifiers of the Algorithms of Electronic Signature

1. The attribute "Signature algorithm" identifies the algorithms (cryptographic mechanism) that are used.

8.1.4 Forms of Naming

See section "Naming" of this document.

8.1.5 Restrictions on names

See section "Naming" of this document.

8.1.6 Policy Identifier

1. QCs are issued in accordance with the Policy of the Provider with OID is recorded in the attribute "Certificate Policy" of the certificate. This Provider Policy is in line with internationally agreed policies under ETSI / ITU-T in EN 319 411-1/2. See Table in item 1.3 of the document.

8.1.7 Indication of a Qualified Certificate

1. The Provider uses in the QC with a profile under the X.509 v.3 standard, "Qualified Statements" attribute with identifiers: „id-etsi-qcs-QcCompliance“ (OID=0.4.0.1862.1.1), „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4) and „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6) with value „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1).

8.2 Profile of the Certificate Revocation List

8.2.1 Version

1. The Provider, through its CA, issues, publishes and maintains Certificate Revocation Lists (CRL) in the H.509 v.2 format.
2. The version number is assigned in the issued CRL.

8.2.2 Format

1. The Provider issues, publishes and maintains a CRL, which format is in accordance with the international guidelines RFC 5280.
2. CAs of the Provider issue, publish and maintain separate and complete CRLs and record therein only revoked certificates issued by the respective CA.
3. The Provider does not issue or maintain a scheme of "partial" (delta) CRL, but reserves the right to introduce such a scheme, if necessary.
4. The main attributes of the CRL are:
   - Version;
   - Issuer Name - identifies the CA that issued and signed the CRL;
   - Effective Date/This update - the time of issue of the CRL;
   - Next Update - the period of validity of the CRL. After that period, the CA periodically issues a new list. During the period of validity, in the event of revocation/suspension of a certificate, the CA immediately issues a new CRL;
   - Signature algorithm - means the cryptographic mechanism/algorithm for electronic signature of CRL;
   - Signature hash algorithm - hash function in the mechanism of the electronic signature.
5. Additional CRL-attributes are:
   - Authority Key Identifier- the identifier of the CA that issues and signs the List. It contains the meaning of "subjectKeyIdentifier" from the certificate of the CA that signs the CRL.

8.2.3 Format of an Element in the CRL

1. The CRL of the CA contains elements for all certificates revoked by the CA. These elements are constant in the List.
2. The CRL of the CA contains an element for every certificate suspended by the CA. Such an element in the List is temporary until the resumption of the certificate.
3. Attributes of the elements in the CRL are as follows:
   - "Serial number" - the serial number of a revoked/suspended certificate;
   - "Revocation date"- the date of revocation/suspension of the certificate;
   - "CRL Reason Code" – code identifying the reason for revocation/suspension.
4. The meanings of the reason for revocation/suspension of the certificate are as follows:
   - "keyCompromise" - compromised private key of the User;
   - "CACompromise" - compromised private key of an operational CA of the Provider;
   - "affiliationChange" - changed status of a User to another person - changes in the representative authority, revocation of representative authority, termination of employment contract, etc.;
   - "superseded" - the certificate is replaced with another;
   - "certificateHold" - the certificate is temporarily suspended.

8.3 OCSP Profile

1. The OCSP server of the Provider shall operate and provide the service "online check of certificate status in real time", in accordance with the internationally recognized recommendation IETF RFC 6960.
2. Information of the request profile and response when operating with the OCSP server is available in the above-mentioned technical recommendation, publicly available on the web site of IETF.

9 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

9.1 Periodic and Circumstantial Inspection

1. The control of the legally regulated activity of the Provider, related to the electronic signature certificates and its compliance with the requirements of the EDETSA and the legislation is exercised by the Communications Regulation Commission, within its competence.
2. Internal control of Provider's activities shall be appointed by the executive management and/or Board of Directors of the legal entity of the Provider, and the order and extent of such controls shall follow the internal documents of the legal entity
3. The management of the Provider shall exercise continuous operational control for the proper performance of the operating instructions by the Provider's staff.
4. The management of BORICA AD shall appoint periodic inspections for compliance of the current activity with the approved Practice Statement and Policies regarding the activities of the Provider.
5. The Provider shall exercise constant control over the activity of the RA/LRA.

9.2 Qualifications of the Inspectors

1. Inspectors can only be persons who are entitled to perform such functions in accordance with the requirements and documents adopted in international practice.
2. Inspectors shall be accredited by an international accreditation organization to perform such inspections.
3. The internal inspections on the operation of the RA/LRA shall be performed by employees of the Provider duly authorized for this activity.
4. Inspectors may not authorize others to perform part or all inspections, except with the explicit consent of the Provider.
5. Inspectors shall be held liable for the facts and circumstances verified, no matter if they have reassigned some or all of the inspections to others with the consent of the Provider.

9.3 Relationship of the Inspecting Persons with the Provider

1. The inspecting persons shall be independent, not directly or indirectly related and have no conflict of interest with the Provider.
2. The relations between the Provider and external inspectors shall be arranged by a contract.

9.4 Scope of the Inspection

1. The inspection by the Authorities to assess compliance with Regulation 910/2014 covers the regulatory requirements to the Provider's activity under the EDETSA.
2. Internal inspection may cover every circumstance or activity referred to in this document, as well as:
   - comparison of practices and procedures specified in this document with their practical implementation upon implementation of the Provider's activity;
   - inspection on the activities of subcontractors (external RAs/LRAs);
   - other circumstances, facts and activities related to the B-Trust infrastructure, at the discretion of the Provider's Management.

9.5 Discussion of Results and Follow-Up Actions

1. Based on assessments and the examination report, the Provider's Management shall outline measures and deadlines for the elimination of the deficiencies and inconsistencies.
2. The staff of the Provider shall take specific actions to eliminate them within the specified period.
3. The results of the check shall be duly stored in the Provider's archive.

10 BUSINESS AND LEGAL ISSUES

10.1 Prices and fees

1. The Provider shall maintain a document "Tariff for certification, information, cryptographic and consulting services".
2. The Provider has the right to change unilaterally the Tariff at any time during the term of Contract, and shall notify the Users by posting the changes on the website.
3. Changes are effective for the User on the day following the day of publication.
4. Within 5 (five) days from the date of the change as far as an increase in the price has occurred, the User is entitled to unilaterally terminate the Contract by giving written notice to the Provider, as of the date of expiry of the last certificate. In this case, the Contract shall be terminated as of the date of change, and contract fees paid for use of services shall not be subject to refund.
5. In the absence of notice of termination, it is considered that the User agrees to the changes.
6. The change in fees cannot affect fees already paid.

10.1.1 Payments

1. The contract value includes one or more of the following payments:
   - fee for issuing and maintaining QC;
   - fee for renewal of QC;
   - fee for consultation and technical assistance provided at the request of the fee for consultation and technical assistance provided at the request of the User;
   - cost of equipment purchased or rented from the Provider;
   - fee for personalization of physical media.
2. Due fees and payments are payable to the Provider in the amounts under the Tariff for the certification, information, cryptographic and consulting services provided by "BORICA" AD, in a time and manner as specified in the Contract and annexes thereto.
3. As far as any advance or subscription fee for the use of a service has been agreed, it is not refundable if the User has not used the service during the relevant period.
4. The price does not include any amounts accrued by telecommunications companies in connection with their services used by the User in relation to services provided by the Provider. These shall be payable entirely by the User to the relevant telecommunications company. The Provider shall not be held liable and responsible for payment of these amounts.
5. All costs and fees for transferring the amounts due to the Provider’s account, including those in correspondent banks, shall be charged to the Client.

10.1.2 Fees for Certification, Cryptographic, Information and Consultancy Services

1. For the provision and use of QC and related services a fee upon requesting the relevant service. In other cases, payment shall be made within 10 days of receipt of the invoice, or as per contract.
2. Services related to provision of technical assistance and consultations for building and maintaining infrastructure and information security solutions shall be based on "man/hours" and shall be paid based on a bilateral protocol signed for the work done. The prices of the hourly rate in the Tariff are valid within the generally accepted working time. When working outside the working hours, prices shall be increased proportionately, as per the Tariff.
3. The "Issuing qualified electronic time stamps" service, upon a Service Level Agreement (SLA,) shall be paid under the contractual terms of delivery and use of service.
4. The cost of equipment purchased or leased from the Provider shall be agreed and is payable as per the terms of contract. Legal relations between the Provider and the User shall be arranged in accordance with the general rules of the Sale Contract or, respectively, the Lease Contract.
5. If payments are delayed after the agreed period, the User shall pay to the Provider legal interest for the period until the final payment of amounts.
6. The use of documents published on the website of the Provider is free. To record and provide these documents on a physical medium, the cost of the medium and the courier costs shall be charged.

10.1.3 Invoicing

1. The Provider shall issue an invoice to the User for the services provided.
2. Failure to receive the invoice does not exempt the User from his obligation to pay the due fees within the agreed deadlines.
3. All amounts due under the Contract shall be paid by the User in cash or by a bank transfer. Payment by bank transfer shall be deemed to be made after the bank account of the Provider is credited with the full amount due.
4. All bank commissions, fees and expenses in connection with bank transfers are at the expense of the User.

10.1.4 Return of Certificate and Recovery of Payment

1. A User may object to the inaccuracy or incompleteness in the content of a QC within 3 days after its publication in the Public Register.
2. If the incorrect content of a certificate is a fault of the RA/LRA, the Provider shall revoke and issue a new certificate with the correct content at their own expense, or shall refund the amount for the terminated certificate containing incorrect information.
3. If the incorrect content of a certificate is a fault of the User, the Provider shall terminate the certificate and shall not refund the payment. The Provider may issue a new certificate with correct content at the expense of the User.
4. The User can refuse a QC issued with correct content, and the Provider shall terminate it immediately, without refunding the payment for the terminated certificate.

10.1.5 Free Services

1. The Provider shall provide free registration and information services relating to the use of the Public Register, as follows:
   - check of a QC of a User published in the Register;
   - validity check of a certificate in the Public Register;
   - real-time certificate status check;
   - certificate for time of presented content/electronic statement without SLA;
   - download of a current CRL and access to CRL archive;
   - download of official certificates of the Provider;
   - download of public documents of the Provider;
   - other services.

10.2 Financial liability

10.2.1 Insurance of Activities

1. The Provider shall make compulsory insurance of its activities as a registered QTSP by the CRC;
2. The compulsory insurance shall be for a continuous period and shall be renewed periodically.
3. Subject of the insurance is the Provider's responsibility to carry out their activities in accordance with the EDETSA and the Ordinance on the Activities of Trust-Service-Providers.
4. The Provider has a compulsory insurance in the amounts specified in Art. 14, para. 1 of the Ordinance on the Activities of Trust-Service-Providers.
5. The compulsory insurance covers the liability of the Provider to the Users, respectively Relying Parties for material and non-material damage suffered, to the limits specified in the EDETSA and the Ordinance on the Activities of Trust-Service-Providers.
6. After the occurrence of an event that could lead to an insurance claim, the affected person shall notify the Provider and the Insurer within 7 days after the event becomes known.

10.2.2 Insurance Coverage

1. The insurance coverage for any non-material and/or material damage suffered by a User shall not exceed the amount established by the Ordinance on the Activities of Trust-Service-Providers.
2. The insurance shall not cover cases of waiver of responsibility, in particular for damages caused by:

- non-compliance of the User's obligations;
- compromise or loss of private key of a User due to nonperforming due diligence in use;
- non-compliance with the requirements for verification of the validity of electronic signature and the certificate by the Relying Party;
- force majeure and other circumstances beyond the control of the Provider.

10.3 Confidentiality of business information

10.3.1 Scope of Confidential Information

1. Any information of a User, which is not included in issued certificates and CRLs constitutes personal data within the meaning of the Law for Protection of Personal Data and is considered confidential.
2. The information under the preceding paragraph shall be collected by the Provider only to the extent necessary for the purposes of issuing and maintaining certificates.
3. Information considered as confidential cannot be provided to third parties without the explicit consent of its respective owners, except where the Provider is obliged by Law, including:
   - Inspections of the Commission for Personal Data Protection;
   - Inspections of external and internal auditors to demonstrate compliance with standards, laws, regulations, and other regulatory requirements explicitly required for implementation of the business processes of the Provider;
   - Providing them to state institutions if this is legally and explicitly required.
4. Confidential information shall be stored with restricted access and shall be available only to personnel of the Provider authorized to operate with the data and revealed with the explicit permission of the User, except in cases where the Provider is obliged by Law.
5. No one except the User, including the Provider, may use the private key for creating an electronic signature. The Provider recommends the Holder not to expose the user access code to the private QC key, even if it is encrypted.
6. All private keys of the staff and the units in the Provider infrastructure are reliably protected against compromise and distribution.
7. Records in registers and logs from the systems of the Provider shall be considered as confidential information and shall be protected from unauthorized access and impact.

10.3.2 Non-Confidential Information

1. Any information contained in the Public Register regarding the certificates issued (unless the User has specified a "prohibition of access" option), in the current CRL and archival copies of this list shall be publicly available.

10.3.3 Protection of Confidential Information

1. The Provider and the User have no right to disseminate or allow dissemination of information made known to them during or in connection with their obligations under the Contract, including payments, without the prior written permission of the other Party.

10.4 Personal data protection

1. The Provider is registered as data controller under the Law for Protection of Personal Data.
2. As a data controller, the Provider strictly complies with the requirements of confidentiality and non-disclosure of personal data of Users that has become known by the Provider in the performance of their business as a QTSP.
3. The personal data that is provided and gathered according 10.3.1 are stored and processed solely for the purposes of the Provider in accordance with the requirements of the EDETSA, the current regulatory framework and on GDPR.
4. According to the approved Policies of the QCs, elements of information therein may contain personal information. In order to carry out its activities and meet the specific requirements to public electronic services with regard to certified information, the Provider shall make it available to third parties through certificates issued, unless the "prohibition of access" option is selected in the

request for a certificate.

5. The User as a subject of personal data has the right:
   - Require the Provider to correct or restrict the processing of his or her personal data or to object to their processing;
   - Require the Provider to erase without undue delay his personal data to be performed by the Provider if the terms of Article 17 of the GDPR are applicable;
   - Receive their personal data upon request in the appropriate order described in 10.11.
   - The portability of personal data under the terms of Article 20 of the GDPR and the regulatory framework in the country.
   - Be advised of the corrections made, deleting and limiting the processing of his or her personal data, if he specifically requests this.
   - Submit a complaint to the Supervisory Authority - the Personal Data Protection Commission, regarding its personal data provided to the Provider

10.5 Intellectual property rights

1. Various data included in certificates issued or published in the Public Register is subject to intellectual property and other property and non-property rights.
2. The relationships regarding these rights between the Provider and other participants in the B-Trust infrastructure, such as external RAs, LRAs, etc. shall be arranged by contract.
3. All certificates issued by the Provider shall be subject to copyright of the Provider.
4. All rights on trademarks used by the Provider (e.g. B-Trust®), as well as trade names used by the Users and contained in the certificates, shall be retained by their owners and shall be used only for the purposes of trust services.
5. Key pairs corresponding to the certificates of the Provider and other participants in the B-Trust infrastructure, as well as the relevant classified material, shall be subject to the rights of the Provider and the relevant participants, regardless of ownership over the physical medium of keys.

10.6 Responsibility and warranties

10.6.1 Responsibility and warranties of the Provider

1. The Provider is responsible and guarantees for complying strictly with the conditions contained in this document, and with the requirements of the EDETSA and regulations on the activities of registered QTSP.
2. The Provider operates the activity of a registered QTSP by:
   - using equipment and technologies that provide system reliability and technical and cryptographic security of processes, including a safe and secure mechanism/key generation and electronic signature device in its infrastructure;
   - issuing QCs after verification of the submitted information by means permitted by Law;
   - storing and maintaining information relating to the issued certificates and operation of the systems;
   - complying with established operating procedures and rules for technical and physical control, in accordance with the terms in this document;
   - issuing the appropriate types of certificates upon request, complying with the conditions and procedures of this document, and with associated Policies;
   - notifying Users of the fact of its accreditation;
   - creating an opportunity for immediate suspension and revocation of the QCs;
   - performing revocation and suspension of certificates under the terms and conditions of the respective Policy;
   - immediately notifying the User after the suspension of a certificate;
   - providing conditions for precise verification of the time of issuance, suspension, renewal and revocation of certificates;
   - providing measures against forgery of certificates and the confidentiality of data disclosed in the process of creating the signature;

- using trustworthy systems to store and manage certificates;
- ensuring that only duly authorized employees have access to make changes, and verify the validity and authenticity of certificates;
- in case of technical problems relating to security, immediately informs the servicing personnel;
- by revoking the validity of the QC upon its expiration;
- informing Users and third Relying Parties of their obligations and due diligence in the use and reliance on the trust services of the Provider, as well as of the proper and safe use of certificates issued and of trust services related thereto;
- using and storing personal and other data for the purposes of its activities on providing trust services under the EDETSA and in accordance with the provisions of the Personal Data Protection Act and other relevant legislation;
- not storing or copying data used to create private keys;
- supporting materials and equipment that enable carrying out its activities;
- insuring for the duration of its activity for damages arising from breach of its obligations under the EDETSA, in compliance with the Insurance Policy;
- employing personnel with the necessary expertise, experience and qualifications to perform the activity;
- announcing and providing access to approved mobile application for cloud QES;
- maintaining a Register to publish issued QCs, an updated CRL and other circumstances and electronic documents, in accordance with this document and the EDETSA;
- providing 24/7 electronic access to the Register;
- providing protection against any unauthorized changes to the Register, as a result of unregulated and unauthorized access or by accident;
- immediately publishing in the Public Register of QCs the certificates issued and signed;
- creating conditions for each Relying Party to check the status of a certificate issued and published in the Public Register;
- in performance of its usual activity for providing all trust services of the portfolio of BORICA AD, the Provider does not discriminate in any way its clients and employees.

3. The Provider shall be responsible to the User and the Relying Party for:
   - its obligations under the preceding paragraph;
   - any incorrect or missing data in a certificate due to his/her fault;
   - any omissions in establishing the identity of the Applicant.

10.6.2 Responsibility and warranties of the RA/LRA

1. The Provider shall ensure that RA/LRA perform their functions and duties in full compliance with the terms in this document, with requirements and procedures of the Policy and internal operational instructions.
2. The Provider shall be held liable for any actions of a RA/LRA in the B-Trust infrastructure.

10.6.3 Responsibility of the User

1. The User must:
   - follow precisely the conditions and procedures of this document and the relevant Policy upon request for issuance of certificate and use of other trust services;
   - pay the due remuneration to the Provider under the Contract and annexes thereto;
   - have basic knowledge on the use of electronic signature certificates and PKI technologies;
   - provide true, accurate and complete information to the Provider as required by law and this document when applying for the issuance and management of the certificate;
   - provide secure and reliable environment and procedure (reliable technical means and software), when generating the key pair outside the infrastructure of the Provider in order to protect the confidentiality of the private key;
   - use algorithms in accordance with the requirements of the Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature when generating

the key pair;
- notify the Provider immediately in case of compromise or suspected compromise of the private key by sending a request for suspension or revocation of the certificate;
- securely store and protect the private key during the whole validity of the certificate against loss and compromise, in accordance with the requirements of the relevant Policy. Any use of the private key shall be considered as an act committed by the User;
- accept the issued certificate for electronic signature immediately after it is presented by the Provider;
- verify the completeness and accuracy of the contents of the certificate within 3 (three) days after its publication. In case of a discrepancy between the information provided under the contract and the certificate, the User shall notify the Provider immediately;
- notify when a change occurs in the certified information and request revocation of the certificate;
- notify the Provider of any change in information not included in the certificate issued, but which is provided in the process of issuing the certificate;
- change their initial access code to the private key /QSCD, before using the certificate;
- use their issued certificates only with licensed cryptographic software;
- use a certificate only in accordance with its intended purpose and in accordance with the applicable Policy and in view of the limitations under which it is issued;
- not use the private key to create an electronic signature after the expiration of the certificate or after its suspension or revocation;
- inform each Relying Party of their due diligence and responsibility when relying the QC;
- accept the conditions of due diligence and responsibility when relying the QC, in the event that they act as a Relying Party.

2. The User shall be held liable if accepted a QC issued by the Provider based on untrue data submitted by them, respectively, based on concealed or missing data.
3. The Provider shall regress to the User any claim for damages resulting from incurred liability of the Provider for failure of obligations arising from this document or from the Contract, if the User:
   - has used an algorithm which does not meet the requirements of the Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature;
   - does not meet strictly the security requirements set by the Provider;
   - fails to request revocation of the certificate when aware that the private key was used improperly or is in danger of unauthorized use;
   - has accepted the certificate being issued when the User was not authorized to hold the private key corresponding to the public key in the certificate;
   - has accepted the certificate being issued by making untrue statements to the Provider relating to the contents of the certificate;
   - has accepted the certificate when the User was not been authorized to apply for the issuance of the certificate.

10.6.4 Due Diligence and Responsibility of the Relying Party

1. Persons who trust QCs must have basic knowledge about the principles of use and applicability of the electronic signature/seal and the services related to the use of the certificate.
2. The Relying Party should perform due diligence by:
   - trusting the certificates only in terms of the Policy regarding their purpose, and the limitations and conditions under which they are issued;
   - checking the status of the certificate before trusting it in the Provider's public register. A check of the electronic authenticity and integrity of the certificate outside the Public Register or in an outdated CRL does not provide verification of its validity and any damages resulting by actions taken after only such a check shall be borne by the Relying Party;
   - verifying the validity of electronic signature/seal, and the validity of electronic signature/seal of the Provider along the chain of certificates to the base certificate;

- ensuring that the applications, with which the certificate is used, are functionally relevant for its intended purpose, and are relevant to the level of security specified in the Policy.

3. Due diligence of the Relying Party is to use secure (qualified) check (validation), which ensures that:
   - the public key used to verify the signature/seal matches corresponds to the one presented in the certificate;
   - the verification of the private key usage is reliably confirmed, and the results of this verification are presented correctly;
   - if necessary, the contents of the signed/sealed electronic document/statement can be identified;
   - the authenticity and the validity of the certificate at the time of signing/sealing are reliably verified;
   - the results of the verification and the electronic identity of the User are presented correctly;
   - any changes relevant to security are identifiable.
4. The Provider shall not be held liable for any damages to the Relying Party incurred by lack of due diligence.

10.7 Disclaimer

1. Except in cases of damages suffered from the use and reliance on QCs, the Provider shall not be held liable for their own negligent.
2. The Provider shall not be held liable in cases where the resulting damages are the result of negligence, lack of due diligence or lack of basic knowledge about the technology of electronic signature of the Signatory, or of Relying Parties.
3. The Provider shall in no way be held liable for cases, when statements signed and accompanied by valid certificates have been withdrawn.
4. The Provider shall not be held liable when a software application or data objects have been signed, and these have caused damage to the Relying Party.
5. The Provider shall not check or monitor the violation of rights of third parties regarding their trademarks, trade names or other property or non-property rights when information contained in certificates issued has led to such violations. In case of any damages suffered by the Provider because of such violations, the Provider may claim them by the User.
6. The Provider shall not be held liable for any direct or indirect, foreseeable or unforeseeable damages that have occurred as a result of use or reliance on suspended, revoked or expired certificates.
7. In addition to the cases under the preceding paragraphs, the Provider shall not be held liable for:
   - the accuracy, authenticity, completeness or suitability of the information included in test, free or demonstration certificates;
   - quality, features or technology of software applications and hardware devices in the infrastructure of B-Trust, used by Holders or Relying Parties;
   - for timely revocation and suspension of certificates and/or for check of the status of certificates for reasons beyond their control (e.g. lack of due diligence by a Relying Party, fraudulent action by a User, telecommunication and power interference, etc.).
8. The Provider shall not be held liable for any damages caused by use of a QC beyond the scope of its intended uses and applicable restrictions.

10.8 Limitation of liability of the Provider

1. For the QCs for QES/QESeal issued, the Provider shall be held liable within a maximum limit of liability - BGN 40 000.
2. The above-specified limit shall be considered limitation of liability of the Provider.

10.9 Indemnities for the Provider

1. For all cases of non-performance of the obligations of the User, the Provider shall seek

responsibility from the Holder for damages and shall have the right to terminate the certificate immediately.

10.10 Term and termination

1. The provisions in this document and the associated Policies on the provision of QCs and trust services by the Provider are valid until issuing and publication of their next version/revision in the repository of documents on the Provider's website.
2. The Contract for trust services between the Provider and the User is valid for a period of three years or until the expiration of the last issued certificate under the Contract.
3. Upon termination of the Provider's activity, the provisions, the Practice Statement and the Policies associated to this document shall be also terminated.
4. In the event that a clause in this document becomes invalid, the validity of the entire document shall be retained and the contract with the User shall not be violated. The invalid clause shall be replaced by mandatory rules of law.
5. The Contract for trust services between the Provider and the User shall be terminated upon expiration of validity of the last issued certificate under the Contract or with the termination of all the certificates issued under the Contract.
6. The Provider shall keep duly and securely all previous versions/revisions of this document and the associated Policies.

10.11 Notices and communication between participants

1. The Provider shall use statements, letters and messages of the RA/LRA, as well as electronic notices published on their website.
2. B-Trust clients can send messages, letters, recommendations, questions and complaints to the Provider using the following address:

   Mailing address: 1612 Sofia, 41"Tsar Boris III" Blvd
   Phone: 0700 199 10
   E-mail: info@b-trust.org
   Official website of the Provider: https://www.b-trust.bg/documents
3. In case of receiving a complaint, the Provider shall perform an immediate inspection and send a reply to the complainant within 2 working days.

10.12 Amendments to the document

1. The Provider may make editorial changes in this document that do not affect the rights and obligations contained herein.
2. Any changes that lead to a new version/revision of this document shall be published on the website of the Provider.
3. The changes shall be communicated to the CRC and stakeholders.
4. Any person may make suggestions for changes and elimination of errors, by using the above contact details of the Provider.

10.13 Dispute settlement (jurisdiction)

1. Any disputes between the Parties to the Contract for trust services shall be settled by agreement between the Parties, through understanding and in the spirit of goodwill, and if no agreement is reached, they shall be settled by the competent Bulgarian court.

10.14 Governing law

1. For matters not covered in this document, the provisions of the Bulgarian legislation shall apply.

10.15 Compliance with applicable law

1. This document is prepared in compliance with the EDETSA and current regulations.