CERTIFICATION PRACTICE STATEMENT

OF THE B-TRUST® QUALIFIED CERTIFICATION SERVICES PROVIDED BY BORICA AD

Policy on issuing qualified certificates for qualified electronic signature and Practice in the provision of qualified certification services

Version 3.2

July, 2017

History of changes to the document				
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.

CONTENTS

ABBREVIATIONS

AD	Joint Stock Company JSC
PIN	Personal Identification Number
ES	Electronic Signature
EDESA	Electronic Document and Electronic Signature Act
QES	Qualified Electronic Signature
QC	Qualified Certificate
QCS	Qualified Certification Services
QCQES	Qualified Certificate for Qualified Electronic Signature
QTSP	Qualified Trusted Services Provider
CRC	Communications Regulation Commission
MTC	Ministry of Transport and Communications
LRA	Local Registration Authority
OACSP	Ordinance on the Activities of Certification Service Providers, the Terms and Procedures of Termination thereof, and the Requirements for Provision of Certification Services
ORQESA	Ordinance on the Requirements for development and verification of Qualified Electronic Signature Algorithms
CPS	Certification Practice Statement for the B-Trust® certification, information, cryptographic and consulting services provided by "BORICA" AD
Practice	Common practice in the provision of qualified certification services
Policy	Policy for the provision of qualified certification services
Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
RA	Registration Authority
CA	Certification Authority
BG	Bulgaria
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CD	Compact Disk
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
DN	Distinguished Name
ETSI	European Telecommunications Standards Institute

EU	European Union
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEC	International Electrotechnical 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
QES	Qualified Electronic Signature
RA	Registration Authority
RSA	Rivest - Shamir - Adelman
QSCD	Qualified Signature Creation Device
B-Trust QSCD	QSCD with protected profile that meets the requirements for security level EAL 4 or higher, according to CC or other specifications defining equivalent security levels
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

COMPLIANCE AND USE

This "Certification Practice Statement":

- is developed by "BORICA" AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- completely replaces all previous versions of the document "Certification Practice Statement";
- enters into force on 01.06.2017;
- contains the conditions under which the Qualified Trusted Services Provider (QTSP) "BORICA" AD (Provider) provide paying customers with qualified certificates (QC) and related qualified certification services (QCS), as well as other information, cryptographic and consulting services under the registered trade mark B-Trust, through an independent unit - B-Trust® Certification Authority, in accordance with the requirements of the Electronic Document and Electronic Signature Act (EDESA);
- constitutes the General Conditions under Art. 33, para. 2 of the Ordinance on the Activities of Certification Service Providers (OACSP) and within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These conditions are part of a written Contract for certification services, which shall be concluded between the Provider and Users under Art. 23 of EDESA. The contract may contain special conditions and if so, these shall take precedence over the general conditions of this CPS;
- includes a detailed description of policies and practices in the provision of QCS by the Provider and is a public document aimed to bring the Provider's activities in line with EDESA and other relevant regulations;
- is publicly available at any time on the Provider's website;
- may be changed by the QTSP and each new version of the CPS shall be published on the Provider's website;
- includes two parts:
- **PART I**: Practice for the provision of qualified certificates and qualified certification services (Qualified Certification Practice Statement, QCPS);
- **PART II**: Policies in the provision of qualified certificates and qualified certification services (Qualified Certificate Policy, QCP);

This document is prepared in accordance with:

- the Electronic Document and Electronic Signature Act (EDESA);
- Ordinance on the activities of Certification Service Providers, the terms and procedures of termination thereof, and the requirements for provision of certification services (OACSP);
- Ordinance on the Requirements for development and verification of Qualified Electronic Signature Algorithms (ORQESA);
- Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The content and structure of this document is in accordance with Regulation (EU) No 910/2014 and refers to the information contained in the following well-established 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: Policy and security requirements for Trust Service Providers issuing certificates
- ETSI EN 319 412: Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

Information concerning this document may be obtained from the Provider at:

41 "Tsar Boris III" Blvd.
Sofia 1612
"BORICA" AD
tel: 02/ 92 15 115
e-mail: info@b-trust.org
Official website of the Provider: www.b-trust.org

PRACTICE IN THE PROVISION OF QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE AND QUALIFIED CERTIFICATION SERVICES

Practice in the provision of QCQES and QCS:

- is an integral part of this document and contains general procedures for the issuing, suspension, renewal and revocation of QCQES, security measures in the provision of QCS, staff requirements, the profile of QCQES currently issued and maintained, and conditions for access to issued and revoked QCQES;
- is implemented in the work of the operational Certification Authority of the Provider and shall be marked with the following identifiers:

Provider's Practice	Identifier(OID)
B-Trust Certification Practice Statement(CPS) for Qualified Certificates (Practice for provision of QCQES)	O.I.D. = 1.3.6.1.4.1.15862.1.6

- uses the following algorithms for electronic signature and data protection:

Algorithm	Name
Hash algorithms:	SHA256
Asymmetric algorithms:	RSA

POLICY OF PROVIDING QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE AND QUALIFIED CERTIFICATION SERVICES

The policy of providing QCQES and QCS:

- describes conditions the Provider complies with and follows in the process of issuing of QCQES, and the applicability of these certificates in view of the security level and restrictions on their use;
- is a set of specific procedures to be followed in the process of issuing and maintaining QCQES, from the identification requirements, conditions and requirements for security level during the creation of the electronic signature and for storing the private key;
- determines the applicability and the level of confidence in facts certified by QCQES.

1. The Provider implements a common Policy for all types of QCQES, which is marked with the following identifiers:

Provider's Policy	Identifier (OID)
B-Trust Personal Qualified Certificate Policy (QCP-n-qscd) (Policy for providing QCQES to individuals)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 (O.I.D. = 0.4.0.194112.1.2)
B-Trust Professional Qualified Certificate Policy (QCP-n-qscd) (Policy for providing QCQES to an individual associated with a legal entity)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 (O.I.D. = 0.4.0.194112.1.2)

Under this policy, the Provider shall issue and support the following types of QCQES:

- personal QCQES to an individual "B-Trust Personal qualified certificate QES";
- professional QCQES to an individual associated with a legal entity "B-Trust Professional qualified certificate QES".

2. The Provider hereby reserves the right to expand the supported certification Policies via the operating Certification Authorities.

PART I:

CERTIFICATION PRACTICE STATEMENT -

IN THE PROVISION OF QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE AND QUALIFIED CERTIFICATION SERVICES

INTRODUCTION

The Practice in the provision of QCS is an integral part of this document, developed by QTSP „BORICA" AD and approved by the CRC.

This part of the document contains a description of the participants in the infrastructure of B-Trust® public keys and its components, used by the Provider to issue, maintain, publish and manage QCQES. It describes the general operating procedures during application for QCQES, identification of Applicants, issuing and publishing, delivery and acceptance of QCQES, maintenance and management of these certificates, as well as procedures for granting access to verification of certificates.

The practice also includes the measures and technical procedures followed by the Provider to ensure safety and reliability of the QCS provided via the B-Trust® infrastructure, in accordance with EDESA 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 requirements under EDESA.

1. GENERAL

1.1 Provider of Qualified Certification Services

1. "BORICA" AD is a legal entity – trader, operating as a QTSP under EDESA and other relevant regulations.
2. As a registered QTSP, "BORICA" AD carries out the following regulated activities:

- Issuing QCQES:
  - acceptance of an application for initial issuing;
  - authentication of the identity and validity of the Titular's details;
  - provision of services creating cryptographic key pairs - private and public key;
  - signing QCQES with an advanced electronic signature of the QTSP;
  - recording the issued QCQES.
- maintenance and management of QCQES:
  - renewal of a valid QCQES;
  - changing the status of a valid QCQES - suspension, renewal and revocation;
  - checking the status of a QCQES;
  - checking the status of a QCQES in real time (OCSP status).
- keeping of records:
  - keeping a Public Register of all issued QCQES;
  - publication of issued QCQES in the Public Register;
  - keeping a list of all revoked QCQES;
  - Immediate publication of a revoked QCQES in the list of revoked certificates;
  - permanent access of third parties to the Public Register and to the list of revoked certificates.
- checking (validation) of electronic signatures.
- providing QSCD for generation and storage of cryptographic keys and for creation of QES.
- certification of time:
  - certification of the exact time of delivery of the content of electronically signed/stamped documents (time of signature/stamp);
  - certification of content at a particular time and irreversibility of content beyond this point;
  - evidence-based inspection of qualified electronic time stamp tokens issued.

3. The Provider provides the QCS specified in accordance with current Practices of the Certification Authority and the Policy specified in the respective certificate.
4. The Provider may provide other qualified certification, cryptographic, information and consultancy services relating to the applicability of the certification services, following generally accepted recommendations, specifications and standards.
5. The Provider may publish separate terms and conditions for these QSC.

1.2 Regulation and Control

1. "BORICA" AD has informed the CRC of the start of operations as a QTSP under EDESA and current regulations.
2. Accreditation of "BORICA" AD as a QTSP by EDESA aims to achieve the highest security level of QCS provided and better harmonization of these activities with similar activities provided in other Member States of the European Union.
3. The Provider shall notify all Users of this accreditation during the provision of QCQES and related QCS.

1.3 Identifiers in the Document

1. Provider's practice in issuing and maintaining QC shall be implemented through the operational Certification Authority:

Operational CA	Identifier (OID)
B-Trust Operational Qualified CA (CA for QCQES)	O.I.D. = 1.3.6.1.4.1.15862.1.6.1

2. Provider's policy on QCQES and QCS provided for them is indicated in the QC issued with the following identifiers:

Qualified Certificate	Name	Policy (OID)
Personal QCQES to an individual	B-Trust Personal qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2
Professional QCQES to an individual associated with a legal entity	B-Trust Professional qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2

3. The Provider follows specified Policy indications for the types of QCQES issued and maintained:

Qualified Certificate	Name	Policy
Personal QCQES to an individual	B-Trust Personal qualified certificate QES	B-Trust Personal Qualified Certificate Policy
Professional QCQES to an individual associated with a legal entity	B-Trust Professional qualified certificate QES	B-Trust Professional Qualified Certificate Policy

1.4 Participants in the B-Trust® Infrastructure

1.4.1 Certification Authority

1. The B-Trust® "Certification Authority" of QTSP "BORICA" AD is a separate organizational unit which operates its' QCQES activities on the provision and maintenance of QCS. The CA has no legal personality and all its operations and activities of its employees are performed in their capacity of employees of the Provider, within their respective powers.
2. The B-Trust® infrastructure has a two-tier hierarchy of the CA for issuing and maintaining QCQES, as follows:
   - Basic CA ***"B-Trust Root Qualified CA"*** - issuing certificates to subordinate operational certification authorities of the Provider and those of other Providers.
   - Operational CA ***"B-Trust Operational Qualified CA "*** - issuing QCQES under the policy for provision of QCS;
3. QTSP reserves the right to expand 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 QCQES;
   - registers applications submitted to the CA for issuance and implements changes in the status of QCQES;
   - performs appropriate checks to verify the identity of the individuals and legal entities, as well as specific details about them using all means admissible, and in accordance with the Policy and Practice in the provision of the respective QCS;
   - notifies the CA to issue QCQES after successful identification and finalized payment for the service;
   - delivers to the Titular the QCQES issued, corresponding to the generated key pair;
   - accepts or rejects registered requests for maintenance and management of QCQES, in accordance with established Practice and Policy;

- concludes contracts for the provision of certification and other cryptographic, information and consultancy services with the Titulars on behalf of the Provider.

2. The Registration Authority may be a separate unit within a legal entity other than Provider, assigned with the task to perform these activities or any part thereof on behalf of the Provider.
3. The Provider's Registration Authority (RA) may provide certification services to Users via the Local Registration Authorities (LRA).
4. When the RA/LRA is a separate legal entity, the power to carry out this activity may be limited by territory, term, certification services, or for a particular category of Titulars. The power is certified before all Applicants and third parties with a written or electronic certificate of the RA /LRA.
5. In cases where the RA is a separate legal entity, LRAs to this body may be opened after explicit approval of the Provider only.
6. Relations between the Provider and the RA /LRA under item 4 shall be governed by a contract.
7. The Provider shall ensure that the activities of the RA /LRA will be consistent with the terms of this CPS.

1.4.3 Qualified Electronic Time Stamp Authority

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

1.4.4 OCSP server

1. "OCSP server" is a separate and integrate unit of the CA, which executes the following activities of the Provider:
   - accepts requests from the Titular or a Relying Party to check in real time the status of issued by the Provider certificate;
   - prepares automatically in real time an electronically signed response on the status of a certificate.
2. OCSP servers of the Provider are: „B-Trust Root Qualified OCSP Authority" and „B-Trust Qualified OCSP Authority"
3. Each Relying Party, when receiving QCQES, may apply for a real time check of certificate status.
4. Real time status checks of certificates are not mandatory for Relying Parties, but the Provider recommends to use this service and its integration in the process of creation or acceptance of electronically signed documents, during inspection and acceptance of electronic transactions, etc.

1.4.5 Titular

1. "Titular" of a QCQES is an individual who creates the electronic signature.

2. The Titular carries out electronic statements on their own behalf, or on behalf of other person, represented by him, and signs them electronically in accordance with its representative authority.
3. In the QCQES can be indicated the person, represented by the Titular.
4. Only the Titular of the QCQES is entitled to access the private key for signing electronic statements (creating a qualified electronic signature).

1.4.6 Relying Parties

1. "Relying Parties" are the recipients of signed electronic statements, which Titulars have QCQES issued by the Provider.
2. Relying Parties should have the knowledge and skills to use QCQES and trust circumstances certified therein only in terms of the applicable Policy, especially regarding the security level when checking the Titulars of these certificates.
3. Relying g Parties have permanent access to the records of the Provider to check the validity of QCQES, to establish the Titulars or other circumstances and data contained in the certificates or recorded in these records.

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 showing the relationship between the Titular and the public key corresponding to the private key with which the Titular has created the electronic signature. It is used to check the signature on electronic documents and objects.
2. QCQES can be used for activities that require electronic documents signing, execution of electronic transactions and authentication.
3. Only certificates with policies listed in this document, issued by the Provider, have the character of QC and contain the requisits provided for in Art. 24 EDESA.

1.5.2 Certificates of the Provider

Root certificate

1. Root certificate of the Provider is a certificate that is self-issued and electronically elf-signed with the private key of the Provider QC for his root public key. The root private key is used by the Provider to electronically sign certificates for public keys of its operational and CA, and Certificates of other (sub-) providers of certification services in the infrastructure of B-Trust.
2. In accordance with EDESA 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 particulars of the root certificate of the Provider's CA "B-Trust Root CA" are:

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 f7 26 40 fa 05 05 fb d1 5a b0 93 e8 98 db 27 dd 29 14 e8

3. Pursuant to Art. 16, para. 3, item 2 of EDESA, electronic stamps of the Provider accompanied by the root certificate are qualified.
4. The Provider may install and maintain other root certificates in the infrastructure of B-Trust.

Operational certificate for issuing of QCQES

1. Certificate of Provider's operational CA of issuing of QCQES is the qualified certificate for public key of the operational CA "B-Trust Operational Qualified CA", electronically stamped with the basic private key of the Provider. Operational CA shall stamp electronically the QCQES issued by the Provider to the Titulars with the private key corresponding to this public key. Main requisits of the operational certificate of the Provider's CA "B-Trust Operational Qualified CA" are:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	02
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	-	2017-04-25T18:36:00Z
Validity to	-	2032-04-24T18:36:00Z
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=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)	-	51 96 52 17 9e 78 be e2 2e a8 13 14 72 7a 8f 60 67 17 2f 32
Thumbprint (Sha256)	-	64 fc 3f 77 db b8 3d a2 79 2a e4 cb 2c d0 ef 3d bb e7 92 7e 9b 80 74 54 de 14 f7 69 77 8d 34 8d

2. Pursuant to Art. 16, para. 3, item 2 of EDESA, electronic stamps of the Provider accompanied by this operational certificate are qualified.
3. The Provider may install and maintain other operational certificates in the infrastructure of B-Trust.

Certificate of OCSP server

1. Certificate of the OCSP server of the Provider "B-Trust Root Qualified OCSP Authority" is a QC for the public key of "B-Trust Root Qualified OCSP Authority", signed with the basic private key of CA "B-Trust Root Qualified CA" of the Provider. The private key of the key pairs of the OCSP server "B-Trust Root Qualified OCSP Authority" is used by the Provider to stamp the result/response of the real-time verification of the status of submitted QSQES, issued by the root certificate of CA "B-Trust Root Qualified CA". Requisites of the official certificate of the Provider's Authority "B-Trust Root Qualified OCSP Authority " are:

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

2. Certificate of the OCSP server of the Provider "B-Trust Qualified OCSP Authority" is a QC for the public key of "B-Trust Qualified OCSP Authority", signed with the private key of the operational CA "B-Trust Operational Qualified CA" of the Provider. The private key of the key pairs of the OCSP server "B-Trust Qualified OCSP Authority" is used by the Provider to stamp the result/response of the real-time verification of the status of submitted QSQES, issued by the operational CA "B-Trust Operational Qualified CA". Requisites of the official certificate of the Provider's Authority "B-Trust Qualified OCSP Authority " are:

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

3. Electronic stamps of the Provider accompanied by the official certificates of "B-Trust Root Qualified OCSP Authority" and "B-Trust Qualified OCSP Authority" are QC for electronic stamp.

1.5.3 Certificates of Other Operational Authorities

1. The Provider may issue operational QC to other CA in the infrastructure of the B-Trust, and other providers when the latter:
   - perform activities outside those legally stipulated in EDESA, in order to function as providers;
   - mutually certify public operational keys to enhance the credibility of certification services (cross-certification);
   - perform the legally regulated activity of a QTSP under the EDESA.
2. Issuing of these certificates is based on a specific agreement with the respective providers.

1.5.4 User Qualified Certificates

1.5.4.1 Qualified Certificates for Qualified Electronic Signature

1. Provider issues to Users QCQES depending on Applicants, the scope of application and purpose of electronic signature:
   - personal QCQES "B-Trust Personal Qualified Certificate QES";
   - professional QCQES "B-Trust Professional Qualified Certificate QES";

2. The Policy and practice of the Provider under this document sets the safety rules and requirements applicable to the issuing and use of QCQES.
3. The Provider issues a QCQES only to individuals.
4. Personal QCQES "B-Trust Personal Qualified Certificate QES" is issued personally to an individual – the Titular.
5. Professional QCQES "B-Trust Professional Qualified Certificate QES" is issued to an individual – the Titular, representing other legal entity under the Law or under a Letter of Attorney.
6. Application for registration and issuing of the QCQES is made online or locally in an office of the RA/LRA, and the identification procedure through validation of the Titular's identity requires from the Titular to be present in person or a person explicitly authorized by the Titular. The identity of the represented person, respectively the individual represented by the Titular (if present) is also checked. The identification procedure and procedures to generate the key pair, and for the issuing and delivery of the QCQES to the Titular guarantee highest level of security of the Titular's data in the certificate and their relation with the public key.
7. QCQES "B-Trust Personal Qualified Certificate QES" and "B-Trust Professional Qualified Certificate QES" and their corresponding private keys are stored and made available to the Titular on QCCD.
8. QCQES are equivalent to a handwritten signature for all purposes within the meaning of Article 13, paragraph 4 of EDESA.

1.5.5 Use of User Qualified Certificates

1. QCQES issued for Users by the CA of the Provider can be used as per the Policy for this certificate.
2. Each QCQES for Users contains as requisite a particular field for use of the certificate. This requisite is identified as "Key Usage" in compliance with RFC 5280 and may be used simultaneously for one or several of the following purposes:
   - digital signature (digitalSignature) – to enable digital signing of electronic statement or content and its verificatio;
   - non-repudiation (nonRepudiation) - to enable subsequent proof to the Titular, of the fact of signature of an electronic statement or content, and to neutralize any possible repudiation of signatures;
   - key encipherment (keyEncipherment) - to encrypt and/or decrypt keys used to encrypt data;
3. Particular "Extended Key Usage" in compliance with RFC 5280, which is also contained in QCQES issued by the Provider, is used to detail the applicability of the certificate in view of its purpose.
4. The applicability of the types of QC issued is as follows:

Type of Certificate	Applicability
Personal QCQES for individual "B-Trust Personal Qualified Certificate QES"	Personal electronic identity in applications requiring highest level of security - web-based e-commerce applications, electronic signing of documents, electronic signing of contracts, bank transactions, correspondence and statements to and from state authorities and local government under the EDESA.
Professional QCQES for individual "B-Trust Professional Qualified Certificate QES"	Electronic professional identity in applications requiring the highest level of security - web-based e-commerce applications, electronic signing of documents, bank transactions, correspondence and statements to and from state authorities and local government under the EDESA.

1.5.5.1. Limitation of a Certificate's Scope

1. If the QCQES is issued with a limitation of its scope and in accordance with Article 24, Paragraph 1, Item 8 of EDESA, the Provider's practice allows a restriction to be made in the certificate, in relation to purposes and/or value of transactions between the Titulars using the signature.
2. The Provider must use the particular "Qualified Statements" in the QCQES.

3. The restrictive scope of QCQES issued in terms of value of transactions concluded between Titulars using an electronic signature shall be agreed between them and any Relying Party and is beyond the scope of this CPS.

1.5.5.2 Use of Certificates outside the Scope of Application and Limitations

1. When the Titular or Relying Party use and trust on a QCQES with use other than the specified in the requisites "Key Usage", "Extended Key Usage", "Certificate Policy" or "Qualified Statements", this is entirely their responsibility and the Provider shall not be held liable in any way.

1.6 Management of Provider's Policy and Practice

1. Provider's policy and practice are subject to the administrative management and control of the Board of Directors of "BORICA" AD.
2. Any changes, revisions and additions that do not affect the rights and obligations arising from this document and the standard agreement between Provider and Users may be introduced after consultation and approval by the Board of Directors only.
3. Each new version or revision of this document presented and approved shall immediately be published on the website of the Provider.
4. Comments, queries and clarifications on this document may be addressed to:
   - e-mail address of the Certification Authority: info@b-trust.org;
   - e-mail address of the Provider: info@borica.bg;
   - Phone: (02) 9215 115, Fax: (02) 981 45 18

2 OBLIGATION TO KEEP AND PUBLISH RECORDS

2.1 Public Register

1. Provider shall keep an electronic Public Register to publish:
   - all QCQES issued to Users and a current List of suspended QCQES (CRL), as well as the Provider's own official certificates;
2. The Public Register of all certificates issued and current CRLs shall be permanently available, except in the case of events beyond the control of the Provider or force majeure.
3. The Titular of a QCQES issued by the Provider is required to verify the accuracy and completeness of information contained in this certificate, despite it being formally accepted.
4. Upon request, the Provider shall provide any third party with information concerning the status of issued QCQES. The Provider shall provide the information contained in the certificate issued, subject to legal obligation to do so and upon a properly filed request by an authorized body or person.
5. Current CRL contains information about all QCQES suspended and revoked until its publication in the Register. A suspended certificate shall be maintained in the CRL for a period of time stipulated by the EDESA and specified in this CPS. If the certificate is resumed or expired, it will be removed and the updated CRL shall be published without it.

2.2 Public Repository of Documents

1. Provider shall publish and maintain an electronic repository with all current and previous versions of:
   - General terms and conditions contained in this CPS;
   - Practice in providing QCS;
   - Policy on provision of QCS;
   - Contract for QCS;
   - Tariff for all QCQES provided;
   - Rules for issuing QCQES;
   - Terms and Conditions for use of QES, including requirements for storing the private key;
   - Documents required for initial issuance of QCQES, for renewal and suspension/revocation of QCQES;
   - Other documents required by regulations and EDESA.

2.3 Publication of Certificate-Related Information

1. Provider shall immediately publish in the Register a valid certificate after it has been issued by the operational CA "B-Trust Operational Qualified CA".
2. Provider shall immediately publish an updated current CRL, signed by the operational CA upon revocation/suspension of a valid certificate. Current CRL shall include the terminated and/or suspended certificate.
3. The effective period of validity of the current published CRL is 30 days, unless it is updated within this period.

2.4 Frequency of Publication

1. Public Register of issued certificates shall be updated automatically and immediately after the publication of any newly issued valid certificate.
2. The current CRL shall be updated automatically in a period of no more than 3 (three) hours or immediately after the revocation or suspension/resumption of a valid certificate. In every CRLs the QTSP states a time for next CRL issue.
3. A new edition or version of the CPS, and of other accompanying documents under EDESA shall be published immediately.

2.5 Access to Registry and Repository

1. Provider shall keep a Public Register of certificates issued, which shall be made publicly available online.
2. Provider may not restrict access to the Public Register. To protect the privacy of Users, third party access to download the published evidence shall be limited, unless the User has explicitly requested for such access to be free.
3. There shall be no limits to access the CPS and its conditions, practices and policies. Any interested person shall have access to the published documents.
4. There shall be 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 CRLs for electronic reading or download.
6. Any interested person shall have free access to official certificates of the Provider.
7. The Provider shall provide free access to all basic and operational certificates of their active certification bodies, and free access to all such inactive certificates for a period of not less than two (2) years after the expiry of validity of these certificates.

3 IDENTIFICATION AND AUTHENTICATION

1. Provider, through its RA /LRA:
   - accepts applications for issuance of QCQES;
   - carries out checks to identify the Titular, as well as specific details of him/her by using all admissible means;
   - approves registered applications 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 Titular.
3. Authentication/identification of the Titular after registration and before issuing the QCQES requires for him/her to be present in person, or the presence of an authorized representative of the Applicant before the RA/LRA.
4. The Provider shall ensure that the individuals and legal entities are properly identified, authenticated and that requests for issuing QCQES are fully, accurately and duly verified and approved, including: full name and legal status of the relevant individual/legal entity; evidence for the connection between the certified data and the individual/legal entity.

3.1 Naming

3.1.1 Use of Names

1. QCQES are in a format conforming to the X.509 RA/LRA standard, working on behalf of the Provider and shall confirm that names specified in the applications for certificates comply with the H.509 standard.
2. The field "Subject" in the certificate electronically identifies the Titular of the public key in the QCQES.
3. Name and other individualizing characteristics of the Titular in the appropriate fields for each type of certificate shall be in accordance with the DN (Distinguished Name), formed according to H.500 and H.520 standards.
4. Official certificates of the Provider, in the fields "Subject" and "Issuer" contain a DN attribute forming its unique name.
5. Detailed specification of QCQES issued by the Provider is contained in the relevant chapters of this document.

3.1.2 Use of Aliases

1. Provider may issue a QCQES using an "Alias" to name the Titular only after the RA /LRA has collected the necessary information about his/her identity and successfully identified such person.

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. QCQES of Users include names matching the authenticated identification names of the Titular, who are the subjects of these certificates.
3. For convenient electronic communication with the Titular, the Provider shall request and certify in the QCQES the Titular's email address. In the event that the latter has no such address, the Provider may provide an email address in the B-Trust domain.

3.1.4 Rules for Name Interpretation

1. Provider shall include in Users' QCQES information for the electronic identification of the Titular that has been successfully checked and validated by the RA/LRA, based on submitted identity documents of the Titular.

2. In all certificates where Titular is entered, the field for name of the person (Common Name, CN) shall contain the full name of the person with which he/she normally identifies himself/herself in their activity.
3. In a professional certificate, the distinguished name (DN) attribute shall contain information about the identity of the entity represented by the Titular.

3.1.5 Unique Names

1. Electronic identification of the Titular of a QCQES issued by the Provider is based on the DN.
2. "Subject" field in the certificate is based on the information about the Titular, to be provided online or on paper by the Applicant or by an authorized agent 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 Titular in the B-Trust domain by adding specific requisites to ensure such uniqueness.
4. A Titular with a unique DN in the B-Trust domain can have more than one valid QCQES issued.
5. Each certificate issued has a unique serial number ("SerialNumber") in the domain of the Provider (B-Trust). The combination of fields "Issuer", "SerialNumber" and "Validity from" ensures the uniqueness of the issued certificate in the public domain.

3.1.6 Recognition, Authenticity and Role of Trademarks

1. A Titular is not allowed to apply for certification 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 terminate it.
5. The Provider does not include trademarks, logos or other graphic material in the certificates.

3.2 Initial Identification and Authentication

1. For the purposes of initial identification/authentication of a Titular of a QCQES, the Provider shall require an application for initial issuance of a certificate.
2. Application for initial issuance of a certificate before the RA/LRA of the Provider is a procedure by which Provider requires, collects and receives information necessary to identify the Titular of the certificate.
3. The registration procedure includes:
   - completing the registration form for issuance of QCQES;
   - generating a key pair;
   - preparing the electronic application containing the public key for which the certificate is to be issued;
   - submitting the required documents to the RA /LRA, in accordance with the Policy of QCQES issuance;
   - an option for application for other services related to the certificate.
4. Identification of the Titular after registration and prior to issuing the requested QCQES requires them to be present in person or to send authorized representative before the RA /LRA.
5. The initial identification and identity verification include:
   - the Titular or the person explicitly authorized by the Titular keeping a private key corresponding to the public key submitted to the Provider for issuing of the certificate;
   - checking and confirming the identity of the Titular of the certificate to be issued.
6. Upon successful verification of the identity of the Titular, the authorized operator in the RA/LRA shall:

- offer a QCS contract signed on behalf of the Provider and store all documents to the contract submitted;
- confirm the application for issuing and send the electronic application for a certificate to the operational CA of the Provider;
- may save the certificate issued on a QSCD and deliver it to the Titular, or to an authorized person.

3.2.1 Proving Possession of Private Key

1. RA/LRA checks the compliance of the submitted public key, which is certified in the certificate issued by the Provider with the private key of the Titular.
2. The electronic application with the public key that is generated by the Applicant for issuing of a QCQES should be signed with the private key that corresponds to the public key in the application. The electronic application must be in a format that allows the Provider - via the RA/LRA - to verify the content of the private key.
3. Online applications for the administration of certificates should be signed by the Applicant 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 holding the key, depending on the type of certificate requested and following the applicable Policy.
5. The key pair corresponding to the QCQES issued by the Provider shall be generated on a QSCD.
6. Control of access to the private key shall only be held by the Titular.

3.2.2 Establishing the Identity of a Legal Entity or a Sole Proprietor

1. Identification and verification of a legal entity or a sole proprietor is performed by the RA/LRA of the Provider under the respective Policy for issuing of a certificate and other internal documents of the Provider.
2. Verifying the identity of a legal entity or a sole proprietor of a professional QCQES "B-Trust Professional Qualified Certificate QES" requires an official representative of the entity to appear before the RA/LRA and provide the required documents proving his/her legal status.

3.2.3 Establishing the Identity of an Individual

1. Identification and verification of the identity of an individual as a Titular or representative of another entity, as well as their empowerment, are carried out by the RA/LRA of the Provider by following the procedural rules and steps set out in the relevant Policy and other internal documents of the Provider.
2. Identification of an individual requires this person or his/her authorized representative to present before the RA/LRA the following documents:

Type of Certificate	Required Documents
Personal QCQES "B-Trust Personal Qualified Certificate QES"	Documents proving the Titular's identity – in case Titular is personally presented. Documents proving the Authorized person's identity and a power of attorney - in case Authorized person is presented
Professional QCQES "B-Trust Professional Qualified Certificate QES"	Documents proving the identity of the Titular and the legal entity , as well as the representative power of the Titular to the legal entity.

3.2.4 Special Attributes

1. The Provider may include in the certificate to be issued specific attributes associated with the Titular, 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 Unconfirmed Information

1. Unconfirmed information is any information beyond the scope of the statutory information subject to verification that should be included in the certificate.
2. The Provider may include unconfirmed information about the Titular in the certificate to be issued, and it shall not be subject to review by the RA/LRA.
3. The Provider shall bear no responsibility for any unverified information included in the certificate.

3.3 Identification and Authentication of Identity upon Renewal

1. The Provider may renew a valid QCQES which is not terminated within the period of its validity in two ways:
   - by renewing the key pair generated for the current certificate (Renew);
   - by generating a new key pair (Re-key).
2. A certificate is renewed for the same pair of asymmetric keys (Renew) of the current QCQES 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.
3. Provider allows multiple renewals of a QCQES, while maintaining the current key pair (Renew), but recommends this practice to be limited in order to reduce the risk of compromising the private key.
4. The Provider will renew the current QCQES with a new key pair (Re-key), only if the Titular 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.
5. After renewal, the current certificate shall not be terminated and remains valid for its period of validity.
6. The identification and authentication of the identity of the Titular of the certificate being renewed does not require him/her to be present in person before the RA/LRA of the Provider.
7. Upon changes in the information about the Titular of the QCQES, the current certificate is not renewed. The Provider shall issue a new QCQES, following the initial identification and authentication of the Titular, and shall immediately terminate the current certificate.
8. 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.
9. The Provider shall observe the following time limits and requirements for identification when renewing a QCQES:

Time interval	Renewal	Requirement
Not later than 30 days before the expiry of a certificate that is not terminated, if there is no change in the information contained therein	- via Renew - via Re-key	1. No change in the "DN" of the certificate 2. The certificate has been issued on QSCD 3. The application for renewal may be submitted remotely
Not later than 30 days after the expiry of a certificate that is not terminated, if there is no change in the information contained therein	- via Renew - via Re-key	1. No change in the "DN" of the certificate 2. The certificate has been issued on QSCD 3. The application for renewal shall be submitted 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 upon Suspension

1. Provider, via the RA/LRA, shall suspend a valid certificate upon request, but for not more than 24 hours.
2. Provider, via the RA /LRA, shall not perform identification and authentication of the Applicant and shall immediately suspend the certificate.

3. Provider, via the RA/LRA, shall resume operation of a suspended certificate in accordance with Art. 26, para. 6 EDESA.

3.5 Identification and Authentication upon Revocation

1. Provider, via the RA/LRA, shall terminate a valid certificate upon request for revocation, in accordance with Art. 27 EDESA.
2. Provider, via the RA/LRA, shall immediately suspend the certificate and perform subsequent identification and authentication of the Applicant.
3. Provider, via 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. Provider, via the RA/LRA, shall terminate the certificate only after successful identification and authentication of the Applicant and verified reason for revocation. Otherwise, the certificate shall be renewed.

3.6 Identification and Authentication after Revocation

1. Renewal of a certificate by "Renew" or "Re-key" after its revocation is not allowed.
2. Titular of a terminated certificate may request a new certificate.
3. Provider, via the RA/LRA, shall perform initial identification and authentication of the Titular, if the latter applies for a new certificate.

4 OPERATIONAL REQUIREMENTS AND PROCEDURES

1. Provider, via RA/LRA, within the contract for QCS, shall provide the following operational procedures for QCS applicable to QCQES:
   - registration of an application for issuing of QCQES;
   - processing of an application for issuing;
   - issuing of a QCQES;
   - delivery of issued QCQES;
   - use of the key pair and QCQES;
   - renewal of a QCQES via "Renew";
   - renewal of a QCQES via "Re-key";
   - suspend/resume operation of a QCQES;
   - revocation of a QCQES;
   - current status of a QCQES.
2. Provider, via RA/LRA, shall give an option to the Titular to terminate the Contract for certification services between them.

4.1 Application for Issuing of Certificate

1. Issuing of a certificate shall be preceded by registration of request by the Applicant before the RA/LRA of the Provider.
2. Application for issuing of a certificate may be filed in person by the Titular, or by an authorized person.
3. The applicant shall register the application for certificate online or through an operator at the RA/LRA of the Provider.
4. 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 Process of Application

1. Application for issuance shall include all information required under Art. 24 EDESA, about the Titular and the type of certificate to be issued. The application may include additional, unverified information, part of which is certified and other part is used to facilitate contact of the Provider with the entity.
2. The process of application allows the operator of the RA/LRA or the Titular to generate the pair of cryptographic keys and to include the public key in the information required for issuing of certificate.
3. The pair of cryptographic keys for issuing a QCQES must be generated in a QSCD that conforms to the security level required for creation of the signature.
4. 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.
5. Where necessary, the RA/LRA shall provide the Titular or an authorized person with protected information/access code to the private key.
6. If the applicant does not have a QSCD, when submitting an application for issuing of a certificate before the RA/LRA of the Provider, he/she needs to only enter information required to identify the Titular, and such other information as necessary, without generating a cryptographic key pair for the requested certificate.
7. Communications between Users and protected Internet websites of the Provider shall be based on the HTTPS protocol.
8. The approved requests for QCQES issuance and management shall be signed by the Provider.

4.2 Procedure of Issuance

4.2.1 Functions of Identification and Authentication

1. The RA/LRA shall perform identification and authentication of the Applicant for a certificate – Titular or his/her representative.
2. After initial identification and following established internal procedures of the Provider, based on an application for the issuance of certificate and other documents submitted, the RA/LRA shall check and verify before the Provider:
   - identity of the Titular or the authorized person;
   - representative power of the individual to the legal entity and of the authorized person;
   - checks authorization;
   - keeping of the private key corresponding to the public key;
   - additional information submitted for inclusion in the certificate, and admissible unverified information;
   - sign a contract for certification services and consent with the terms of this CPS.
3. If the key pair is generated with the Titular, the RA/LRA should check the electronic application and requirements for the security level of QSCD.

4.2.2 Confirmation or Rejection of a Request for Issuance

1. After successful checks, an authorized operator of the RA/LRA shall approve the application for a certificate before the Provider.
2. RA/LRA shall reject the application for certificate if the validation fails.
3. 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. RA/LRA shall properly store and archive documents submitted and the confirmed electronic application for a certificate.
6. RA/LRA shall control and approve before the Provider the correctness and accuracy of the information included in the certificate only at the time of issue.
7. The Titular of a QCQES shall immediately inform the Provider of any changes to verified information occurring after issuance.

4.2.3 Time Limit for Processing an Application for Certificate

1. RA/LRA of the Provider shall immediately, in the presence of the Applicant – Titular or authorized person, perform all checking operations, after the Applicant has submitted the necessary documents, and shall approve the information submitted with the application for the issuing of certificate.
2. CA of the Provider shall issue the certificate immediately after approval of the electronic application for issuing by the RA/LRA.

4.3 Issuing of a Certificate

4.3.1 Operation of the Certification Authority

1. CA of the Provider shall identify by electronic means the RA/LRA that has approved the electronic application for issuing of a QCQES.
2. CA shall generate the QCQES in accordance with the selected profile, sign it with the Provider's electronic signature and shall promptly publish it in its Public Register.

4.3.2 Notification of the Titular of the Certificate by the Provider

1. Provider, via the Office for Notification of Users of QCS, shall immediately notify the Titular of a certificate issued and published.
2. Office for Notification shall send to the Titular an e-mail with information about the QCQES issued, the unique serial number of the certificate and its validity period, except in cases where no email address has been specified.

3. Provider shall deliver the certificate issued to the Titular or, respectively, to the authorized person, via the RA /LRA.
4. An authorized operator of the RA/LRA shall record the certificate on the QSCD where the cryptographic key pair for this certificate has been generated, when possible.

4.4 Adoption and Publication of the Certificate

1. Provider, via the operational CA, shall promptly publish the certificate issued in the Public Register of certificates issued.
2. Titular 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 Titular in the above period, it shall be deemed that the certificate is accepted.

4.5 Use of the Key Pair and Certificate

4.5.1 By the Titular

1. The private key corresponding to the certified public key shall be controlled by the Titular. Responsibility for using the private key lies with the Titular.
2. The Titular 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 within the validity period of the certificate;
   - for checking an affixed qualified electronic signature;
   - until the certificate is revoked;
   - where the certificate is suspended, shall not use the private key, particularly for creating a qualified electronic signature;
   - as per the Contract for certification services with the Provider.

4.5.2 By the Relying Party

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

4.6 Renewal of a Certificate

1. Renewal of a QCQES shall retain information of the current certificate; the period of validity in the renewed certificate shall be changed.
2. Renewal of a QCQES, which was not terminated during its period of validity can be performed in two ways:
   - by retaining the key pair generated for the current certificate (Renew);
   - by generating a new key pair (Re-key).
3. Renewal of a QCQES shall be preceded by an application for renewal before the RA/LRA.
4. An application for renewal of a certificate shall be registered online, where the Titular has a valid QCQES that must be renewed.

5. When the certificate has expired and the application for renewal meets the time frames and requirements for identification upon renewal, the Titular or his/her representative must personally visit the RA/LRA of the Provider.
6. Titular or his/her authorized representative may renew a QCQES multiple times, subject to the conditions for renewal specified below.
7. Provider shall not permit the use of a key pair for a period greater than 3 (three) years.
8. Provider does not recommend repeated renewal of a QCQES via the "Renew" function, in order to reduce the risk of compromising the private key.
9. Provider recommends that Titular renew his/her certificate via the "Re-key" function.

4.6.1 Conditions for Renewal of a Certificate

1. RA /LRA will renew a QCQES via the "Renew" function, subject to the following conditions:
   - the certificate is not terminated during its period of validity;
   - the Titular or his/her authorized representative should declare that no change in the information contained in its current certificate has occurred;
   - an application for renewal has been filed 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 QCQES via "Re-key", subject to the following conditions:
   - the certificate is not terminated during its period of validity;
   - Titular or his/her authorized representative should declare that no change in the information contained in its current certificate has occurred;
   - an application for renewal has been filed 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 Titular of the current certificate has occurred, the latter shall not be renewed, and the Provider shall issue a new certificate.

4.6.2 Who May Apply for Renewal of a Certificate?

1. Titular or his/her authorized representative may file application for renewal of the certificate subject to the time limitations, requirements and conditions for renewal.

4.6.3 Procedure for Renewal of a Certificate

1. Renewal of a QCQES is preceded by the registration of an application for renewal before the RA/LRA of the Provider.
2. An application for renewal of a certificate by electronic application shall be certified by QES.

   If the certificate being renewed has expired, the Titular 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 fulfil the confirmed application 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 file application for a new QCQES.

4.6.4 Notification of the Titular upon Renewal of the Certificate

1. Provider, via the Office for Notification of Users of certification services, shall immediately notify the Titular of the renewed and published certificate.
2. Office for Notification shall send to the Titular an email notification containing information about the issued QCQES, unique serial number and validity period of the renewed certificate and the address (URL) which can be used to deliver the renewed certificate.
3. When the Applicant for renewal of a certificate visits the RA/LRA, the Titular 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.

4.6.5 Publication of the Renewed Certificate

1. Provider, via the operational CA, shall immediately publish a renewed certificate in the Public Register.

4.7 Replacement of a Cryptographic Key Pair in a Certificate

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

4.8 Change in a Certificate

1. Provider shall allow changes in the content of information in an issued and published QCQES only subject to the requirements and conditions for issuing a new certificate.
2. Provider shall not allow a change in the profile of QCQES, as specified in Part II of this document.
3. Provider does not offer service "Certificate Modification".

4.9 Revocation and Suspension of a Certificate

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 QCQES, the effect of any certificates issued by this Authority that are still valid shall be terminated.
3. Only the operational CA that has issued the certificate may suspend 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 the hold and revoked certificates 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: +359 2 97 13 461.
6. In case of failure of the system, 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 of a Certificate

1. The Provider shall terminate a QCQES issued by them upon:
   - death or disability of the Titular with revocation of the legal entity of the Titular;
   - revocation of the representative power of the Titular to the legal entity;
   - incorrect data provided upon issuing the certificate;
   - certified information that has subsequently become untrue;
   - change in already certified information of the Titular;
   - compromising the private key;
   - delay in payment of outstanding remuneration;

- application for revocation filed by the Titular, after verifying their identity and representative power of the Titular.

2. Provider shall immediately suspend the QCQES in each of the above circumstances.
3. Provider shall terminate all certificates they have issued, in case of terminating their activity without transferring it to another provider.
4. Provider may suspend and terminate a certificate of CA from its infrastructure upon reasonable doubts that the private key of this authority has been compromised.

4.9.2 Procedure for Revocation of a Certificate

1. Revocation of the certificate shall be 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 Titular has (another) certificate valid and accessible for use. Otherwise, the application shall be made before 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 Titular.
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 Titular or his/her representative must personally visit the RA/LRA of the Provider for verification of the identity, respectively the Applicant's identity.
6. The RA/LRA shall strictly follow the requirements for identification and authentication of the Applicant and the reasons for revocation.
7. Upon successful electronic authentication by the RA/LRA via an authorized operator, the operational CA shall fulfil the application for revocation of 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 Applicant of the reasons.
9. A rejected Applicant for revocation of certificate may submit a new application for revocation of the certificate after they have removed the reasons for refusal.
10. Upon revocation of the certificate, the Provider, via its operational CA, shall immediately publish the terminated certificate in the CRL, and shall issue a new CRL.
11. Upon revocation of the certificate, the Provider, via the Office for Notification, shall immediately inform the Titular of the terminated certificate.
12. Terminated certificate of a Titular is not subject to resumption or renewal.
13. Authorized persons from the personnel of the Provider shall 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 of the Certificate

1. Prior to terminating a valid QCQES, 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 Applicant and the reasons for revocation.
3. Upon failure of validation, or after the end of the grace period, the Provider shall resume the certificate.
4. The Provider shall resume the certificate upon application of the Titular or his/her representative before the expiry of the grace period.

4.9.4 Timeframe During Which a Certification Authority Must Satisfy an Application for Revocation

1. The Provider shall satisfy an application 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 Requirements for Relying Parties to Check a Terminated Certificate

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

4.9.6 Frequency of Publication of an Updated List of Terminated Certificates

1. Provider, through its operational CA, shall immediately publish a new updated CRL, every time a valid QCQES 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 Publication of an Updated List of Terminated Certificates

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

4.9.8 Ability to Check the Status of a Certificate in Real Time

1. Provider shall provide real-time online verification of the status of QC issued, by using the OCSP protocol.

4.9.9 Requirements for Using the OCSP

1. Real time checks of the status of a QCQES (using the OCSP protocol) requires 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 QCQES (using the OCSP protocol) can be made via the Provider's website.

4.9.10 Conditions for Suspension of a Certificate

1. Provider, through its operational CA, shall suspend a valid QCQES under certain conditions and for a period of up to 24 hours.
2. Provider shall take immediate action on an application for the 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 shall be void (invalid).

4.9.11 Who May Apply for Suspension of a Certificate?

1. Provider shall suspend a validly issued certificate, upon:
   - application of the Titular or his/her representative, without being obliged to verify their identity, or representative authority of the latter;
   - application of a person who, under the circumstances, could be aware of any breaches of the private key as an agent, partner, employee, etc.;
   - receives a 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 EDESA.

4.9.12 Procedure for Suspension of a Certificate

1. Suspension of the certificate shall be preceded by registration of an application for suspension before the RA/LRA.
2. The application 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 application shall be certified by QES.

4. The authorized operator at a RA/LRA shall immediately suspend the certificate, without identifying the Applicant. Suspension of the certificate shall be performed by its temporary inclusion in the Certificate Revocation List, as per Art. 26, Para. 5 EDESA.
5. Upon successful electronic authentication by the RA/LRA via an authorized operator, the operational CA shall fulfil the application for suspension of the certificate.
6. RA/LRA may not refuse to suspend a certificate.
7. Upon revocation of the certificate, the Provider, via its operational CA, shall immediately publish the terminated certificate in the CRL, and shall issue a new CRL.
2. Upon revocation of the certificate, the Provider, via its Office for Notification, shall immediately inform the Titular of the terminated certificate.

4.9.13 Limitation of the Period of Suspension of a Certificate

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

4.9.14 Resuming the Operation of a Suspended Certificate

1. Provider shall resume operation of a suspended QCQES:
   - up to 24 hours after its suspension;
   - after the end of the period of suspension (24 hours), if not application for resuming has been received;
   - after the end of all reasons for suspension, before expiry of the period of suspension;
   - at the application of the Titular, after the Provider, respectively CRC, ensures that the former was made aware of the reason for suspension and that the application for renewal is made as a consequence of this.
2. After resuming the operation of a certificate, it shall be deemed valid.

4.9.15 Procedure for Resuming the Operation of a Certificate

1. RA/LRA shall resume a suspended QCQES after receiving an application for resumption by the Titular and upon successful verification.
2. RA/LRA shall resume a suspended certificate after receiving a written order of the CRC, or the Chairman of the CRC, to resume the certificate.
3. RA/LRA shall immediately resume a suspended certificate at the end of the period of suspension (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 Status of a Certificate

1. All valid QCQES, issued by the Provider shall be published in the Public Register.
2. Any certificates 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 terminated 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 OCSO 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 a Contract for Certification Services

1. A contract for certification 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 Recovery of keys

1. The Provider does not offer the service Key Escrow and Key Recovery.

5 FACILITIES, MANAGEMENT AND OPERATIONAL CONTROL

5.1 Physical Control

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:
   - Root CA "B-Trust Root Qualified CA";
   - Operational CA "B-Trust Operational Qualified CA";
   - Registration Authority;
   - Public Register;
   - B-Trust Qualified Time Stamp Authority;
   - OCSP server "B-Trust Root Qualified OCSP Authority";
   - OCSP server "B-Trust Qualified 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 Premises and Construction of Premises

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 shall be controlled by access control systems, video surveillance, alarm systems, etc.
2. Physical access control systems shall be periodically inspected and keep all necessary logs.
3. Authorized staff of the Provider shall 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 shall be personified in the access control systems for the premises and strict verification is required.

5.1.3 Power Supply and Climatic Conditions

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 Flooding

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

5.1.5 Fire Prevention and Fire Protection

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

5.1.6 Storage of Data Media

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 shall be observed and after its end, they shall be removed from use.

5.1.8 Duplication of Technical Components

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

5.2 Procedure Control

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

5.2.1 Job Positions and Activities

1. The Provider shall maintain qualified staff on positions to perform duties at any time related to the issue, maintenance and management of QCQES, in accordance with applicable regulations.
2. The Provider shall operate using trier own staff.
3. For certain activities under Art. 5 OACSP, the Provider may hire external stuff.

5.2.2 Number of Employees for a Specific Task

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

5.2.3 Job Descriptions

1. The Provider shall develop job descriptions for each of the positions of personnel performing activities.
2. The positions of Provider's personnel include activities such as:
   - generating and maintaining the infrastructure of the public key of the certification service provider;
   - administration of systems and ensuring their security;
   - creating and managing QCQES, including creation of a key pair - public and private for a QCQES;
   - data storage and archiving.

5.2.4 Requirements for Division of Responsibility

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

5.3 Qualification and Training of Staff

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 shall undergo initial and further vocational 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 shall prepare and update internal instructions for operation, and shall provide these to staff for the purpose of self-study and training at work.

5.4 Preparing and Keeping Records

5.4.1 Records of Important Events

1. The Provider shall keep logs created by the computers’ operating systems in B-Trust infrastructure, as follows:
   - 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 shall kepp 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";
   - 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;
   - publishing valid certificates issued in the Public Register;
   - configuration of certificates profiles;
   - real time certificate status checks;
   - issuing qualified electronic time stamp token of provided content.
3. Access to information contained in logs shall be restricted only to authorized staff, responsible for systems support.
4. The Provider shall keep 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. Shall store records created by communication components of the infrastructure.
6. Shall store records 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 shall be generated automatically.
2. Records and logs shall be periodically analyzed by authorized employees of the Provider.

5.4.3 Period of Storage of Records

1. Records shall be kept for a period of 1 (one) year.

5.4.4 Protection of Records

1. Information from records in the logs shall be 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 shall have access and use these records and logs.

5.4.5 Maintenance of Backup Copies

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

5.4.6 Notification Following an Analysis of Log Entries

1. Log entries shall be 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 Archive and its Maintenance

1. Information about significant events shall be 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 shall be archived on paper or on electronic media.
3. The Provider shall kepp records in a format allowing for reproduction and recovery.

5.5.1 Types of Records

1. The Provider shall maintain paper and electronic records.

5.5.2 Period of Storage

1. The archive shall be stored for a period of 10 (ten) years.

5.5.3 Protection of Archived Information

1. Security of records shall be ensured, as follows:
   - backup files in electronic form shall be signed electronically;
   - specific events and data that are recorded in the archive shall be 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 shall sign electronically all certificates and lists of revoked and suspended certificates;
   - only authorized systems maintenance personnel shall work with the protected archived information;
   - electronic communications between local components of infrastructure shall be protected in conformity with the PKIX standard;
   - remote electronic communications shall be protected and based on the PKIX standard;
2. The Provider shall assure the appropriateness of use of postal and courier services and fax communications with Users.

5.5.4 Restoration of Archived Information

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

5.5.5 Requirement to Certify the Date and Hour

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

5.5.6 Storage of the Archive

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

5.5.7 Acquisition and Verification of Information from the Archive

1. Public archive information of the Provider shall be published and shall be 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 shall be only available to Applicants, or to persons duly authorized by the latter.
2. This CPS, Policies and the Contract for certification services shall be publicly available in the Provider's register of documents and may be obtained and downloaded from the website of the Provider.
3. The Provider shall ensure that information on public archives is in readable form.

5.6 Change of Key

1. The Provider may change the key corresponding to an issued QCQES only by issuing a new certificate, or by renewing a current certificate with the "Re-Key" function.

5.7 Compromise of Keys and Recovery after Accidents

1. The Provider shall take due care to maintain continuity and integrity of the certification services related to all certificates issued, maintained and managed by the Provider.
2. The Provider shall take 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 Titulars, 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 message on the Provider's official website.

5.8 Compromise of a Private Key

5.8.1 Of a Certification Authority

1. The Provider shall take the following actions upon compromise of the private key an operational CA:
   - immediately terminate 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 an Author

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

5.9 Termination of the Activities of the Provider

1. Activities of the Provider shall be terminated under OACSP.
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 Provider;
   - inform Users about the conditions of maintenance of certificates transferred to the successor Provider;
   - The QSCP 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 MANAGEMENT AND CONTROL OF TECHNICAL SECURITY

6.1 Generation and Installation of a Key Pair

1. Cryptographic key pairs for official certificates of the Provider shall be 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 his/her infrastructure;
   - to sign the CRL issued and published;
   - to sign all QCQES issued and published to Users.
3. The cryptographic (RSA) key pairs of QCQES issued in the infrastructure of the Provider shall be generated, as follows:
   - by the Titular - using hardware and software that is under their control;
   - by the RA/LRA of the Provider - using hardware and software that is under the control of the Provider.
4. The generation of a key pair to a QES certificate always shall use SSCD, with a protected account under the regulations of EDESA.
5. The Provider may, on the basis of a contractual relationship, provide Titulars 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 are QCQES.
7. The Titular shall use only licensed software for operation with QCQES and QSCD.

6.2 Generation Procedure

6.2.1 Generating cryptographic keys to a Certification Authority of the Provider

1. The Provider shall generate 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" and "B-Trust Operational Qualified 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 Public.
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 shall be 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 shall be 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 these keys to be compromised and/or reproduced without authorization of the Provider.

6.2.2 Generating cryptographic keys to a Titular

1. The key pair of a Titular of a QCQES shall be generated by the use of specialized software that is entirely under the control of the Provider.

2. When the key pair of a Titular of a QCQES is generated by the Provider, he/she uses specialized licensed software verified for successful operation through the interfaces of the B -Trust infrastructure.
3. The key pair of a Titular of a QCQES shall be generated in a QSCD approved by the Provider with verified security level. When the key pair is generated at the Provider, B-Trust QSCD is always used. The private key of the generated key pair can not be acquired from the QSCD.
4. The private key shall be 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.
5. When a key pair is generated with the Titular, the Provider shall advise the latter to use an approved solution in the B-Trust infrastructure, or equivalent.
6. For the purposes of using QES the Provider shall recommend the User to use a B-Trust QSCD or other QSCD compatible with B-Trust infrastructure.

6.2.3 Delivery of a Private Key

1. When the key pair is generated with the Provider, the Titular or explicitly authorized by them person shall receive the private key and the certificate issued at the RA/LRA of the Provider.
2. When issuing a QCQES the private key and the issued certificate shall be 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.
3. The Titular is obliged to change the initial access code and enter their own code.
4. When the Titular generates the key pair by themselves, they have the full responsibility for guaranteeing the holding of the private key.
5. When the Titular generates the key pair for the QCQES by themselves, they declare to the Provider that the key pair fully meets the requirements for a QES in accordance with the Regulation.

6.2.4 Delivery of Public Key at the Provider

1. This is performed only by the Titular who generates their own key pair and who should deliver such public key to the Provider for the needs of the process of issuing the certificate.
2. The Titular supplies through the RA/LRA of the Provider the public key of the generated key pair.
3. The Titular may submit an application form on electronic media in person at the RA/LRA, along with other documents in accordance with the Provider's Policy, through the website of the Provider or in any other appropriate manner.
4. The RA/LRA of the Provider shall check whether the Titular is holding the private key.

6.2.5 Delivery of the Provider's Public Key to Relying Parties

1. Provider's public keys shall be publicly accessible on the Provider's webpage, where their official certificates are published.
2. Each Relying Party builds trust towards the Provider, by accepting and loading official certificates of the Provider into systems under its control.

6.2.6 Length of Keys

1. The length of the root RSA-key of the Provider shall be 4096 bits.
2. The length of the RSA-key pair of the operational CA "B-Trust Operational Qualified CA" shall be 4096 bits.
3. The length of the RSA-key pair of the operational authorities "B-Trust Root Qualified OCSP Authority" and "B-Trust Qualified OCSP Authority" shall be not less than 2048 bits.
4. The length of the key pair (RSA) for QES of a Titular generated by infrastructure of the Provider shall be at least 2048 bits.
5. The length of the key pair (RSA) for QES of a Titular generated outside the Provider's infrastructure shall be at least 2048 bits.

6. Regardless of where the key pair for issuing a QCQES shall be generated, the key must have a length of at least 1024 bits for RSA algorithms.

6.2.7 Parameters of a Public Key

1. The parameters of a public key shall be listed and certified in the certificate issued by the Provider for that public key, corresponding to the private key.

6.2.8 Key Usage

1. Parameters for using the key pair, respectively, the private key, shall be contained in the certificate issued by the Provider via the attributes "keyUsage" and "extended keyUsage".

6.3 Protection of a Private Key and Control of the Cryptographic Module

6.3.1 Standards

1. The main components in the infrastructure of B-Trust "B-Trust Root Qualified CA" and "B-Trust Operational Qualified CA" shall use a HSM, certified for security level FIPS 140-2 Level 3 (respectively CC EAL 4+ or higher), which meets all regulatory requirements.
2. B-Trust QSCD, where the private key of the Titular is generated and stored, shall have a security level of CC EAL 4+ /FIPS 140-1 Level 2.
3. 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 a level of security CC EAL 4 and higher equivalent.

6.3.2 Control of Use and Storage of a Private Key

1. Private keys of the CA of the Provider shall be used in HSM only and shall be available via access codes divided into several parts, kept by 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 shall be performed, in accordance with established internal procedures.
3. The private key of the Titular shall be used in B-Trust QSCD only or in QSCD with equivalent security level, and shall be accessible via a personal access code. Along with generating the key pair, the private key shall be stored in the QSCD.

6.3.3 Storage and Backup of the Private Key

1. Private keys of the CA shall be separately stored on separate QSCDs with protection profile CC EAL 4+ or higher, and access to any QSCD shall be controlled by an access code held by an authorized person of the Provider's staff.
2. The access code to any QSCD shall be personal for each authorized person of the Provider's staff.
3. Separate storage of private keys of CA on several QSCDs and private control of access to these QSCDs shall 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 a QCQES of a Titular shall be stored on QSCD only and may not be reproduced on another QSCD.
6. Upon failure of a SSCD, the User must replace it and apply for a new certificate.

6.3.4 Transfer of a Private Key to and from a Cryptographic Module

1. Transfer of a private key of a Certification Authority of the Provider from the cryptosystem (HSM) to a backup system 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 an Author/Holder to and from the Provider in another SSCD for the purposes of storage and recovery shall not supported.

3. The private key of the Author/Holder shall be stored only in the SSCD where the key pair is generated and can not be transferred/replicated to another SSCD.
4. The Provider shall not in any way store or archive a private key of a Titular for issuing QES, regardless of where the key pair is generated.

6.3.5 Method of Activation of the Private Key

1. A private key of the Provider shall be 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, shall access to the slot in the HSM be permitted and the private key shall be activated.
3. A private key of a Titular shall be activated by entering the user access code where the key is stored, or other means of identification is used.

6.3.6 Method of De-activation of the Private Key

1. A private key of the Provider in the cryptosystem of the CA is deactivated (the possibility to use/access) the private key is suspended by suspension of logical access to the appropriate key contained therein.
2. A private key of the Titular shall be deactivated (the possibility to use/access the private key is suspended) by terminating the logical access to the location where the key is stored.

6.3.7 Destruction of a Private Key

1. A private key of the Provider in the cryptosystem of the CA shall be 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 QCQES of a Titular shall be destroyed by deletion from the location where the key is stored securely.
3. A private key of QCQES of a Titular shall be destroyed by deletion from the QSCD or by complete deletion/initialization/destruction of the QSCD.

6.4 Other Aspects of Key Pair Management

6.4.1 Backing up the Public Key

1. Public keys of CA shall be contained in official certificates of the Provider and stored in an internal register. These shall be publicly available through publication of certificates of the Provider.
2. Public keys of CA shall be archived and stored for 10 years after the period of validity or termination of the respective certificates.
3. Public keys of Titulars shall be contained in certificates issued to them, which were published in the Public Register and stored in an internal register.
4. Public keys of Titulars shall be stored and maintained by periodical archiving in the internal register.

6.4.2 Validity Period of Certificates and Use of a Key Pair

1. QCQES shall have the following validity periods:
   - of the root CA "B-Trust Root Qualified CA" - 20 (twenty) years;
   - of the operational CA "B-Trust Operational Qualified CA" - 15 (fifteen) years;
   - of a Titular – as per the contract between the Provider and the Titular, but not more than 3 (three) years.
2. When the key is used for signing after the period of validity of the certificate has expired, the signature shall be invalid and the signed statement or object should be considered void.
3. Six months before the expiration of the validity of the CA the Provider shall generate a new key pair and shall apply 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 shall be generated and its public part shall be 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 for QCQES by the Titular, they create and manage the activation data.
2. When generating a key pair for QCQES of the Titular by the Provider, the latter shall provide, together with the private key, the control of the activation data to the Titular.
3. Upon initial issuance of a certificate on a B-Trust QSCD, before generating a key pair, the B-Trust QSCD shall be initialized and the following access/activation codes shall be created: User ("User") and Administrative ("SO") respectively, for access to the personal private key in QSCD and to unblock a blocked QSCD.
4. Initial User and Administrative access code and code to unlock the B-Trust QSCD shall be provided to the Titular or his/her authorized representative in a sealed, non-transparent paper envelope.
5. The Titular must change the initial User access code through the software that comes with the B-Trust QSCD.
6. The Provider shall recommend the Titular to periodically change their user code to access the QSCD.
7. The Titular must use the Administrative access code to unblock a blocked B-Trust QSCD.

6.5.2 Protection of Activation Data

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

6.5.3 Other aspects of Activation Data

1. After a number of unsuccessful attempts to enter the correct code to access the private key of a Titular, the B-Trust QSCD shall be blocked.
2. The Titular must use the provided Administrative access code to unblock a blocked B-Trust QSCD.

6.6 Security of Computer Systems

6.6.1 Security Requirements

1. Computer platforms operating all critical components of the B-Trust infrastructure shall be equipped and configured with a means of local protection of access to software and information.
2. The Provider shall use 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. Reliability of systems, and of technical and cryptographic security of the processes they perform, shall provided by tests and checks of technical equipment and technology under the methodology for security assessment.
4. Inspections and tests shall be carried out periodically, and after any changes that affect the security infrastructure.

6.6.2 Level of Security

1. The degree of security of systems used in the infrastructure of B-Trust meets the legal requirements for implementing the activities of the Provider and shall be 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 certification services related to certificates issued and maintained by the Provider shall be performed on separate systems, completely independent of those in regular operation.

2. Products, software and services offered by the Provider shall be initially tested on development systems, before being put into operation.
3. New products and certification services offered by the Provider shall be accompanied by operational procedures and instructions for use.

6.7.2 Operation

1. Certification services and products put into operation by the Provider shall be maintained by dedicated separate operating computer systems.
2. The Provider shall provide all certification services through its operational systems.
3. Products and services of the Provider shall be tested in real working conditions.

6.8 Additional tests

1. The Provider shall provide the ability to perform tests for operation of the issued Qualified Certificates for Qualified Electronic Signature on its official website.

6.9 Network Security

1. The Provider shall use modern 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 Verification of Time

1. The Provider shall publish in a separate document the Policy and Practice of the Qualified Electronic Time Stamps.

7 PROFILES OF QCQES, CRL AND OCSP

7.1 Profile of Qualified Certificates

1. The full content (profile) of QCQES shall be contained in the CPS, Part II: Policy to Provide QCQES and QCS.

7.1.1 Version Number

1. The Provider issues QCQES in a X.509, v3 format.
2. Version is recorded in the issued QCQES.

7.1.2 Extensions in the Form of a Certificate

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

7.1.3 Identifiers of the Algorithms of an Electronic Signature

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

7.1.4 Forms of Naming

See section "Naming" of this document.

7.1.5 Limitations of the Names

See section "Naming" of this document.

7.1.6 Policy Identifier

1. QCQES are issued in accordance with the Policy of the Provider that shall be recorded in the attribute "Certificate Policy" of the certificate.

7.1.7 Indication of a Qualified Certificate

1. The Provider uses in the QCQES with standard profile X.509 v.3 the attribute "Qualified Statements" with the 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).
2. The Provider uses in the QCQES with standard profile X.509 v.3 the attribute "Certificate Policy", to which the identifier (OID) is assigned as follow:

Qualified Certificate	Name	Identifier (OID) indicated in the attribute "Certificate Policy"
Personal QCQES to an individual	B-Trust Personal qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2
Professional QCQES to an individual	B-Trust Professional qualified certificate QES	O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 O.I.D. = 0.4.0.1456.1.1 O.I.D. = 0.4.0.194112.1.2

7.2 Profile of the Certificate Revocation List

7.2.1 Version

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

7.2.2 Format

1. The Provider issues, publishes and maintains a CRL, which format is in accordance with the international guidelines RFC 3280.
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. CRL's main attributes are:
   - "Version" – version number;
   - "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 issued and signed the List. It contains the meaning of "subjectKeyIdentifier" from the certificate of the CA that signs the CRL;

7.2.3 Format of an Element in CRL

1. The CRL of a CA shall contain elements for all certificates revoked by the CA. These elements are constant in the List.
2. The CRL of a CA shall contain an element for every certificate suspended by the CA. Such an element in the List is temporary until the renewal of the certificate.
3. Attributes of the elements in the CRL are:
   - "Serial number" - the serial number of revoked/suspended certificate;
   - "Revocation date" - the time of revocation/suspension of the certificate;
   - "CRL Reason Code" - code identifying the reason for revocation/suspension.
4. The meaning of the reasons for revocation/suspension of the certificate are as follows:
   - "keyCompromise" - compromised private key of the Titular;
   - "CACompromise" - compromised private key of an operational CA of the Provider;

- "affiliationChange" - changed status of the Titular to another entity - 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.

7.3 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 internationally recognized recommendation IETF RFC 6960.
2. Information for the request's profile and response when operating with the OCSP server shall be contained in the above technical recommendation, publicly available from the web site of IETF.

8 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

8.1 Periodic and Circumstantial Inspection

1. Control of the regulated legal activity of the Provider, associated with the electronic signature certificates and its compliance with the requirements of EDESA and the applicable regulations shall be carried out 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 be in compliance with the internal documents of the legal entity.
3. Management of the Provider shall perform continuous operational control for the proper performance of the operating instructions by the Provider's staff.
5. The management of „BORICA" AD shall appoint periodic checks for compliance of the current activity with the established Policy and Practice regulating the activities of the Provider.
6. The Provider shall perform constant control over the activity if the RA/LRA.

8.2 Qualifications of the Inspectors

1. Inspectors may be only persons authorized to perform such functions in accordance with the requirements of the accepted international practice and documents.
2. Inspectors shall comply with the requirements of Article 32, paragraph 2, item 4 of EDESA and Chapter Five of OACSP, or shall be accredited by an international accreditation organization to perform such checks.
3. Internal checks 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 checks, except with the explicit consent of the Provider.
5. Inspectors shall be held liable for the facts and circumstances they have checked, whether they have reassigned some or all of the checks to others with the consent of the Provider, or not.

8.3 Relationship of the Inspectors with the Provider

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

8.4 Scope of the Check

1. Check by the CRC shall cover the statutory requirements to the Provider's activity under EDESA.
2. Internal examination may cover every circumstance or activity referred to in this document, as well as:
   - comparison of practices and procedures specified in this CRS with their practical implementation upon execution of the Provider's activity;
   - checking the activities of subcontractors (external RA/LRAs;
   - other circumstances, facts and activities related to the B-Trust infrastructure, at the discretion of the Provider's Management.

8.5 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.

9 OTHER BUSINESS CONDITIONS AND LEGAL ASPECTS

9.1 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 unilaterally change the Tariff at any time during the term of Contract, and shall notify the Titular by posting the changes on the website.
3. Changes shall be effective for the Titular 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 Titular 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 shall be considered that the Titular agrees to the changes.
6. The change in fees may not affect fees already paid.

9.1.1 Fees

1. The value of the contract shall include one or more of the following fees:
   - fee for issuing and maintaining QCQES;
   - fee for renewal of QCQES;
   - fee for consultation and technical assistance provided at the request of the Titular;
   - price for equipment purchased or leased by the Provider;
   - fee for customizing a physical medium.
2. Outstanding fees and amounts shall be 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 use of services has been agreed, it shall not be refundable if the Titular has not used the service during the period covered by the advance or subscription fee.
4. The price does not include any amounts accrued by telecommunications companies in connection with their services used by the Titular in relation to services provided by the Provider. These shall be payable entirely by the Titular 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.

9.1.2 Fees for Certification, Cryptographic, Information and Consultancy Services

1. For the provision and use of QCQES and related services a fee shall be paid when ordering 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 time, prices shall be increased proportionately, as per the Tariff.
3. The "Issuing qualified electronic time stamps" service, upon a service level agreement (SLA, Service Level Agreement) 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 shall be payable as per the terms of contract. Legal relations between the Provider and the Titular shall be arranged as per the general rules of the Sale Contract or, respectively, the Lease Contract.

5. If payments are delayed after the agreed period, the Client shall pay to the Provider legal interest for the period until the final payment of amounts due.
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.

9.1.3 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 its 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 a 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 shall be paid by the User.

9.1.4 Return of Certificate and Recovery of Payment

1. A Titular can object to the inaccuracy or incompleteness in the content of a QCQES 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 terminate and issue a new certificate with the correct content at their own expense, or shall refund the amount for the terminated certificate containing such incorrect information.
3. If the incorrect content of a certificate is a fault of the Titular, 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 QCQES with correct content, and the Provider shall terminate it immediately, without refunding the payment for the terminated certificate.

9.1.5 Free Services

1. The Provider shall provide free registration and information services relating to the use of the Public Register, as follows:
   - checking a QCQES of a Titular published in the Register;
   - validity check of a certificate in the Public Register;
   - checking certificate status in real time;
   - 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.

9.2 Financial Responsibilities

9.2.1 Insurance of Activities

1. The Provider shall take compulsory insurance of its activities as a registered QTSP from the CRC;
2. Compulsory insurance shall be for a continuous period and shall be renewed periodically.
3. Subject of insurance is the Provider’s responsibility to carry out their activities in accordance with EDESA and OACSP.
4. The Provider have a compulsory insurance in the amounts referred to in Art. 14, para. 1 of OACSP:
5. The compulsory insurance shall cover the liability of the Provider to the Titulars, respectively Relying Parties for material and non-material damage suffered, to the limits specified in EDESA and OACSP.

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.

9.2.2 Insurance Coverage

1. Insurance coverage for any non-material and/or material damage suffered by a Titular shall not exceed the amount established by OACSP.
2. The insurance shall not cover cases of waiver of responsibility, in particular for damages caused by:
   - non-compliance of the Titular's obligations;
   - compromise or loss of private key of a Titular, as a result of improper care or use;
   - non-compliance with requirements to verify the validity of electronic signature and the certificate by the Relying Party;
   - force majeure and other circumstances beyond the control of the Provider.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

1. Information for Titular which is not included in issued certificates and CRLs constitutes personal data within the meaning of the Personal Data Protection Act (PDPA) and shall be considered confidential.
2. The information under the preceding paragraph shall be collected by the Provider 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.
4. The Provider may collect additional information that is also not included in the certificate, but is used for the purpose of maintaining quality certification services.
5. Confidential information shall be stored on site, access to such information shall be limited to personnel of the Provider authorized to operate with the data and shall be revealed with the explicit permission of the Titular, except where the Provider is obliged by Law.
6. No one except the Titular, including the Provider, may use the private key for creating an electronic signature. The Provider recommends the Titular not to expose the user access code to the private QCQES key, even if it is encrypted.
7. All private keys of staff and units in the Provider infrastructure shall be reliably protected against compromise and distribution.
8. Journal entries and logs from the system of the Provider shall be regarded as confidential information and shall be protected from unauthorized access and impact.

9.3.2 Non-Confidential Information

1. Any information contained in the Public Register in respect of certificates issued and published in the current CRL and archival copies of this list shall be publicly available.

9.3.3 Protection of Confidential Information

1. The Provider and the Titular are not allowed 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.

9.4 Privacy of Personal Data

1. The Provider shall be registered as an administrator of personal data under the PDPA.
2. As an Administrator of personal data, the Provider shall strictly comply with the requirements of confidentiality and non-disclosure of personal data of Titulars that has become known by the Provider in the performance of their business as a QTSP.
3. According to the approved policy of the QCQES, 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 option "prohibition of access" is checked in the application for issuance of a certificate.

4. In connection with Art. 22, item 4 of EDESA, the Provider shall publish each certificate issued and provide access to third parties, according to the Titular's instructions.

9.5 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. Relations on the occasion of these rights between the Provider and other participants in the B-Trust infrastructure, such as external RA, 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 Titulars and contained in the certificates, shall be retained by their Titulars and shall be used only for the purposes of certification 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.

9.6 Liability and Guarantees

9.6.1 Accountability and Guarantees of the Provider

1. The Provider is responsible and guarantees that shall comply strictly with the conditions contained herein, and with the requirements of EDESA and regulations on the activities of registered QTSPs.
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 QCQES after verifying the submitted information by means permitted by Law;
   - storing and maintaining information relating to the issued certificates and operation of 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 a QCQES;
   - performing revocation and suspension of certificates under the terms and conditions of the respective Policy;
   - immediately notifying the Titular 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 QCQES upon its expiration;

- informing Titulars and third Relying Parties of their obligations and due diligence in the use and reliance on the certification services of the Provider, as well as of the proper and safe use of certificates issued and of certification services related thereto;
- using and storing personal and other data for the purposes of its activities on providing certification services under EDESA 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 EDESA, in compliance with the Insurance Policy;
- employing personnel with the necessary expertise, experience and qualifications to perform the activity;
- maintaining a Register to publish issued QCQES, an updated CRL and other circumstances and electronic documents, in accordance with this document and EDESA;
- providing 24/7 electronic access to the Registry;
- providing protection against any unauthorized changes to the Register, as a result of unregulated and unauthorized access or by accident;
- immediately publishing certificates issued and signed in the Public Register of QCQES;
- creating conditions for each Relying Party to check the status of a certificate issued and published in the Public Register of certificates.

3. The Provider shall be responsible to the Titular 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.

9.6.2 Responsibility and Guarantees of the RA/LRA

1. The Provider shall ensure that RA/LRA perform its 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.

9.6.3 Responsibility of the Titular

1. The Titular shall:
   - follow precisely the conditions and procedures of this document and the relevant Policy upon request for issuance of certificate and use of other certification services;
   - pay the due fee 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 hardware and software), when generating the key pair outside the infrastructure of the Provider with a view to preserving the confidentiality of the private key;
   - use algorithms in accordance with the requirements of ORQESA 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 CPS. Any use of the private key shall be considered as an act committed by the Titular;

- 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 any discrepancies between the information provided under the contract and the certificate, he/she shall immediately notify the Provider;
- notify a change in the certified information and request for revocation of the certificate;
- notify the Provider of any change in information that is not included in their issued certificate, 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 certificates issued using licensed cryptographic software only;
- use a certificate only in accordance with its intended purpose and in accordance with applicable policies and restrictions under which it is issued;
- not use the private key to create a digital signature after the expiry of the certificate or after suspension or revocation thereof;
- inform each Relying Party of the care and responsibility required from the latter when relying the QCQES;
- accept the conditions of care and responsibility when relying the QCQES, in the event that they act as a Relying Party.

2. The Titular shall be held liable if they have accepted a certificate issued by the Provider based on false data submitted by them, respectively, based on suppressed or missing data.
3. The Provider shall regress to the Titular 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 latter has used an algorithm that does not meet the requirements of ORQESA;
   - fails to meet 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 Titular was not authorized to hold the private key corresponding to the public key in the certificate;
   - has accepted the certificate being issued by making false statements to the Provider relating to the certificate;
   - has accepted the certificate when the Titular was not authorized to apply for the issuance of the certificate.

9.6.4 Care and Responsibility of the Relying Party

1. Persons who rely on QCQES shall have basic knowledge of the principles of use and applicability of electronic signatures and services related to the use of electronic signature certificates.
2. A Relying Party shall take reasonable care, by:
   - trusting certificates only in terms of the Policy on their purpose and the limitations and conditions under which they were issued;
   - verifying the status of the certificate maintained in the Public Register by the Provider. Electronic verification of authenticity and integrity of the certificate outside the Public Registry or in an outdated CRL list does not provide verification of its validity and all damages incurred by actions taken after making only such an inspection shall be at the expense of the Relying Party;
   - verifying the validity of electronic signatures in electronically signed statements, and validity of electronic signature of a chain of certificates to the root certificate;
   - ensuring that applications used with the certificate are functionally relevant for its intended purpose, and are also relevant to the level of security specified in the Policy.
3. Due diligence of the Relying Party requires the use of the mechanism for secure signature verification, which ensures that:

- the public key used to verify the signature matches that which is presented to the Relying Party;
- the verification of the private key is securely confirmed and the results of this verification are presented fairly;
- if necessary, the contents of the signed electronic document could be identified;
- authenticity and validity of the certificate at the time of signature is reliably verified;
- results of the verification of electronic identity of the Titular 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 resulting from failure to perform due diligence.

9.7 Waiver of Liability

1. Except in cases of damages suffered from the use and reliance on QCQES, the Provider shall not be held liable for their own negligent actions.
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 Titular, 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 as a result of such violations, they may bring a claim against the Titular.
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 the test, free or demonstration certificates;
   - quality, features or technology of software applications and hardware devices in the infrastructure of B-Trust, used by Titulars or Relying Parties;
   - for timely revocation and suspension of certificates and/or for checks of the status of certificates for reasons beyond their control (e.g. lack of due diligence by a Relying Party, fraudulent action by a Titular, telecommunication and power interference, etc.).
8. The Provider shall not be held liable for any damages caused by use of a QCQES beyond the scope of its intended uses and applicable restrictions.

9.8 Limitation of Liability of the Provider

1. For the QCQES issued, the Provider shall be held liable within a maximum limit of liability - BGN 40 000.
2. These limits of liability shall be deemed to limit the liability of the Provider within the meaning of Art. 24, in conjunction with Art. 29, para. 3 EDESA.

9.9 Compensation for the Provider

1. For all cases of non-performance of the obligations of the Titular, the Provider shall seek responsibility from the Titular for damages and shall have the right to immediately terminate the certificate.

9.10 Term and Termination

1. The provisions of this document and the Policy and Practice of certification services by the Provider included herein shall be valid until issuing and publication of their next version/revision in the repository of documents on the Provider's website.
2. Contract for certification services between the Provider and the User shall be for a period of three years or until the expiration of the last issued certificate under this Contract.
3. Upon termination of the Provider’s activity, the provisions, Policy and Practice contained in this document shall be terminated too.
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. Contract for certification services between the Provider and the User shall be terminated upon expiration of the validity of the last issued certificate under the Contract or with the termination of all the certificates issued under the Contract.
6. Provider shall keep duly and securely all previous versions/revisions of this document and of the Practices and Policies.

9.11 Notification and Communication between the Parties

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

   Mailing address: 1612 Sofia, 41"Tsar Boris III" Blvd.

   Phone: 02 / 92 15 115

   Fax: 02 / 981 45 18

   e-mail address: info@b-trust.org

   Official website of the Provider: www.b-trust.org
3. In case of receiving a complaint, the Provider performs an immediate inspection and sends a reply to the complainant within 2 working days.

9.12 Changes to the Document

1. Provider may make editorial changes in this document that do not affect the content of 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. 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.

9.13 Dispute Resolution and Place of Jurisdiction

1. Any disputes between the Parties under the Contract for certification services shall be settled by agreement between the Parties, through understanding and good faith, and if no agreement is reached, shall be decided by the competent Bulgarian court.

9.14 Applicable Law

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

9.15 Compliance with applicable law

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

PART II:

POLICY

IN PROVIDING QUALIFIED CERTIFICATES

FOR QUALIFIED ELECTRONIC SIGNATURE

AND QUALIFIED CERTIFICATION SERVICES

1. Policy of providing QCQES and QCS is a document that is an integral part of the Certification Practice Statement. It describes the policies and procedures followed by the Provider upon issuing QCQES, the types of QCS applicable to such certificates, as well as their scope.
2. Policy defines the manner and level of security for identification of the Titular, procedures for the issuance, maintenance and management of the certificate, required security level of QSCD to create a signature and store the private key, and determines the degree of confidence in the certified data its use in various applications.
3. Provider maintains and implements Policies for the following types of QCQES, issued, maintained and managed by "BORICA" AD as a registered QTSP:

Qualified Certificate	Type of Certificate	Policy
Personal QCQES for individual	B-Trust Personal qualified certificate QES	B-Trust Personal Qualified Certificate Policy (QCP-n-qscd) (Policy for providing QCQES to individuals)
Professional QCQES for individual	B-Trust Professional qualified certificate QES	B-Trust Professional Qualified Certificate Policy (QCP-n-qscd) (Policy for providing QCQES to an individual associated with a legal entity)

4. General requirements and responsibilities of the Provider, Titular and due diligence of each Relying Party using the QCQES are specified in Part I (PRACTICE) of this CPS.
5. General Procedures for suspension, renewal and revocation of issued valid QCQES are specified in Part I (PRACTICE) of this CPS.
6. Prices of certificates and services for issuing and maintaining QCQES are specified in the Provider's Price List, available on their website.

10 POLICY ON PROVIDING PERSONAL QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE (QCQES) FOR INDIVIDUALS

B-Trust Personal Qualified Certificate Policy (QCP-n-qscd)
B-Trust O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1 (ETSI EN 319 411-2 O.I.D. = 0.4.0.194112.1.2)

10.1 General Characteristics of the Certificates

1. Electronic signature certificate issued under this policy has the character of a QCQES within the meaning of Art. 16 para. 1, EDESA.
2. Personal QCQES for an individual is issued to a Titular - individual and certifies the electronic identity of the Titular and his/her relationship with the public key.
3. For issuing such certificate the Titular or his/her representative needs to be present in person before the RA/LRA of the Provider and verification of their identity is required.
4. Identification procedures include proof of identity of the Titular and verification.
5. Verification of the request for issuing Personal QCQES for an individual shall be carried out in accordance with the preceding paragraphs and shall provide the highest level of security regarding the identity of the Titular and their relationship with the public key.
6. Titular can generate a key pair using the B-Trust QSCD and a relevant software, or other equivalent QSCD, compatible with the Provider's infrastructure.
7. Private key for the issuing Personal QCQES for an individual must be generated in QSCD and can not be derived out of it.
8. An issued Personal QCQES for an individual, certifying a public key that corresponds to a private key, is recorded in the QSCD, which is provided to the Titular.
9. The Provider reserves the right to add additional attributes to the Personal QCQES to an individual, if necessary.

10.2 Purpose and Applicability of the Certificates

1. Personal QCQES for an individual can be used when creating/signing QES by an individual identified as a Titular in the certificate to electronic documents and in applications that require high levels of information security.
2. Relying Party needs to exercise due diligence to verify the purpose and applicability of the certificate and software applications used for the creation and verification of signature, when relying an electronic signature accompanied by such certificate.
3. Relying Party should check the policy indicated in the Personal QCQES for an individual as being applicable to this certificate (attribute "Certificate Policy") and the purpose and limitations of the certificate, described in the attributes "Key Usage" and "Extended Key Usage", before trusting the electronic signature.

10.3 Designation of the Policy

1. The Provider maintains and implements a common policy designated in a Personal QCQES for an individual with a policy identifier O.I.D. = 1.3.6.1.4.1.15862.1.6.1.1, corresponding to policy „QCP-n-qscd" (OID 0.4.0.194112.1.2) under ETSI EN 319 411.
2. The Provider also adds in the Personal QCQES for an individual the policy „qcp-public-with-sscd" (O.I.D. = 0.4.0.1456.1.1) under ETSI EN 101 456, indicating that the private key has been generated, stored and used on QSCD.
3. The Provider adds in the Personal QCQES for an individual the attribute „Qualified Statements" with an identifier „id-etsi-qcs-QcCompliance " (OID=0.4.0.1862.1.1), indicating that the certificate is qualified.
4. The Provider adds in the Personal QCQES for an individual the attribute „Qualified Statements" with an identifier: „id-etsi-qcs-QcSSCD" (OID=0.4.0.1862.1.4), indicating that the private key has been generated, stored and used on QSCD.

5. The Provider adds in the Personal QCQES for an individual the attribute „Qualified Statements" with an identifier: „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), having value „id-etsi-qct-esign“ (oid=0.4.0.1862.1.6.1), indicating that the certificate is used as a qualified electronic signature.

10.4 Profile of the Certificate

1. The Provider shall issue Personal QCQES for an individual (B-Trust Personal qualified certificate QES) with the profile specified below:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Common Name: A name selected by the individual. If not selected, the full name of the individual shall be entered]
	G =	[First name of the individual on the ID card]
	SN =	[Family name of the individual on the ID card]
	SERIALNUMBER =	[Identifier of the individual. • For a Bulgarian citizen - one of the following: o PNOBG-XXXXXXXXXX for PIN o PASSBG-XXXXXXXX for passport number o IDCBG-XXXXXXXXX for an ID card number o TINBG-XXXXXXXXX for VAT number of an individual o PI:BG-XXXXXXXXXX for personal number of a foreigner o BT:BG-XXXXXXXXXX for individual number issued by B-Trust CA • For a foreign person - one of the following: o PNOYY- XXXXXXXXXX for a national personal number o PASSYY- XXXXXXXX for passport number o IDCYY- XXXXXXXXX for national ID card number where YY is a two-letter code of the individual’s country according to ISO 3166]
	E =	[E-mail address]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[hash of „Public key"]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy:

		Policy identifier=0.4.0.194112.1.2	
Enhanced Key Usage	-	Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

10.5 Operational Procedures for Issuing, Renewal and Management of the Certificate

1. Operational procedures for issuing, renewal and management of a Personal QCQES for an individual are described in Chapter 12 of this document.

11 POLICY ON PROVIDING PROFESSIONAL QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE (QCQES) FOR INDIVIDUALS ASSOCIATED WITH LEGAL ENTITIES

B-Trust Professional Qualified Certificate Policy (QCP-n-qscd)
B-Trust O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2 (ETSI EN 319 411-2 O.I.D. = 0.4.0.194112.1.2)

11.1 General Characteristics of the Certificates

1. Electronic signature certificate issued under this policy has the character of a QCQES within the meaning of Art. 16 para. 1, EDESA.
2. Professional QCQES for an individual associated with a legal entity is issued to a Titular - individual and certifies the electronic identity of the Titular and his/her relationship with the public key.
3. For issuing such certificate the Titular or his/her representative needs to be present in person before the RA/LRA of the Provider and verification of their identity is required.
4. Identification procedures include proof of identity of the Titular and verification.
5. Verification of the request for issuing Professional QCQES for an individual associated with a legal entity shall be carried out in accordance with the preceding paragraphs and shall provide the highest level of security regarding the identity of the Titular and their relationship with the public key.
6. Titular can generate a key pair using the B-Trust QSCD and a relevant software, or other equivalent QSCD, compatible with the Provider's infrastructure.
7. In the request for issuing Professional QCQES for an individual associated with a legal entity shall be also indicated the entity, represented by the Titular. The identity of this entity is also checked.
8. Private key for the issuing of QES must be generated in QSCD and can not be derived out of it.
9. An issued Professional QCQES for an individual associated with a legal entity, certifying a public key that corresponds to a private key, is recorded in the QSCD, which is provided to the Titular.
10. The Provider reserves the right to add additional attributes to the Professional QCQES for an individual associated with a legal entity, if necessary.

11.2 Purpose and Applicability of the Certificates

1. Professional QCQES for an individual associated with a legal entity can be used when creating/signing QES by an individual identified as a Titular in the certificate to electronic documents and in applications that require high levels of information security.
2. Relying Party needs to exercise due diligence to verify the purpose and applicability of the certificate and software applications used for the creation and verification of signature, when relying an electronic signature accompanied by such certificate.
3. Relying Party should check the policy indicated in the Professional QCQES for an individual associated with a legal entity as being applicable to this certificate (attribute "Certificate Policy") and the purpose and limitations of the certificate, described in the attributes "Key Usage" and "Extended Key Usage", before trusting the electronic signature.

11.3 Designation of the Policy

1. The Provider maintains and implements a common policy designated in a Professional QCQES for an individual associated with a legal entity with a policy identifier O.I.D. = 1.3.6.1.4.1.15862.1.6.1.2, corresponding to policy „QCP-n-qscd" (OID 0.4.0.194112.1.2) under ETSI EN 319 411.
2. The Provider also adds in the Professional QCQES for an individual associated with a legal entity the policy „qcp-public-with-sscd" (O.I.D. = 0.4.0.1456.1.1) under ETSI EN 101 456, indicating that the private key has been generated, stored and used on QSCD.

3. The Provider adds in the Professional QCQES for an individual associated with a legal entity the attribute „Qualified Statements" with an identifier „id-etsi-qcs-QcCompliance " (OID=0.4.0.1862.1.1), indicating that the certificate is qualified.
4. The Provider adds in the Professional QCQES for an individual associated with a legal entity the attribute „Qualified Statements" with an identifier: „id-etsi-qcs-QcSSCD" (OID=0.4.0.1862.1.4), indicating that the private key has been generated, stored and used on QSCD.
5. The Provider adds in the Professional QCQES for an individual associated with a legal entity the attribute „Qualified Statements" with an identifier: „id-etsi-qcs-QcType" (OID=0.4.0.1862.1.6), having value „id-etsi-qct-esign" (oid=0.4.0.1862.1.6.1), indicating that the certificate is used as a qualified electronic signature.

11.4 Profile of the Certificates

1. The Provider shall issue a Professional QCQES for an individual associated with a legal entity (B-Trust Professional qualified certificate QES) with the profile specified below:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Common Name: A name selected by the individual. If not selected, the full name of the individual shall be entered]
	G =	[First name of the individual on the ID card]
	SN =	[Family name of the individual on the ID card]
	SERIALNUMBER =	[Identifier of the individual. • For a Bulgarian citizen - one of the following: ○ PNOBG-XXXXXXXXX for PIN ○ PASSBG-XXXXXXXX for passport number ○ IDCBG-XXXXXXXXX for an ID card number ○ TINBG-XXXXXXXXX for VAT number of an individual ○ PI:BG-XXXXXXXXX for personal number of a foreigner ○ BT:BG-XXXXXXXXX for individual number issued by B-Trust CA • For a foreign person - one of the following: ○ PNOYY- XXXXXXXXX for a national personal number ○ PASSYY- XXXXXXXX for passport number ○ IDCYY- XXXXXXXXX for national ID card number where YY is a two-letter code of the individual's country according to ISO 3166]
	O =	[Name of the legal entity]
	2.5.4.97= (organizationIdentifier)	[Identity of a legal entity with which the individual is associated. One of the following: • VATBG-XXXXXXXXX – for VAT number • NTRBG-XXXXXXXXX – for UIC (BULSTAT)]
	E =	[E-mail address]

	C =	BG	
Public key	-	RSA(2048 bits)	
Subject Key Identifier	-	[Hash of „Public key "]	
Authority Key Identifier	KeyID =	[Hash of „Public key " of „Issuer“]	
Issuer Alternative Name	URL =	http://www.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.2 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2	
Enhanced Key Usage	-	Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL=http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1) id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

11.5 Operational Procedures for the Issuance, Renewal and Maintenance of the Certificate

1. Operational procedures for issuing, renewal and management of a Professional QCQES for an individual associated with a legal entity are described in Chapter 12 of this document.

12 OPERATING PROCEDURES FOR ISSUING, RENEWAL AND MAINTENANCE/MANAGEMENT OF QUALIFIED CERTIFICATES FOR QUALIFIED ELECTRONIC SIGNATURE

1. Operational procedures of the Provider for issuing, renewal and maintenance/management of QCQES are common for the different types of QCQES.

12.1 Registration of Application for Issuance of Qualified Certificate

1. Applicant for QCQES files an application to the RA/LRA of the Provider through an Operator of LRA at the place of issuance of the certificate.
2. Application for issuing shall include the information required under Art. 24 EDESA, individualizing the Titular and the type of requested certificate. The application may include additional, unverifiable information, some of which has to be certified, and another part is required to facilitate contact of the Provider with the Titular.
3. Application process requires that the Applicant (Titular or his/her representative) or the operator of the RA/LRA generate a cryptographic (RSA) key pair and include the public key information in the certificate.
4. The pair of cryptographic keys for QCQES must be generated in the B-Trust QSCD or other equivalent QSCD that meets the requirements for security level EAL 4 or higher, according to CC or other specifications defining equivalent levels of security.
5. The electronic format of the application for issuing of QCQES, together with information that will be included in the certificate, is a structure and shall be signed with the private key of the generated key pair.
6. When the Applicant does not generate the cryptographic key pair alone, the application process for a certificate shall only require information identifying the Titular, the type of certificate and other additional information, not including the generation of a cryptographic key pair for the QCQES. Generation of the key pair as a step in the application for a certificate is executed by an operator in the RA/LRA.
7. Upon successful registration of an application for issuing of a certificate, the operator in the RA/LRA must identify the identity of the Applicant.

12.2 Identification and Acceptance/Rejection of the Application

1. The Applicant shall be familiar with the list of documents required for issuing a QCQES selected by him/her, including the proposed type of Contract for certification services.
2. Applicant shall properly prepare the required documents from the list.
3. Applicant must personally visit a LRA of his/her choice and present the prepared documents.
4. Operator at the RA/LRA shall perform the procedure of identification and authentication of the Applicant for issuing of a certificate – Titular or authorized individual.
5. In compliance with the CPS - Part I (PRACTICE) and established internal procedures of the Provider, based on a received and registered application for a QCQES and documents submitted in the Applicant's presence – Titular or his/her representative, - RA/LRA confirms before the Provider:
   - the identity of the Titular;
   - representative power of the Titular, if authorized by another entities;
   - possession of the private key corresponding to the public key presented in the process;
   - the application for issuance of certificate;
   - additional information declared for inclusion in the certificate, excluding unconfirmed information;
   - accepts the Contract for Certification Services and the conditions under this CPS.

6. RA/LRA of the Provider, in the presence of the Applicant – Titular or his/her representative - upon successful verification of identification and consent to the information included in the certificate, shall immediately validate the information submitted via the application for issuing a certificate.
7. Based on the approved application for issuance, the CA of the Provider issues the type of certificate requested.
8. Upon rejection of an application for the issuance of certificate, the Applicant shall be notified by indicating the reasons for refusing the application.

12.3 Issuing and Publication of the Certificate

1. CA of the Provider identifies by electronic means the RA/LRA that has approved the electronic application for issuance of a QCQES.
2. CA generates the requested QCQES, signs it with the digital signature of the Provider and publishes it in its Public Register.
3. Notification Authority of the Provider sends e-mail notification to the Titular containing information of the issued QCQES, its serial number and the term of validity, except in the cases when no e-mail address was provided.

12.4 Acceptance of the Certificate

1. Acceptance of the content of the certificate is an act that is performed prior to issuing and publication by the Provider through the operational CA.
2. Provider, through the operational CA, shall publish the certificate issued in the Public Register of issued certificates.
3. Following publication of the certificate, the Titular is required within 3 (three) days of the publication to review the contents of the certificate again and, if necessary, make objections to the Provider or the RA/LRA concerning the correctness and completeness of its contents.
4. Upon objection made under the preceding item, Provider shall immediately suspend this certificate and take further action to reissue the certificate with the correct and complete information.

12.5 Delivery of the Certificate

1. Upon successful issuing of QCQES, operator of the RA/LRA of the Provider submits the issued QCQES to the Titular or his/her authorized representative. If necessary, the Operator records the certificate on B-Trust QSCD.
2. If the key pair is generated with the Titular, the Provider shall notify him/her via the e-mail address contained in the issued certificate, indicating the website where the issued certificate can be downloaded.
3. Upon presenting an identity document, Titular or authorized person receives the QCQES set issued on a B-Trust QSCD, where the private key of the certificate shall be generated.

12.6 Renewal of the Certificate

1. Renewal of a QCQES shall be performed by the Provider in accordance with the general operating procedure for the renewal of certificates described in the CPS - Part I (PRACTICE).

12.7 Suspending/Resuming the Certificate

1. Suspending/resuming the QCQES shall be performed by the Provider, in accordance with the general operating procedures for Suspending/Resuming a certificate described in the CPS - Part I (PRACTICE).

12.8 Revocation of the Certificate

1. Revocation of a QCQES shall be executed by the Provider, in accordance with the general operating procedure for revocation of a certificate described in the CPS - Part I (PRACTICE).