CERTIFICATION PRACTICE STATEMENT

ON THE B-TRUST ® CERTIFICATION, INFORMATION, CRYPTOGRAPHY AND CONSULTING SERVICES FOR QUALIFIED ELECTRONIC SIGNATURES PROVIDED BY "BORICA - BANKSERVICE" AD

Version 2.3

March 21, 2016

CONTENTS

ABBREVIATIONS IN BULGARIAN

AD	Joint Stock Company JSC
SG	Statement Gazette
EGN	Bulgarian Personal identification Number.
LT	Law of the Telecommunications
ZEDEP	Law for the Electronic Document and Electronic Signature
QES	Qualified Electronic Signature
KPC	Communications Regulation Commission
MTC	Ministry of Transport and Communications
NDDUU	Regulation on the activity of providers of certification services, procedures for its dissolution and requirements for providing certification services
NIAKEP	Regulation on algorithm requirements for development and verification of qualified electronic signature
Manual	Certification Practice Statement for the B-Trust® certification, information, cryptographic and consulting services provided by "BORICA - BANKSERVICE" AD
PIN	Personal Identification Number
Practice	Common practice in the provision of certification services
Policy	Policy for the provision of certification services

ABBREVIATIONS IN ENGLISH

ASN.1	Abstract Syntax Notation One
BG	Bulgaria
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation
CD	Compact Disk
CEN	European Committee for Standardization
CENELEC	European Committee for Electro-technical Standardization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard
IEC	International Electro-technical Commission
ISO	International Standardization Organization
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSE	Personal Security Environment
QES	Qualified Electronic Signature
RA	Registration Authority
RSA	Rivest - Shamir – Adelman Cryptographic algorithm for signature creation
SSCD	Secure Signature Creation Device
B-Trust SSCD	SSCD 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 - Hash algorithm for the hash identifier
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TRM	Tamper Resistant Module
URL	Uniform Resource Locator

COMPLIANCE AND USE

This "Certification Practice Statement":

- is developed by "BORICA - BANKSERVICE" 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 for certification, information, cryptographic and consulting services for universal electronic signature";
- enters into force on 21.03.2016;
- contains the conditions under which the Certification Services Provider "BORICA – BANKSERVICE" AD (Provider) provide paying customers with certificates for qualified electronic signature and related certification services, and other certification, 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 Law for the Electronic Document and Electronic Signature (ZEDEP)
- constitutes General Conditions under Art. 33, para. 2 of the Regulation on the Activities of Providers of Certification Services (NDDUU) and within the meaning of Art. 16 of the Law on Obligations and Contracts (ZZD). These conditions are part of a written Contract for certification services, which shall be concluded between the Provider and Users under Art. 23 of ZEDEP. The contract may contain special conditions and if so, these shall take precedence over the general conditions of this Manual;
- includes a detailed description of policies and practices in the provision of certification services by the Provider and is a public document aimed to bring the Provider's activities in line with ZEDEP and other relevant regulations;
- may be changed by the CSP and each new version of the Guide shall be published on the Provider's website;
- includes two parts:
- PART I: Practice for the provision of certificates and certification services for qualified electronic signatures (Certification Practice Statement, CPS);
- PART II: Policies in the provision of certificates and certification services for qualified electronic signature (Certificate Policy, CP);

This document is prepared in accordance with:

- the Law for the Electronic Document and Electronic Signature (ZEDEP)
- Regulation on the activity of providers of certification services, procedures for its termination and the requirements for providing certification services (NDDUU);
- Regulation on algorithm requirements for development and verification of qualified electronic signature (NIAKEP);

The content and structure of this document is in accordance with generally accepted international guideline RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework and refers to the information contained in the following well-established international guidelines, specifications and standards:

- RFC 3280: 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 2560: Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- ETSI TS 101 456: Policy requirement for certification authorities issuing qualified certificates;
- ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 101 862: Qualified certificate profile.

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

41 "Tzar Boris III" Blvd.
Sofia 1612
"BORICA - BANKSERVICE" AD

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

Practice in the provision of certificates and certification services for qualified electronic signature (QES):

- is an integral part of this document and contains general procedures for the issuing, suspension, renewal and revocation of QES certificates, security measures in the provision of certification services, staff requirements, the profile of certificates currently issued and maintained, and conditions for access to certificates issued and revoked;
- 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 CPS QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1

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

Algorithm	Name
Hash algorithms:	SHA1, SHA256
Asymmetric algorithms:	RSA

POLICY OF PROVIDING CERTIFICATES AND CERTIFICATION SERVICES FOR QUALIFIED ELECTRONIC SIGNATURE

The policy of providing certificates and certification services for qualified electronic signature:

- describes conditions the provider complies with and follows in the process of issuing of QES certificates, 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 QES certificates, 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 feasibility and the level of confidence in facts certified by such certificates.

1. The Provider implements a common Policy for all types of QES certificates, which is marked with the following policy identifiers in the relevant certificates:

Provider's Practice	Identifier(OID)
B-Trust CPS QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1

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

- personal QES certificate to an individual "B-Trust Personal certificate QES";
- professional QES certificate to an individual "B-Trust Professional certificate QES".

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

CERTIFICATION PRACTICE STATEMENT - PART I:

PRACTICE

IN THE PROVISION OF CERTIFICATES

AND SUPPORTING SERVICES FOR

QUALIFIED ELECTRONIC SIGNATURE

INTRODUCTION

The Practice in the provision of certification services for QES is an integral part of this document, developed by CSP „BORICA - BANKSERVICE" AD and approved by 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 QES certificates. It describes the general operating procedures during application for certificates, identification of applicants, issuing and publishing, delivery and acceptance of certificates, maintenance and management of these certificates.

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

1. GENERAL

1.1 Provider of Certification Services

1. "BORICA - BANKSERVICE" AD is a legal entity – trader, operating as a CSP under ZEDEP and other relevant regulations.
2. As a registered CSP, "BORICA - BANKSERVICE" AD carries out the following regulated activities:
- certification:
- acceptance of an application for initial issuing;
- authentication of the identity and validity of the Author/Holder's details;
- signing of the certificate;
- recording the certificate on a SSCD.
- maintenance and management of certificates:
- renewal of a valid certificate;
- changing the status of a valid certificate - suspension, renewal and revocation;
- checking the status of a certificate;
- checking certificate status in real time (OCSP status).
- keeping of records:
- keeping a Public Register of all issued certificates;
- publication of new certificates in the Public Register;
- keeping a list of all revoked certificates;
- Immediate publication of a revoked certificate in the list of revoked certificates;
- permanent access of third parties to the Public Register and to the list of revoked certificates.
- certification of time:
- certification of the exact time of delivery of the content of electronically signed documents (time of signature);
- certification of content at a particular time and irreversibility of content beyond this point;
- evidence-based inspection of time certificates issued.
- provide SSCD for generation and storage of cryptographic keys and for creation of digital signatures.

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

1.2 Regulation and Control

1. "BORICA – BANKSERVICE" AD has informed the CRC of the start of operations as a CSP under ZEDEP and current regulations.
2. Accreditation of "BORICA - BANKSERVICE" AD as a CSP by ZEDEP aims to achieve the highest security level of certification services 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 QES certificates and related certification services.

1.3 Identifiers in the Document

1. Provider's practice in issuing and maintaining QES certificates is implemented through the operational Certification Authority B-Trust Operational CA QES and is indicated in the certificate of this authority with the following identifier:

O.I.D. = 1.3.6.1.4.1.15862.1.5.1

2. Provider's policy on QES certificates and certification services provided for these is indicated in the certificates issued with the following identifier:

O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1

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

Type of Certificate	Name of Certificate	Policy	Policy Identifier (OID)
Personalized QES certificate of an individual	B-Trust Personal Certificate QES	B-Trust CP QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1
Professional QES certificate of an individual	B-Trust Professional Certificate QES	B-Trust CP QES	O.I.D. = 1.3.6.1.4.1.15862.1.5.1.1

1.4 Participants in the B-Trust® Infrastructure

1.4.1 Certification Authority

1. The B-Trust® "Certification Authority" of CSP "BORICA - BANKSERVICE" AD is a separate organizational unit which operates its' QES certification activity, and activities on the provision and maintenance of certification services. The Certification Authority 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. B-Trust® infrastructure has a two-tier hierarchy of the Certification Authority for issuing and maintaining QES certificates, as follows:

- Basic Certification Authority *"B-Trust Root CA"* - issuing certificates to subordinate operational certification authorities of the Provider and those of other providers. It also issues certificates for maintenance operational authorities of the CSP;
- Operational Certification Authority *"B-Trust Operational CA QES"* - issue QES certificates to users;

3. CSP reserves the right to expand B-Trust® infrastructure with further hierarchy of Certification Authorities, other than the hierarchy for QES (e.g., for application-oriented certificates).

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 certificates;
- registers applications submitted to the Certification Authority for issuance and implements changes in the status of certificates;
- performs appropriate checks to verify the identity of the Author and the identity of the Holder, 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 certification service;
- notifies the Certification Authority to issue a certificate after successful identification and finalized payment for the service;
- delivers to the Author/Holder the QES certificate issued, corresponding to the generated key pair;
- accepts or rejects registered requests for maintenance and management of certificates, in accordance with established Policy and practice;
- concludes contracts for the provision of certification and other cryptographic, information and consultancy services with holders 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 may open and provide certification services to Users via the Local Registration Authorities (LRA).

4. When the Registration Authority/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 Authors/Holders. The power is certified before all applicants and third parties with a written or electronic certificate of the Registration Authority/LRA.

5. In cases where the Registration Authority 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 Registration Authority/LRA under item 4 shall be governed by contract.

7. The Provider shall ensure that the activities of the Registration Authority/LRA will be consistent with the terms of this Guide.

1.4.3 Time Verification Authority

1. "Time Verification Authority" is a separate and integrate unit to the Certification Authority, which executes the following activities of the Provider:

- accepts requests for time verification of the content of an electronic document presented by the Author/Holder or a Trusting Party;
- issues a time certificate for the electronic document presented;
- allows for subsequent (after the period of validity of the certificate) proof, with respect to the Author, of the fact of signature of a statement or an electronic document.

2. "B-Trust TSA" is the Provider's time verification authority.

3. The electronic signature on the time certificate has the status of a qualified electronic signature of the Provider.

4. Time certificates are issued to physical persons and legal entities who are Authors/Holders or Trusting Parties for the respective electronic signature certificates.

5. Time certificates 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.
6. The Provider shall develop and publish a separate Policy of the Time Verification Authority.

1.4.4 Validation Authority

1. "Validation Authority" is a separate and integrate unit of the Certification Authority, which executes the following activities of the Provider:
- accept requests from an Author/Holder or a Trusting Party to check in real time the status of issued by the Provider certificate;
- prepare automatically in real time an electronically signed response on the status of a certificate.
2. "B-Trust VA" and "B-Trust VA QES" are the Provider's Validation Authorities.
3. The electronic signature on the resulting answer has the status of a QES of the Provider.
4. Each Trusting Party, when receiving electronic signature certificates, may apply for a real time check of certificate status.
5. Real time status checks of certificates are not mandatory for Trusting Parties, but Provider recommends to use this service and its integration in the creation or acceptance of QESs, during inspection and acceptance of electronic transactions, etc.

1.4.5 Subscribers

1. "Subscriber" is a person or legal entity who has signed a written contract with the Provider for the provision of certification services.
2. Subscriber who has completed application for the issuing of QES to the Provider, is called Author/Holder and in this capacity shall sign the issued by the Provider certificate.

1.4.6 Holder

1. "Holder" in a QES certificate is a physical person or legal entity on whose behalf the Author shall sign electronic statements, and is indicated as such in the certificate issued.

1.4.7 Author

1. "Author" in a QES certificate is a physical person who carries out electronic statements on their own behalf, or on behalf of the Holder, if any, and signs them in accordance with its representative authority, and is indicated as an Author in the certificate issued.
2. The QES certificate may indicate the reason for the empowerment of the Author.
3. Only the Author, as User of the QES certificate, is entitled to access the private key for signing electronic statements (creating an electronic signature).

1.4.8 Trusting Parties

1. "Trusting Parties" are the recipients of signed electronic submissions, whose Authors have issued QES certificates by the Provider.
2. Trusting Parties should have the knowledge and skills to use electronic signature certificates and trust circumstances certified therein only in terms of the applicable Policy, especially regarding the security level when performing identity verifications of Authors and Holders of these certificates.
3. Trusting Parties have permanent access to the records of the Provider to check the validity of QES certificates, to establish the electronic identity/authenticity of Authors/Holders 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. "Public Key Certificate" ("certificate") is an electronic document signed by the Provider, containing certain requisites showing the relationship between the Author/Holder and the public key corresponding to the private key with which the Author has created the electronic signature. It is used to check the signature on electronic documents and objects.
2. Certificates can be used for activities that require electronic identification, signing, authentication and encryption of electronic documents and objects.
3. Only certificates with policies listed in this document, issued by the Provider, have the character of QES certificates and contain the requisits provided for in Art. 24 ZEDEP.

1.5.2 Certificates of the Provider

Root certificate

1. Root certificate of the Provider is a certificate that is self-issued and self-signed with the private key of the Provider for his root public key. The root private key is used by the Provider to sign certificates for public keys of its operational and Certification Authorities, and Certificates of other (sub-)providers of certification services in the infrastructure of B-Trust.

2. In accordance with ZEDEP and the hierarchy of Certification Authorities in the infrastructure of the B-Trust, the Provider provides the valid certificate of the root Certification Authority to the CRC.

3. The main particulars of the root certificate of the Provider's Certification Authority "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 CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 April 2015 09:25:01 UTC
Validity to	-	16 April 2035 09:25:01 UTC
Subject	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d

Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d
		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path Length Constraint =	CA 4
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=All issuance polices [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	70 01 49 a2 e6 3c 21 ac d0 54 9f 87 de 8c df aa c9 93 f1 b0
Thumbprint (Sha256)	-	1f b2 11 4a 2c e4 bc 4d 56 b1 7b 03 a4 55 18 3b 31 65 40 b2 a0 fa d5 ce c2 b2 5a 84 eb 83 d5 29

4. Pursuant to Art. 16, para. 3, item 2 of ZEDEP, signatures of the Provider accompanied by the root certificate are QES.

5. The Provider may install and maintain other root certificates in the infrastructure of B-Trust.

Operational certificate for issuing of QES certificates

1. Certificate of Provider's operational Certification Authority of issuing of QES certificates is the certificate for public key of the operational Certification Authority "B-Trust Operational CA QES", signed with the basic private key of the Provider. Operational Certification Authority shall sign User certificates, signed by the Provider with the private key corresponding to this public key.

2. In accordance with ZEDEP and the hierarchy of Certification Authorities in the infrastructure of the B-Trust, the Provider provides the valid certificates of operating Certification Authorities to the CRC.

Main requisits of the operational certificate of the Provider's Certification Authority "B-Trust Operational CA QES" are:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	02
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 April 2015 09:29:53 UTC
Validity to	-	16 April 2030 09:29:53 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier	-	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a

Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d
		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate Serial Number=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints (critical)	Subject Type = Path length Constrain =	CA 3
Certificate Policies	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.2 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps
CRL Distribution Points	-	[1] CRL Distribution Point

		Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
Key Usage (critical)	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbprint (Sha1)	-	91 ab 04 6d 20 c6 ac 63 57 6d 69 d8 7c 2b 9f 3b 40 3d ef c2
Thumbprint (Sha256)	-	f3 b7 0a 38 f7 83 36 b5 97 b7 72 e7 85 24 85 44 ce 1b fc ee 28 15 3b 87 07 f7 e2 1f 2a 33 45 3d

3. Pursuant to Art. 16, para. 3, item 2 of ZEDEP, signatures of the Provider accompanied by this operational certificate are QES.

4. The Provider may install and maintain other operational certificates in the infrastructure of B-Trust.

Certificate of Time Verification Authority

1. Certificate of Time Verification Authority of the Provider is a certificate for the public key, signed with the basic private key of the Provider. The private key of the Provider's Time Verification Authority is used to sign certificates for time of presentation of contents of an electronic document by a User and/or Trusting Party.

2. Requisites of the official certificate of the Provider's Time Verification Authority "B-Trust TSA" are:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	0b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 April 2015 09:34:16 UTC
Validity to	-	15 April 2020 09:34:16 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5tss@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117.
	CN =	B-Trust Time Stamp Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2d 79 0e 96 e8 dc 9d c2 40 fd 08 71 da ae 06 67 4e 49 e6 2e
Authority Key	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d

Identifier		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://tss.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage (critical)	-	Time Stamping (1.3.6.1.5.5.7.3.8)
Thumbprint (Sha1)		17 8e 35 12 63 06 b2 eb 74 a9 e5 c7 72 e6 9d 7a ee a8 0a 8c
Thumbprint (Sha256)		4f a4 8f 10 1b a9 69 db 32 b3 1f d9 00 3b 74 4a fa 97 91 c2 20 5a 37 10 a4 94 5b 94 a7 7b e7 0d

3. Signatures of the Provider accompanied by the official certificate of the Time Verification Authority "B-Trust TSA" are QES.
4. The Provider publishes a separate Policy, including the conditions and procedures for issuing of certificates by the Time Verification Authority.

Certificates of Validation Authorities
1. Certificates of the Provider’s Validation Authorities are certificates of the public key, signed with the basic private keys of the Provider. Private keys of the key pairs of the Provider’s Validation Authorities „B-Trust VA" and „B-Trust VA QES" are used to sign the result/response of the real-time verification of the status of submitted electronic signature certificates.
2. The requisites of the official certificate of the Provider’s Authority "B-Trust VA" are:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	0c
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 April 2015 10:34:53 UTC
Validity to	-	15 April 2020 10:34:53 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5va@b-trust.org
	PostalCode =	1784
	STREET =	bul. Tsarigradsko shose No 117
	CN =	B-Trust Validation Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	14 e9 ea 3d 65 1c cc 97 e9 c6 7b 98 f2 02 11 18 c4 d7 a7 34

Authority Key Identifier	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d
		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name:

		URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
Key Usage (critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		66 7a 4d 10 e5 2d e2 df bb 89 b9 d3 01 bb 9d a1 97 1d 7c 2a
Thumbprint (Sha256)		ba e0 56 2a cf 8d 57 de f9 8e db 2d fc 03 f7 fe b0 20 bf f0 c6 77 dd 72 13 24 47 42 25 d7 ae ac

3. The requisites of the official certificate of the Provider’s Authority "B-Trust VA QES" are:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	10
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	07 May 2015 10:51:30 UTC
Validity to	-	06 May 2020 10:51:30 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5va@b-trust.org
	PostalCode =	1784
	STREET =	bul. Tsarigradsko shose No 117
	CN =	B-Trust Validation Authority QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2c 36 5a f3 2a db c1 a0 e8 f6 5e ae 95 25 94 d2 e3 4d 5a 0a
Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a
Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://ocsp.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	-	OCSP Signing (1.3.6.1.5.5.7.3.9)
OCSP No Revocation Checking	-	05 00
Thumbprint (Sha1)		2a 58 a0 7e 93 ab ea 40 79 9e 03 08 ba a4 26 80 89 3e 1c 6c
Thumbprint (Sha256)		7d f3 55 fc 8f 61 78 d9 ad a9 87 43 89 ab 47 05 91 d5 a5 e0 fa aa ac b9 4a 4c bc af d1 37 3a ca

4. Signatures of the Provider accompanied by the official certificates of „B-Trust VA" or „B-Trust VA QES" are QES.

1.5.3 Certificates of Other Operational Authorities

1. The Provider may issue operational certificates to other certification bodies in the infrastructure of the B-Trust, and other providers when the latter:

- perform activities outside those legally stipulated in ZEDEP, in order to function as providers;
- mutually certify public key their operational keys to enhance the credibility of certification services (cross-certification);
- perform the legally regulated activity of a CSP under the ZEDEP.

2. Issuing of these certificates is based on a specific agreement with the respective providers.

1.5.4 Certificate of Qualified Electronic Signature

1. Provider issues to Users QES certificates depending on applicants, the scope of application and purpose of electronic signature:

- personal QES certificate "B-Trust Personal Certificate QES";
- professional QES certificate "B-Trust Professional 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 QES certificates.

3. The Provider issues a QES certificate in the scope of Art. 24 ZEDEP only to individuals.

4. Personal QES certificate "B-Trust Personal Certificate QES" is issued personally to an individual – the Author. The application for issuing of this certificate is entered remotely (by electronic means), or locally, in an office of the Registration Authority/LRA. Identification procedure requires from the Author/Holder to be present in person or a person explicitly authorized by the Author. The identification procedure and procedures to generate the key pair, and for the issuing and delivery of the certificate to the Author guarantee highest level of security of the Author's data in the certificate and their relation with the public key.

5. Professional QES certificate "B-Trust Professional Certificate QES" is issued to an individual – the Author, representing the Holder under the Law or under a Letter of Attorney.

6. Application for registration and issuing of the corresponding qualified certificate is made online or locally in an office of the Registration Authority/LRA, and the identification procedure through validation of the Author's and Holder's identity requires from the Author/Holder to be present in person or a person explicitly authorized by the Author, respectively a person properly authorized by the Holder. The identification procedure and procedures to generate the key pair, and for the issuing and delivery of the certificate to the Author/Holder guarantee highest level of security of the Author's/Holder's data in the certificate and their relation with the public key.

7. Certificates "B-Trust Personal Certificate QES" and "B-Trust Professional Certificate QES" and their corresponding private keys are stored and made available to users on SSCD.

8. QES certificates are equivalent to a handwritten signature for all purposes within the meaning of Article 13, paragraph 4 of ZEDEP.

1.5.5 Use of QES Certificates

1. QES certificate issued by Certification Authority of the Provider can be used as per the Policy for this certificate.

2. Each certificate contains as a particular field for use of the certificate. This requisite is of the "critical" category and is identified as "Key Usage".

3. Certificates issued by the Provider may be used simultaneously for one or several of the following purposes:

- authentication - to establish the authorship of electronic statements made;
- confidentiality - to encrypt and decrypt electronic statements made or information objects;
- integrity - to preserve the integrity and irreversibility of electronic statements made or of information objects;
- non-repudiation - to enable subsequent proof to the Author, of the fact of signature of an electronic statement or content, and to neutralize any possible repudiation of signatures.

4. Particular "Extended Key Usage", which is also contained in QES certificates issued by the Provider and is of the category "non-critical", is used to detail the applicability of the certificate in view of its purpose.

5. The applicability of the types of QES certificates issued is as follows:

Type of Certificate	Applicability
Personal QES certificate "B-Trust Personal 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 ZEDEP.

Professional QES certificate “B-Trust Professional Certificate QES"	Electronic professional identity in applications requiring the 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 ZEDEP.

1.5.6 Limitation of a Certificate’s Scope

1. If the QES certificate is issued with a limitation of its scope and in accordance with Article 24, Paragraph 1, Item 8 of ZEDEP, the Provider’s practice allows a restriction of the electronic signature to be made in the certificate, in relation to purposes and/or value of transactions between Holders using the signature.
2. Upon discretion, the Provider may use the particular "Qualified Statements" or other suitable requisit in the profile X.509, v.3 of QES certificates.
3. The restrictive scope of QES certificates issued in terms of value of transactions concluded between Holders using an electronic signature shall be agreed between them and any Trusting Party and is beyond the scope of this Manual.

1.5.7 Use of Certificates outside the Scope of Application and Limitations

1. When the Author/Holder, or Trusting Party use and trust on a QES certificate with use other than 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 - BANKSERVICE" 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@bobs.bg;
Phone: (02) 9215 100, 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 QES certificates issued to Users and a current List of suspended QES certificates (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 Author/Holder of a certificate 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 a certificate. 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 certificates 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 ZEDEP and specified in this Guide. 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 Manual;
- Experience in providing certification services;
- Policy on provision of certification services;
- Contract for certification services;
- Tariff for all certification services provided;
- Rules for issuing QES certificates, including the rules for establishing the identity of a QES Holder;
- Terms and Conditions for use of QES, including requirements for storing the private key;
- Documents required for initial QES certification, for renewal and suspension/revocation of certificates;
- Other documents required by regulations and ZEDEP

2.3 Publication of Certificate-Related Information

1. Provider shall immediately publish in the Register a valid certificate after it has been signed by the operational Certification Authorities "B-Trust Operational QES".

2. Provider shall immediately publish an updated current CRL, signed by the operational Certification Authority upon revocation/suspension of a valid QES 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 CSP states a time for next CRL issue.

3. A new edition or version of the Manual, and of other accompanying documents under ZEDEP shall be published immediately.

2.5 Access to Registry and Repository

1. Provider shall keep a Public Register of QES 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 Manual and its conditions, practices and policies. Any interested person shall have access to 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 Registration Authority/LRA:
- accepts applications for issuance of certificates;
- carries out checks to identify the Author and, respectively, the Holder, as well as specific details of these by using all admissible means;
- approves registered applications upon successful verification, or rejects them;
- notifies the Certification Authority to issue the requested certificate.

2. The Registration Authority/LRA collects and receives the necessary information for identification and authentication of the Author/Holder.
3. Authentication/identification of the Author/Holder after registration and before issuing the QES certificate requires for him/her to be present in person, or the presence of an authorized representative of the applicant before the Registration Authority/LRA.
4. The Provider shall ensure that the individuals and legal entities are properly identified, authenticated and that requests for issuing QES certificates 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. QES certificates are in a format conforming to the X.509 standard. A Registration Authority/LRA, working on behalf of the Provider, 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 Author/Holder of the public key in the QES certificate.
3. Name and other individualizing characteristics of the Author/Holder 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 QES certificates issued by the Provider is contained in the relevant chapters of this document.

3.1.2 Use of Aliases

1. Provider may issue a QES certificate using an "Alias" to name the Author only after the Registration Authority/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 certification bodies contain unique names with a commonly understood semantics, allowing identification of the Provider that is the subject of such certificate.
2. QES certificates of Users include names matching the authenticated identification names of the Holders/Authors who are the subjects of these certificates.
3. For convenient electronic communication with the Author/Holder, the Provider shall request and certify in the QES certificate the Author’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’ QES certificates information for the electronic identification of the Author/Holder that has been successfully checked and validated by the Registration Authority/LRA, based on submitted identity documents of the Author and identity of the Holder.
2. In all certificates where an Author is entered, the field for name of the person (Common Name, CN) shall contain the full name of the person/Author, or his/her alias.
3. In a professional certificate, the distinguished name (DN) attribute shall contain information about the identity of the entity/Holder of the certificate.

3.1.5 Unique Names

1. Electronic identification of the Author/Holder of a QES certificate issued by the Provider is based on the DN.
2. "Subject" field in the certificate is based on the information about the Author/Holder, 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 Registration Authority/LRA based of submitted documents.
3. Provider guarantees a unique "DN" of the Author/Holder in the B-Trust domain by adding specific requisites to ensure such uniqueness.
4. An Author/Holder with a unique DN in the B-Trust domain can have more than one valid QES certificate 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. Authors/Holders are not allowed to apply for certification using names that infringe upon the property or moral rights of others.
2. Holders of such rights shall certify these with an official document before the Registration Authority/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 Holder and of an Author of a QES certificate, the Provider shall require an application for certification.
2. Application for initial issuance of a certificate before the Registration Authority/LRA of the Provider is a procedure by which Provider requires, collects and receives information necessary to identify the Author/Holder of the certificate.
3. The registration procedure includes:

- completing the registration form for a certificate;
- 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 Registration Authority/LRA, in accordance with the certification Policy;
- an option for application for other services related to the certificate.

4. Identification of the Author/Holder after registration and prior to issuing the requested QES certificate requires them to be present in person or to send authorized representative before the Registration Authority/LRA.
5. The initial identification and identity verification include:

- the Author or the person explicitly authorized by the Author 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 Author/Holder of the certificate to be issued.

6. Upon successful verification of the identity of the Author/Holder, the authorized operator in the Registration Authority/LRA shall:

- offer a certification services 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 Certification Authority of the Provider;
- may save the certificate issued on a SSCD and deliver it to the Author/Holder, or to an authorized person.

3.2.1 Proving Possession of Private Key

1. Registration Authority/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 Author.
2. The electronic application with the public key that is generated by the applicant for issuing of a QES certificate 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 Registration Authority/LRA - to verify possession 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 Registration Authority/LRA – shall verify such a signature.
4. Registration Authority/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 certificate issued by the Provider shall be generated on a SSCD and control of access to the private key in the SSCD shall only be held by the Author.

3.2.2 Establishing the Identity of an Entity or a Sole Proprietor as a Holder

1. Verification and identification of an entity or a sole proprietor as a Holder of a certificate is performed by the Registration Authority/LRA of the Provider under the respective Policy for issuing of a certificate and other internal documents of the Provider.
2. Establishing the identity of an entity or a sole proprietor as a Holder of a professional QES certificate "B-Trust Professional Certificate QES" requires an official representative of the Holder to appear before the Registration Authority/LRA and produce the required documents proving the Holder's legal status.

3.2.3 Establishing the Identity of an Individual as an Author, Holder or Holder's Representative

1. Identification and verification of the identity of an individual as an Author, Holder or Holder's representative, and empowerment of the Author, are carried out by the Registration Authority/LRA of the Provider by following the procedural steps set out in the relevant Policy and other internal documents of the Provider.
2. Identification of an individual as an Author/Holder, a person explicitly authorized by the Author or Holder's representative, requires this person to present before the Registration Authority/LRA the following documents:

Type of QES Certificate	Required Documents
Personal QES Certificate „B-Trust Personal Certificate QES"	Documents proving the Author's identity – in case Author is personally presented Documents proving the Authorized person's identity and a letter of attorney - in case Authorized person is presented
Professional QES Certificate „B-Trust Professional Certificate QES"	Documents proving the identity of the Author, Holder and the representative power of the Author to the Holder.

3.2.4 Special Attributes

1. The Provider may include in the certificate to be issued specific attributes associated with the Author/Holder, if the certificate is issued for a specific purpose under the respective Policy.
2. This information is subject to verification by the Registration Authority or registration office.

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 pursuant to Art. 24 ZEDEP.
2. The Provider may include unconfirmed information about the Author/Holder in the certificate to be issued, and it shall not be subject to review by the Registration Authority or registration office.
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 QES certificate 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 certificate of a particular Author/Holder if the information about the Author/Holder 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 QES certificate, 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 certificate of an Author/Holder with a new key pair (Re-key), only if the latter so requests and declares that no change of information contained in the current certificate has occurred. The renewed certificate has a different public key and a new period of validity; verified information about the Author/Holder 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 Author/Holder of the certificate being renewed does not require them to be present in person before the Registration Authority/LRA of the Provider.
7. Upon changes in the information about the Author/Holder of the certificate, the current certificate is not renewed. The Provider shall issue a new certificate, following the initial identification and authentication of the Author/Holder, and shall immediately terminate the current certificate.
8. Renewal of certificate of a Certification Authority of the Provider „BORICA - BANKSERVICE" AD is not allowed. In any event that requires replacement of the certificate, a new certificate of the Certification Authority is always issued.
9. The Provider shall observe the following time limits and requirements for identification when renewing a QES certificate:

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 SSCD 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 SSCD 3. The application for renewal shall be submitted at the Registration Authority/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 Registration Authority/LRA, shall suspend a valid certificate upon request, but for not more than 48 hours (ZEDEP, Art. 26).
2. Provider, via the Registration Authority/LRA, shall not perform identification and authentication of the applicant and shall immediately suspend the certificate.
3. Provider, via the Registration Authority/LRA, shall resume operation of a suspended certificate in accordance with Art. 26, para. 6 ZEDEP.

3.5 Identification and Authentication upon Revocation

1. Provider, via the Registration Authority/LRA, shall terminate a valid certificate upon request for revocation, in accordance with Art. 27 ZEDEP.
2. Provider, via the Registration Authority/LRA, shall immediately suspend the certificate and perform subsequent identification and authentication of the applicant.
3. Provider, via the Registration Authority/LRA, shall perform identification and authentication of the applicant within the admissible time limit for suspension of the certificate, which is 48 hours.
4. Provider, via the Registration Authority/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. Author/Holder of a terminated certificate may request a new certificate.
3. Provider, via the Registration Authority/LRA, shall perform initial identification and authentication of the Author/Holder, if the latter applies for a new certificate.

4 OPERATIONAL REQUIREMENTS AND PROCEDURES

1. Provider, via Registration Authority/LRA, within the contract for certification services, shall provide the following operational procedures for certification services applicable to QES certificates:

- registration of an application for certificate;
- processing of an application for issuing;
- issuing of a certificate;
- delivery of a certificate;
- use of the key pair and certificate;
- renewal of a certificate via "Renew";
- renewal of a certificate via "Re-key";
- suspend/resume operation of a certificate;
- revocation of a certificate;
- current status of a certificate.

2. Provider, via Registration Authority/LRA, shall give an option to the Author/Holder 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 Registration Authority/LRA of the Provider.

3. Application for issuing of a certificate may be filed in person by the Author/Holder, or by an authorized representative of the Holder (authorized person).

4. The applicant shall register the application for certificate online or through an operator at the Registration Authority/LRA of the Provider.

5. An operator of the Registration Authority/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 ZEDEP, about the Author/Holder 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 Holder.

2. The process of application allows the operator of the Registration Authority/LRA or the Author/Holder to generate the pair of cryptographic (RSA) keys and to include the public key in the information required for issuing of certificate.

3. The pair of cryptographic keys for issuing a QES certificate must be generated in a SSCD 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 in SSCD.

5. Where necessary, the Registration Authority/LRA shall provide the Author/Holder or an authorized person with protected information/access code to the private key in SSCD.

6. If the applicant does not have a SSCD, when submitting an application for issuing of a certificate before the Registration Authority/LRA of the Provider, he/she needs to only enter information required to identify the Author/Holder, and such other information as necessary, without generating a cryptographic key pair (RSA) 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 QES issuance and management shall be signed by the Provider.

4.2 Procedure of Issue

4.2.1 Functions of Identification and Authentication

1. The Registration Authority/LRA shall perform identification and authentication of the applicant for a certificate - Author/Holder 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, in the applicant's presence - Author/Holder or his/her representative, the Registration Authority/LRA shall check and verify before the Provider:

- identity of the Author/Holder, respectively, of the authorized person;
- representative power of the Author to the Holder and of the authorized person to the Holder;
- 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 Manual.

3. If the key pair is generated with the Author/Holder, the Registration Authority/LRA should check the electronic application and requirements for the security level of SSCD.

4.2.2 Confirmation or Rejection of a Request for Issuance

1. After successful checks, an authorized operator of the Registration Authority/LRA shall approve the application for a certificate before the Provider.
2. Registration Authority/LRA shall reject the application for certificate if the validation fails.
4. Registration Authority/LRA shall immediately notify the applicant and specify the reasons for rejection.
5. Rejected applicant may file another application after having removed the reasons for rejection.
6. Registration Authority/LRA shall properly store and archive documents submitted and the confirmed electronic application for a certificate.
7. Registration Authority/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.
8. The Author/Holder of a QES certificate 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. Registration Authority/LRA of the Provider shall immediately, in the presence of the applicant - Author/Holder 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. Certification Authority of the Provider shall issue the certificate immediately after approval of the electronic application for issuing by the Registration Authority/LRA.

4.3 Issuing of a Certificate

4.3.1 Operation of the Certification Authority

1. Certification Authority of the Provider shall identify by electronic means the Registration Authority/LRA that has approved the electronic application for issuing of a QES certificate.
2. Certification Authority shall generate the certificate 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 Author/Holder of the Certificate by the Provider

1. Provider, via the Office for Notification of Users of certification services, shall immediately notify the Author/Holder of a certificate issued and published.
2. Office for Notification shall send to the Author/Holder an e-mail with information about the Author's name, type of QES certificate issued, 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 Author/Holder or, respectively, to the authorized person, via the Registration Authority/LRA.
4. An authorized operator of the Registration Authority/LRA shall record the certificate on the SSCD where the cryptographic key pair (RSA) for this certificate has been generated.

4.4 Adoption and Publication of the Certificate

1. Provider, via the operational Certification Authority, shall promptly publish the certificate issued in the Public Register of certificates issued.
2. Author/Holder may object before the Provider or via the Registration Authority/LRA, if the certificate contains errors or omissions, within 3 (three) days of its publication in the Public Register. These shall be immediately removed by the Provider through issuing of a new certificate without charge, unless they have been made due to false data provided.
3. In the absence of objection by the Author/Holder 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 Author

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

4.5.2 By the Trusting Party

1. The public key in the certificate corresponding to the private key held by the Author is publicly available to everyone.
2. Each Trusting Party, including an operator in the Registration Authority/LRA should use the public key and the certificate of the Author/Holder, 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 electronic signature;
- until the certificate is revoked;
- where the certificate is suspended, the public key is not to be used.

4.6 Renewal of a Certificate

1. Renewal of a QES certificate shall retain information about the Author/Holder of the current certificate; the period of validity in the renewed certificate shall be changed.
2. Renewal of a QES certificate, 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 QES certificate shall be preceded by an application for renewal before the Registration Authority/LRA.
4. An application for renewal of a certificate shall be registered online, where the Author/Holder has a valid QES certificate 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 Author/Holder or his/her representative must personally visit the Registration Authority/LRA of the Provider.
6. Author/Holder or his/her authorized representative may renew a QES certificate multiple times, subject to the conditions for renewal specified below.
7. Provider shall not permit the use of a key pair for QES for a period greater than 3 (three) years.
8. Provider does not recommend repeated renewal of a QES certificate via the "Renew" function, in order to reduce the risk of compromising the private key.
9. Provider recommends that Author, respectively Holder or an authorized persons to renew his/her certificate via the "Re-key" function.

4.6.1 Conditions for Renewal of a Certificate

1. Registration Authority/LRA will renew a QES certificate via the "Renew" function, subject to the following conditions:
- the certificate is not terminated during its period of validity;
- the Author/Holder 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. Registration Authority/LRA will renew a QES certificate via "Re-key", subject to the following conditions:
- the certificate is not terminated during its period of validity;

- Author/Holder 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 Author/Holder 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. Author/Holder 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 QES certificate is preceded by the registration of an application for renewal before the Registration Authority/LRA of the Provider.
2. An application for renewal of a certificate by electronic application shall be certified by electronic signature corresponding to the valid certificate of the Author/Holder being renewed.

If the certificate being renewed has expired, the Author/Holder or his/her representative must personally visit the Registration Authority/LRA of the Provider. The Registration authority/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 Registration Authority/LRA confirms the application for renewal before the operational Certification Authority of the Provider.
4. Upon successful electronic authentication by the Registration Authority/LRA via the authorized operator, the operational Certification Authority shall fulfil the confirmed application for renewal of the certificate.
5. Upon unsuccessful identification and verification of the conditions for renewal, the Registration Authority/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 QES certificate.

4.6.4 Notification of the Author/Holder upon Renewal of the Certificate

1. Provider, via the Office for Notification of Users of certification services, shall immediately notify the Author/Holder of the renewed and published certificate.
2. Office for Notification shall send to the Author/Holder an email name with the name of the Author/Holder, the type of QES certificate, unique serial number and validity period of the renewed certificate and the address (URL) which can be used to deliver the renewed certificate.
3. Where the applicant for renewal of a certificate visits the Registration Authority/LRA, the Author/Holder receives the renewed certificate from the authorized operator who records it on the SSCD where the pair of cryptographic keys (RSA) for the certificate has been generated.

4.6.5 Publication of the Renewed Certificate

1. Provider, via the operational Certification Authority, 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 QES certificate 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 Changing a Certificate

1. Provider shall allow changes in the content of information in an issued and published QES certificate only subject to the requirements and conditions for issuing a new certificate.
2. Provider shall not allow a change in the profile of QES certificates, as specified in Part II of this document.

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 Certification Authority for issuing and maintaining QES certificates, the effect of any certificates issued by this Authority that are still valid shall be terminated.
3. Only the operational Certification Authority that has issued the QES 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 Certification Authority, 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.

6. In case of failure of the system, services, or other factors that are beyond the control of the Certification Authority, the CSP 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.

4.9.1 Conditions for Revocation of a Certificate

1. The Provider shall terminate a certificate upon:
- death or disability of the Author/Holder with revocation of the legal person of the holder;
- revocation of the representative power of the Author to the Holder;
- the establishment of misrepresentation in the certificate;
- certified information that has subsequently become untrue;
- change in already certified information of the Author/Holder;
- compromising the private key;
- delay in payment of outstanding remuneration;
- application for revocation filed by the Author/Holder, after verifying their identity and representative power of the Author.

2. Provider shall immediately suspend the certificate in each of the above circumstances.
3. Provider shall terminate all certificates it has issued, if it ceases to operate without transferring the activities to another provider.
4. Provider may suspend and terminate the certificate of an Certification Authority of 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 Registration Authority/LRA of the Provider.
2. The application for revocation of a certificate may be registered electronically only when the Author/Holder has (another) QES certificate valid and accessible for use. Otherwise, the application shall be made before an authorized operator of the LRA.
3. Revocation of certificate on application filed by electronic means shall be certified by QES corresponding to a valid certificate of the Author/Holder.
4. The authorized operator at a Registration Authority/LRA shall immediately suspend the certificate, without identifying the applicant, for not more than 48 hours.
5. In all cases, the Author/Holder or his/her representative must personally visit the Registration Authority/LRA of the Provider for verification of the applicant's identity.
6. The Registration Authority/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 Registration Authority/LRA via an authorized operator, the operational Certification Authority shall fulfil the application for revocation of the certificate.
8. Upon unsuccessful identification and verification of the conditions for revocation, the Registration Authority/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 Certification Authority, shall immediately publish the terminated certificate in the CRL, and shall issue a new CRL.
11. Upon revocation of the certificate, the Provider, via its Office for Notification, shall immediately inform the owner and holder of the terminated certificate.
12. Terminated certificate of an Author/Holder 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 certificate, the Provider through its Registration Authority/LRA shall suspend the certificate for not more than 48 hours.
2. During this grace period, the Provider through its Registration Authority/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 action of this certificate.
4. The Provider shall resume the certificate upon application of the Author/Holder 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 Trusting Party shall accept a QES certificate 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 Validation Authority "B-Trust VA" or "B-Trust VA QES".
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 Certification Authority, shall immediately publish a new updated CRL, every time a valid certificate issued by that authority is terminated.
2. Provider, through its operational Certification Authority, 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 Certification Authority 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 QES certificates issued, by using the OCSP protocol.

4.9.9 Requirements for Using the OCSP

1. Real time checks of the status of a certificate in (using the OCSP protocol) requires a software client (OCSP-client) and online access via the Internet to the Validation Authority "B-Trust VA" or "B-Trust VA QES".
2. Real time checks of the status of a certificate in (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 Certification Authority, shall suspend a valid under certificate certain conditions and for a period of up to 48 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 Author/Holder 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 ZEDEP.

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 Registration Authority/LRA of the Provider.
2. The application for suspension of a certificate may be registered electronically or before an authorized operator of the LRA.
3. Suspension of a certificate on application filed by electronic means shall be certified by QES corresponding to a valid certificate of the Author/Holder.

4. The authorized operator at a Registration Authority/LRA shall immediately suspend the certificate, without identifying the applicant. Suspension of the certificate shall be performed by its temporary inclusion in the CRL, as per Art. 26, Para. 5 ZEDEP

5. Upon successful electronic authentication by the Registration Authority/LRA via an authorized operator, the operational Certification Authority shall fulfil the application for suspension of the certificate.

6. Registration Authority/LRA may not refuse to suspend a certificate.

7. Upon revocation of the certificate, the Provider, via its operational Certification Authority, 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 owner and holder of the terminated certificate.

4.9.13 Limitation of the Period of Suspension of a Certificate

1. Provider shall suspend a QES certificate for up to 48 hours of receiving the application for suspension.

2. Provider shall suspend the certificate for 48 hours of before its revocation.

4.9.14 Resuming the Operation of a Suspended Certificate

1. Provider shall resume operation of a suspended certificate:

- up to 48 hours after its suspension;
- after the end of the period of suspension (48 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 Holder, 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. Registration Authority/LRA shall resume a suspended certificate after receiving an application to that effect by the Author/Holder and upon successful verification of his/her identity.

3. Registration Authority/LRA shall resume a suspended certificate after receiving a written order of the CRC, or the Chairman of the CRC, to resume the certificate.

4. Registration Authority/LRA shall immediately resume a suspended certificate the end of the period of suspension (48 hours).

5. 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 QES certificates, issued by the Provider through its operational Certification Authority "B-Trust Operational CA QES" 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 list of terminated certificates) 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 Validation Authorities "B-Trust VA" or "B-Trust VA QES", as follows:

- "good" - the certificate is not suspended/terminated, but asserts 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 Validation Authority 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.

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 Certification Authority "B-Trust Root CA";
- Operational Certification Authority "B-Trust CA QES";
- Operational Certification Authority "B-Trust CA AES";
- Registration Authority;
- Public Register;
- Time Verification Authority e "B-Trust TSA";
- Validation Authority "B-Trust VA";
- Validation Authority "B-Trust VA QES".

3. The Provider's B-Trust infrastructure is physically and logically separate and not used in other activities operated by "BORICA - BANKSERVICE" 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 Certification Authority of the Provider and all central components of the infrastructure - "B-Trust Root CA", "B-Trust CA QES " and " B-Trust CA AES ".

5.1.2 Physical Access

1. Physical access to the specialized premises shall be controlled by access control systems, video surveillance, alarm systems, air conditioning, 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 Guide relating to B-Trust infrastructure, shall be implemented in full accordance with 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 QES certificates, in accordance with applicable regulations.
2. The Provider shall operate using its own staff.
3. For certain activities under Art. 5 NDDUU, 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 qualified electronic signature certificates, including creation of a key pair - public and private, for a qualified electronic signature;
- data storage and archiving.

5.2.4 Requirements for Division of Responsibility

1. The activities of the Provider 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, 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 anomalies 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 certification bodies and components in the infrastructure of the B-Trust;
- management of crypto-modules (HSM) of "B-Trust Root CA", "B-Trust CA QES" and "B-Trust CA AES";
- 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;
- time verification of 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 Registration Authority/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 User Guide, 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 one (1) 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 User 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 ten (10) 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 detefined and documented by the Provider;
- stored on reliable electronic media that cannot be easily destroyed or deleted during the storage of the archive;
- the Certification Authority electronically shall sign 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;
- communications between Users and protected Internet websites of the Provider shall be based on the HTTPS protocol.

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 Restoration 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 Guide, Policies, the Contract for certification services and instructions for service/work to Users 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 certificate 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 his Certification Authorities as a result of natural disasters or accidents.
3. In case of failures in computer resources, software or information, the Provider shall notify Authors/Holders, restore the infrastructure components and resume access to the Public Register and CRL.

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 Certification Authority:

- 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 Certification Authority;
- 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 Certification Authority:

- immediately terminate the certificate of the root authority;
- follow all the steps in the preceding paragraph;
- inform the CRC and accredit/register new Certification Authority(-ies).

5.8.2 Of an Author

1. Upon compromise of the private key of an Author, the latter or the Holder, if the certificate specifies any, 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 NDDUU.

3. Upon termination of activities, the Provider shall:

- notify the CRC of its 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 his 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 SCP changes the status of its certificates and duly submit all documentation relating to its 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 its activities to another registered provider, he 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 (RSA) 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 its private keys only for the purpose of its activities, as follows:

- to sign official certificates issued to operating authorities of its infrastructure;
- to sign the CRL issued and published;
- to sign all QES certificates issued and published to Users.

3. The cryptographic (RSA) key pairs (public and private) of QES certificates issued in the infrastructure of the Provider shall be generated, as follows:

- by the Author/Holder - using hardware and software that is under his/her control, but is approved by the Provider;
- by an operator of the Registration Authority/LRA of the Provider - using hardware and software that is under the control of the infrastructure of B-Trust.

4. The generation of a key pair to a QES certificate always shall use SSCD, with a protected account under the regulations of ZEDEP.

5. The Provider may, on the basis of a contractual relationship, provide Authors/Holders 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 SSCD are QES.

7. The Author/Holder shall use only licensed software to work with SSCD.

6.2 Generation Procedure

6.2.1 To a Certification Authority of the Provider

1. The Provider shall generate pairs of cryptographic (RSA) keys to the root and operational Certification Authorities by using a hardware crypto system (HSM, Hardware Security Module) 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, storing and installing key pairs of the root and operational Certification Authorities, respectively, "B-Trust Root CA" and "B-Trust Operational CA QES", 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 Board of Directors of BORICA - BANKSERVICE "AD and a Notary Public.

4. A key pair of a Certification Authority 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 activation of access to the corresponding private key by a single person is impossible.

7. Private keys of Certification Authorities shall be stored separately on individual SSCDs, 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 Certification Authorities stored in different SSCDs does not allow these keys to be compromised and/or reproduced without authorization outside the Provider.

6.2.2 To an Author/Holder

1. The key pair of an Author/Holder of a QES certificate shall be generated only in a SSCD approved by the Provider, after being checked for level of security and for seamless operation through the interfaces of the B-Trust infrastructure.

2. When the key pair is generated at the Provider, a B-Trust SSCD shall be always used. The private key of the generated key pair can not be derived from the SSCD.

3. The private key shall be controlled by an access code; the key length for QES shall be at least 2048 bits. The Author shall use the private key to create the signature by entering the access code in the SSCD.

4. When a key pair is generated with the Author/Holder, the Provider shall advise the latter to use an approved SSCD in the B-Trust infrastructure, or equivalent.

5. The Provider shall reccomend the User to use a B-Trust SSCD or other SSCD compatible with B-Trust infrastructure.

6.2.3 Delivery of a Private Key

1. When the key pair is generated with the Provider, the Author/Holder or explicitly authorized by him person shall receive the private key and certificate issued on a B-Trust SSCD at a LRA of the Provider.
2. The SSCD shall ensure the highest level of security and protection of the private key and shall be supplied with an initial access code.
3. The Author/Holder is obliged to change in the initial access code and insert their own code.
4. When the Author/Holder generates the key pair in another SSCD, the private key shall be contained in this SSCD, but through the Registration Authority/LRA, the Provider shall check whether the Author/Holder is holding this key.

6.2.4 Delivery of Public Key at the Provider

1. This Is performed only by the Author/Holder who generates their own key pair and who should deliver such public key for the needs of the process of issuing the certificate.
2. The Author/Holder supplies through the Registration Authority/LRA of the Provider the public key of the generated key pair by an application in electronic form.
3. The Author/Holder may submit an application form on electronic media in person at the Registration Authority/LRA, along with other documents in accordance with the Provider's Policy, or through the website of the Provider.

5. The Registration Authority/LRA of the Provider shall check whether the Author/Holder is holding the private key.

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

1. Provider's public keys shall be publicly accessible on the Provider's webpage, where its official certificates are published.
2. Each Trusting 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 Certification Authority "B-Trust Operational CA QES" shall be 4096 bits.
3. The length of the RSA-key pair of the operational Authorities "B-Trust TSA","B-Trust VA" and "B-Trust VA QES" shall be not less than 2048 bits.
4. The length of the key pair (RSA) for QES of an Author/Holder generated by infrastructure of the Provider (B-Trust SSCD) shall be at least 2048 bits.
5. The length of the key pair (RSA) for QES of an Author/Holder generated outside the Provider's infrastructure shall be at least 2048 bits.
6. Regardless of where the key pair for a QES certificate shall be generated, the key must have a length of at least 1024 bits for RSA and DSA algorithms, and 160 bits for ECDSA 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 in the SSCD.

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 CA" and "B-Trust CA QES" shall use a highly reliable cryptographic system (Hardware Security Module, HSM), certified for security level FIPS 140-2 Level 3, which meets all regulatory requirements.
2. B-Trust SSCD, where the private key of the Author/Holder is generated and stored, shall have a security level of CC EAL 4+ / FIPS 140-1 Level 2.
3. All SSCDs outside the infrastructure of B-Trust that a User could use to generate the key pair and store the private key must be certified for a level of security CC EAL 4 and equivalent or higher.

6.3.2 Control of Use and Storage of a Private Key

1. Private keys of the Certification Authorities of the Provider shall be used in the cryptosystem (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 Certification Authority, the procedure for storing the private key (or key pair) shall be performed, in accordance with established internal procedures.
3. The private key of the Author/Holder shall be used in B-Trust SSCD only or in SSCD with equivalent security level, and shall be accessible via a personal access code.
4. Along with generating the key pair of an Author/Holder, the private key shall be stored in the SSCD.
5. The Provider shall not store or archive in any way the private key of an Author/Holder used to create a QES, irrespective of where the pair is being generated.

6.3.3 Storage and Backup of the Private Key

1. Private keys of the Certification Authorities shall be separately stored on separate SSCDs with protection profile CC EAL 4+ or higher, and access to any SSCD shall be controlled by an access code held by an authorized person of the Provider's staff.
2. The access code to any SSCD shall be personal for each authorized person of the Provider's staff.
3. Separate storage of private keys of Certification Authorities on several SSCDs and private control of access to these SSCDs 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 cryptographic system (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 its own SSCD.
5. The private key of an Author/Holder shall be stored on SSCD only and may not be reproduced on another SSCD.
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.

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 the introduction of all parts of the access code, shall access to the slot in the cryptosystem (HSM) be permitted and the private key shall be activated.
3. A private key of an Author/Holder shall be activated by entering the user access code in the SSCD 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 Certification Authorities 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 Author/Holder shall be deactivated (the possibility to use/access the private key is suspended) by suspension of logical access to the SSCD, or its physical destruction.

6.3.7 Destruction of a Private Key

1. A private key of the Provider in the cryptosystem of the Certification Authorities shall be destroyed by deletion of the key, or deletion of the appropriate slot. If necessary, recovery media (SSCDs) stored in the archive shall be deleted as well.
2. A private key of an Author/Holder shall be destroyed by deletion from the SSCD or by complete deletion/initialization of the SSCD.

6.4 Other Aspects of Key Pair Management

6.4.1 Backing up the Public Key

1. Public keys of Certification Authorities 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 Certification Authorities shall be archived and stored for 10 years after the period of validity or cancellation of the respective certificates.
3. Public keys of Authors/Holders 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 Authors/Holders 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. QES certificates shall have the following validity periods:
- of the root Certification Authority "B-Trust Root CA" - 20 (twenty) years;
- of the operational Certification Authority "B-Trust CA QES" - 15 (fifteen) years;
- of an Author/Holder – as per the contract between the Provider and the Author/holder, 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 Certification Authority 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 Certification Authority 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. Upon initial issuance of a certificate on a B-Trust SSCD, before generating a key pair, the SSCD 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 SSCD and to unblock a blocked SSCD.
2. Initial User and Administrative access code and code to unlock the B-Trust SSCD shall be delivered to the Author/Holder or his/her authorized representative in a sealed, opaque paper bag.
3. The Author must change the initial User access code through the software that comes with the B-Trust SSCD.
4. The Provider shall reccomend the Author to periodically change their user code to access the SSCD.
5. The Author/Holder must use the Administrative access code to unblock a blocked B-Trust SSCD.

6.5.2 Protection of Activation Data

1. The Author must store and keep from compromising the access codes of their SSCD.

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 an Author, the SSCD shall be blocked.
2. The Author must use the provided Administrative access code to unblock a blocked B-Trust SSCD.

6.6 Security of Computer Systems

6.6.1 Security Requirements

1. Computer platforms operating all critical components of 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 provides all certification services through its operational systems.
3. Products and services of the Provider shall be tested in real working conditions.

6.8 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.

6.9 Verification of Time

1. The Provider shall publish a separate document - Policy and Practice of the Time Verification Authority.

7 PROFILES OF QES CERTIFICATES, CRLs AND OCSPs

7.1 Profile of QES Certificates

1. The full content (profile) of QES certificates shall be contained in the User's Manual, Part II: Policy to Provide Certificates and Certification Services.

7.1.1 Version Number

1. The Provider issues QES certificates in a X.509, v3 format.
2. Version number is recorded in the issued certificate.

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 Certification Authority 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" – has two policies: 1.3.6.1.4.1.15862.1.5.1.1 determines the identifier of the policy for QES certificates issued by the Provider; 0.4.0.1456.1.1 determines the QES certificate as issued on Secure Signature Creation Device (SSCD). This attribute in QES certificates has the meaning of 0.4.0.1456.1.1.
6. Attribute "Key Usage" - a critical 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 Certification Authority of the Provider.
9. Attribute "Authority Information Access" - contains the URL-address of the Validation Authority "B-Trust VA" or "B-Trust VA QES".
10. Attribute "Qualified Statements" - the attribute contains an indication that the certificate is for QES (qualified electronic signature) and the private key is generated and stored in SSCD.

7.1.3 Identifiers of the Algorithms of an Electronic Signature

1. The attribute "Signature algorithm" identifies algorithms (cryptographic mechanism) used for QES.

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. CPE certificates are issued in accordance with the Policy of the provider that recorded in the attribute "Certificate Policy" of the certificate.

7.1.7 Indication of a QES Certificate

1. The Provider uses in the certificate with X.509 v.3 profile the attribute "Qualified Statements" with the identifier (OID) 0.4.0.1862.1, in accordance with specification ETSI TS 101 862.
2. The QES certificate is clearly indicated by the attribute "Certificate Policy", which is assigned an identifier (OID) of importance 1.3.6.1.4.1.15862.1.5.1.1.

7.2 Profile of the Certificates Revoked List

7.2.1 Version

1. The Provider, through its Certification Authorities, issues, publishes and maintains lists of revoked certificates (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, whose format is in accordance with international guidelines RFC 3280 Internet PKI Certificate and Certificate Revocation List (CRL) Profile.
2. Certification Authorities of the Provider issue, publish and maintain separate and complete CRLs and record therein only revoked certificates issued by the respective Authority.
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 Certification Authority that issued and signed the List;
- "Effective Date"/"This update" - the time of issue of the List;
- "Next Update" - the period of validity of the List. After that period, the Authority periodically issues a new list. During the period of validity, in the event of revocation/suspension of a certificate, the Authority immediately issues a new CRL;
- "Signature algorithm" - means the cryptographic mechanism/algorithm for digital 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 Authority that issued and signed the List. It contains the meaning of "subjectKeyIdentifier" from the certificate of the Authority that signed the List;

7.2.3 Format of an Element in CRL

1. The CRL of a Certification Authority shall contain all certificates revoked by the Authority. These elements are constant in the List.
2. The CRL of a Certification Authority shall contain an element for every certificate suspended by the Authority. Such an element in the List is temporary until the renewal of the certificate.
3. Attributes 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 Author;
- "ACompromise" - compromised private key of an operational Certification Authority of the Provider;
- "affiliationChange" - changed status of the Author to the Holder - changes in the power of attorney, revocation of power of attorney, termination of employment contract, etc.;
- "superseded" - the certificate is replaced with another;
- "certificateHold" - the certificate is temporarily suspended.

7.3 OCSP Profile

1. The Validation Authorities "B-Trust VA" and "B-Trust VA QES" of the Provider shall operate and provide the service "online check of certificate status in real time", in accordance with internationally agreed recommendation IETF RFC 2560 Internet PKI On-line Cerificate Status Protocol.
2. Information on the user's query and response when dealing with "B-Trust VA" and "B-Trust VA QES" 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 ZEDEP and regulations shall be implemented 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 person of the Provider, and the order and extent of such controls shall be consistent with the internal documents of the 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 - BANKSERVICE” AD shall appoint periodic checks for compliance of 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 Registration Authority/LRA.

8.2 Qualifications of the Inspectors

1. Inspectors may be only persons authorized to perform such functions in accordance with the requirements of accepted international practice and documents.

2. Inspectors shall comply with the requirements of Article 32, paragraph 2, item 4 of ZEDEP and Chapter Five of NDDUU, or shall be accredited by an international accreditation organization to perform such checks.

3. Internal checks on the work of the Registration Authority/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 express 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 governed by contract.

8.4 Scope of the Examination

1. Examination by the CRC shall cover the statutory requirements to the Provider’s activity under ZEDEP.

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 Guide with their practical implementation in the performance of activities;
- checking the activities of subcontractors (external Registration Authorities/LRAs;
- other circumstances, facts and activities relating to the infrastructure of B-Trust, 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 to remedy the deficiencies and inconsistencies.

3. The staff of the Provider shall take specific remedial action within the specified period.

4. The results of the examination shall be preserved in the archives of the Provider.

9 OTHER BUSINESS CONDITIONS AND LEGAL ASPECTS

9.1 Prices and Fees

1. The Provider shallmaintain 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 Holder by posting the changes on the website.
3. Changes shall be effective for the respective Holder on the day following publication.
4. Within 5 (five) days from the date of the change as far as an increase in the price has occurred, the Holder 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 recoverable.
5. In the absence of notice of termination, it is considered that the Holder 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 of the certificate;
- fee for renewal of certificate;
- fee for consultation and technical assistance provided upon application of the Holder;
- price for equipment purchased or leased from 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 - BANKSERVICE" 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 Holder 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 Author/Holder in relation to services provided by the Provider. These shall be payable entirely by the Holder 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 the transfer of amounts due on account of the Provider, including those in correspondent banks shall be charged to the Client.

9.1.2 Fees for Certification, Cryptographic, Information and Consultancy Services

1. Services to provide and use electronic signature certificates and related services shall be paid when ordering the respective 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 advice for building and maintaining infrastructure and information security solutions shall be based on "man hours" and paid based on a bilateral protocol signed for the work performed. The prices of the hourly rate in the annexed 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 "Time Verification" 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 Holder shall be governed by general rules of the Sale Contract or, respectively, the Lease Contract.

6. If payments are delayed after the agreed period, the Customer shall owe the Provider legal interest for the period until final payment of amounts due.
7. 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 paper and courier costs shall be charged.

9.1.3 Invoicing

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

9.1.4 Return of Certificate and Recovery of Payment

1. An Author/Holder can object to the inaccuracy or incompleteness in the contents of a certificate within 3 days after its publication in the Public Register.
2. If the cause of a false content of a certificate lies with the Registration Authority/LRA, the Provider shall terminate and issue a new certificate with the correct content at their own expense, or shall recover the amount for the terminated certificate containing such false information.
3. If the cause of a false content of a certificate lies with the Author/Holder, the Provider shall terminate the certificate and shall not recover the payment. The Provider may issue a new certificate with correct content, to the User's expense.
4. The User can refuse a QES certificate with true content, and the Provider shall terminate it immediately, without recovering the payment for this 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 certificate of an Author/Holder 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 CSP 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 its activities in accordance with ZEDEP and NDDUU.
4. The Provider shall take a compulsory insurance in the amounts referred to in Art. 14, paragraph 1 of NDDUU:
5. The compulsory insurance shall cover the liability of the Provider to Holders, respectively Trusting Parties for material and non-material damage suffered, to the limits specified in ZEDEP and NDDUU.
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 an Author/Holder shall not exceed the amount established by NDDUU.
2. The insurance shall not cover cases of waiver of responsibility, in particular for damages caused by:

- non-compliance of Authors/Holders of certificates;
- compromise or loss of private key of the Author, as a result of improper care or use;
- non-compliance with requirements to verify the validity of electronic signature and the certificate by the Trusting 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 Authors/Holders 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. Confidential information considered can not 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 the data and shall be revealed with the explicit permission of the Author/Holder, except where the Provider is obliged by Law.
6. No one except the Author may use the private key for creating an electronic signature. The Provider recommends the Author not expose the user access code to a B-Trust SSCD, 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 Authors/Holders 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 Authors/Holders that have become known to it in the performance of its business as a CSP.
3. According to the approved policy of the QES certificates, elements of information therein may contain personal information of Authors and Holders. 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 ZEDEP, the Provider shall publish each certificate and provide access to third parties, as instructed by the Author/Holder.

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 tangible and intangible rights.
2. Relations on the occasion of these rights between the Provider and other participants in the infrastructure of B-Trust, such as external Registration Authorities, LRAs, etc. shall be governed 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 (eg, B-Trust®), and on trade names used by the Holder and contained in the certificates, shall be retained by their respective holders 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 infrastructure of B-Trust, 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 media 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 ZEDEP and regulations on the activities of registered CSPs.
2. The Provider operates the activity of a registered CSP 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 digital signature device in its infrastructure;
- issuing certificates after verifying submitted information by means permitted by Law;
- storing and maintaining information relating to the issued certificates and interoperability of systems;
- complying with established operating procedures and rules for technical and physical control, in accordance with the terms in this document;
- upon application, issues the appropriate types of certificates, 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 certificate;
- performing revocation and suspension of certificates under the terms and conditions of the respective Policy;
- immediately notifying the Holder and Author 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 for preserving the confidentiality of data disclosed to it 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 certificate upon its expiration;
- informing Authors, Holders 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 ZEDEP 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 it to carry out its activities;
- insuring for the duration of its activity for damages arising from breach of its obligations under ZEDEP, 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 certificates, an updated CRL and other circumstances and electronic documents, in accordance with this document and ZEDEP;
- providing non-stop 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 certificates;
- creating conditions for each Trusting Party to check the status of a certificate issued and published in the Public Register of certificates.

3. The Provider shall be responsible before the Author/Holder and Trusting Party for:

- its obligations under the preceding paragraph;
- any incorrect or missing data in a certificate due to fault of its own;
- any omissions in establishing the identity of the applicant.

9.6.2 Responsibility and Guarantees of the Registration Authority/LRA

1. The Provider shall ensure that Registration Authority/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 Registration Authority/LRA in the infrastructure of B-Trust.

9.6.3 Responsibility of the Author/Holder

1. The Author/Holder shall:

- follow precisely the conditions and procedures of this document and the relevant Policy upon application for the issuance of certificate and use of other supporting 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 NIAKEP when generating the key pair;
- notify Provider immediately in case of compromise or suspected compromise of the private key by sending an application 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 Guide. Any use of the private key shall be considered to be an act committed by the Holder;
- accept the certificate for electronic signature immediately after it is presented by the Provider;

- verify the completeness and accuracy of the contents of the certificate within three (3) days of 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 apply 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 SSCD, before using the certificate;
- use their certificates issued using licensed cryptographic software only;
- use a certificate only in accordance with its intended purpose and use it 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 Trusting Party of the care and responsibility required from the latter when relying the QES certificate;
- accept the conditions of care and responsibility when relying the QES certificate, in the event that they act as a Trusting Party.

2. The Author/Holder 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 will regress to the Author/Holder 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 NIAKEP;
- 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 at issue when the Author was not authorized to hold the private key corresponding to the public key in the certificate;
- has accepted the certificate at issue by making false statements to the Provider relating to the certificate;
- has accepted the certificate when the Author was not authorized to apply for the issuance of the certificate.

9.6.4 Care and Responsibility of the Trusting Party

1. Persons who rely on electronic signature certificates 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 Trusting 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 borne by the Trusting Party;
- verifying the validity of electronic signatures in electronically signed statements, and validity of electronic signature of a chain of certificates to the basic 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 Trusting 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 Trusting 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 determined;
- authenticity and validity of the certificate at the time of signature is reliably verified;
- results of the verification of electronic identity of the Author/Holder are presented correctly;
- any changes relevant to security are identifiable.

4. The Provider shall not be held liable for any damages to the Trusting 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 QES certificates, 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 Author/Holder, 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 Trusting 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 moral 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, it may bring a claim against the Holder.
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. Outside 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 Authors, Holders or Relying Parties;
- for early revocation and suspension of certificates and/or for checks of the status of certificates for reasons beyond his control (e.g. lack of due diligence on the part of the Trusting Party, fraudulent action by Authors or Holders, telecommunication and power interference, etc.).
8. The Provider shall not be held liable for any damages caused by use of a QES certificate beyond the scope of its intended uses and applicable restrictions.

9.8 Limitation of Liability of the Provider

1. For the QES certificates issued, the Provider shall be held liable within the following limits:

Types of Certificates	Maximum Limit of Liability /BGN/
B-Trust Personal Certificate QES	40,000
B-Trust Professional Certificate QES	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 ZEDEP.

9.9 Compensation for the Provider

1. For all cases of non-performance by the Author/Holder, the Provider shall seek responsibility from the Author/Holder 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 registry of public documents.
2. Contract for Certification Services between the Provider and the User shall have a period of three years or until the expiration date of the last certificate issued under said Contract.
3. With the cessation of the Provider, the provisions, Policy and Practice contained in this document shall terminate.
4. In the event of invalidity of any individual clauses of this document, the validity of the document as a whole 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 have a period of one year or until the expiration date of the last certificate issued under said Contract.
6. Provider shall keep proper and safe 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 Registration Authority/LRA and electronic notices published on its website.
2. Users of the infrastructure of B-Trust shall send messages, letters, recommendations, questions and complains to the Provider using the following contact address:

Mailing address: 1612 Sofia, 41"Tzar Boris III" Blvd.
Phone: 02 / 92 15 100
Fax: 02 / 981 45 18
e-mail address: info@b-trust.org

3. In case of receiving a complaint the Provider conducts 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.

4. Changes shall be communicated to the CRC and stakeholders.

5. Any person may make suggestions for changes (structural and content-wise), and for 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 ZEDEP and current regulations.

CERTIFICATION PRACTICE STATEMENT - PART II:

POLICY

IN PROVIDING CERTIFICATES

AND SUPPORTING SERVICES FOR

QUALIFIED ELECTRONIC SIGNATURES

1. Policy of providing certificates and certification services is a document that is an integral part of the Certification Practice Statement. It describes the policies and procedures followed by the Provider in issuing of QES certificates, types of certification services applicable to such certificates, and their scope.

2. Policy defines the manner and level of security for identification of the Author/Holder, procedures for the issuance, maintenance and management of the certificate, required security level of SSCDs 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 QES certificates, issued, maintained and managed by "BORICA - BANKSERVICE" AD as a registered CSP:

- QES certificates with policy identifier OID = 1.3.6.1.4.1.15862.1.5.1.1;

4. General requirements and responsibilities of the Provider, Author/Holder and due diligence of each Trusting Party using the QES certificates are outlined in Part I (Practice) of this Manual.

5. General Procedures for suspension, renewal and revocation of valid QES certificate are contained in Part I (Practice) of this Manual.

6. Prices of certificates and services for issuing and maintaining QES certificates are contained in the Provider's Price List, available on its website.

10 POLICY FOR ISSUING, MAINTENANCE AND MANAGEMENT OF A PERSONAL CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE

10.1 General Characteristics of the Certificate

1. Personal certificate "B-Trust Personal Certificate QES" is issued to an Author/Holder - individual and certifies the electronic identity of the Author/Holder and his/her relationship with the public key.
2. "B-Trust Personal Certificate QES" has the character of a QES certificate within the meaning of Art. 16 para. ZEDEP 1.
3. For issuing of a certificate "B-Trust Personal Certificate QES", the Author/Holder or his/her representative needs to be present in person before the Registration Authority/LRA of the Provider, for verification of their identity.
4. Identification procedures include proof of identity of the Author and of the Holder.
5. Examination of the application for a personal certificate under sections 3 and 4 provides a high level of certainty regarding the identity of the Author/Holder and their relationship with the public key.
6. Author/Holder can generate a key pair using the B-Trust SSCD and dedicated software, or other equivalent SSCD, compatible with the Provider’s infrastructure.
7. Private key for the issuing of QES must be generated in SSCD and can not be derived out of it.
8. An issued personal QES certificate, certifying a public key that corresponds to a private key, is recorded in the SSCD, which is then provided to the Author/Holder.
9. The Provider reserves the right to add additional attributes to the personal QES certificate, if necessary.

10.2 Purpose and Applicability of the Certificate

1. A personal certificate can be used when creating/laying the QES of an individual identified as the Author in the certificate to sign electronic documents and use software applications that require high levels of information security.
2. Trusting 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. Trusting Party should check the policy indicated in the QES certificate 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 accepting the electronic signature.

10.3 Designation of the Policy

1. The Provider maintains and implements a common policy designated in the personal QES certificate "B-Trust Personal Certificate QES" with a policy identifier OID = 1.3.6.1.4.1.15862.1.5.1.1.

10.4 Profile of the Certificate

1. The Provider shall issue a personal QES certificate with the profile specified below:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha1RSA / Sha256RSA
Signature hash algorithm	-	Sha1 / Sha256
Issuer	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Full name of Author]
	E =	[E-mail address]
	OU =	EGN/PID: [EGN/PID of Author] (if any)
	OU =	Personal certificate [– UES]

	S =	[[Address of Author], PK:[Postal Code],]* EGN/PID:[EGN/PID of Author] (if any)
	C=	BG
Subject Alternative Name*	CN =	FID: [Number of identity document of foreigner - Author]
	C =	[Country code of identity document of foreigner – Author]
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[hash of „Subject"]

Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a
		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1]*
Enhanced Key Usage	-	Client Authentication, Secure Email, IP security (end system, tunnel termination, end user, IKE)
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment, Data Encipherment, Key Agreement

Qualified Statement	QStatement:	StatementId = (1)
		statementInfo = 0.4.0.1862.1
		StatementId =(4)
		StatementInfo=qcSSCD (0.4.0.1862.1.4)

* Fields marked with an asterisk may not appear in the certificate

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

1. Operational procedures for issuing, renewal and management of a personal QES certificate "B-Trust Personal Certificate QES" are described in Chapter 12 of this document.

11 POLICY OF ISSUING, MAINTENANCE AND MANAGEMENT OF A PROFESSIONAL CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE

11.1 General Characteristics of the Certificate

1. Professional Certificate "B-Trust Professionall Certificate QES" is issued to a Holder, respectively, to an individual Author, authorized as such by the Holder, and certifies the electronic identity of the Holder and the Authors, as well as the link of the Author/Holder with their public key issued for the certificate.
2. "B-Trust Professional Certificate QES" has the character of a QES certificate within the meaning of Art. 16 paragraph 1 of ZEDEP and every electronic signature.
3. For issuing of a certificate "B-Trust Professional Certificate QES", the Author/Holder or his/her representative needs to be present in person before the Registration Authority/LRA of the Provider, for verification of their identity.
4. Identification procedures include proof of identity of the Author and of the Holder.
5. Examination of the application for a professional certificate under sections 3 and 4 provides high level of certainty regarding the identity of the Author/Holder and their relationship with the public key.
6. Author/Holder can generate a key pair using the B-Trust SSCD and dedicated software, or other equivalent SSCD, compatible with the Provider's infrastructure.
7. Private key for issuing of QES must be generated in SSCD and can not be derived out of it.
8. An issued professional QES certificate, certifying a public key that corresponds to a private key is recorded in the SSCD, which is then provided to the Author/Holder.
9. Provider reserves the right to add additional attributes to the professional QES certificate, if necessary.

11.2 Purpose and Applicability of the Certificate

4. A professional certificate can be used when creating/laying the QES of an individual identified as the Author in the certificate and authorized to sign to electronic documents on behalf of the Holder and use applications that require high levels of information security.
5. Trusting 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 the signature, when relying an electronic signature accompanied by such certificate.
6. Trusting Party should check the policy indicated in the QES certificate 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 accepting the electronic signature.

11.3 Designation of the Policy

1. Provider shall maintain and implement a common Policy for the professional QES certificate marked "B-Trust Professionall Certificate QES" with the policy identifier OID = 1.3.6.1.4.1.15862.1.5.1.1.

11.4 Profile of the Certificate

1. The Provider shall issue a professional QES certificate with the profile specified below:

Field	Attributes	Meaning/Value
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha1RSA / Sha256RSA
Signature hash algorithm	-	Sha1 / Sha256
Issuer	Phone =	+359 2 9 215 100
	E =	ca5qes@b-trust.org
	PostalCode =	1784
	STREET=	Bul. Tsarigradsko shoes No 117
	CN =	B-Trust Operational CA QES
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	S =	Sofia
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Full names of Author]
	O =	[Name/Full names of Holder]
	OU =	BULSTAT: [UIC(BULSTAT) of Holder] (if any)

	OU* =	EGN/PID: [EGN/PID of Holder] (if any)
	S =	[[Business address of Author at Holder], PK:[Postal Code],]* EGN/PID:[EGN/PID of Author] (if any)
	OU =	Professional certificate – UES
	E =	[E-mail address]
	C =	BG
Public key	-	RSA(2048 bits)
Subject Alternative Name*	CN* =	FID: [Foreigner’s identity document – Author]
	C* =	[Country code of Foreigner’s identity document – Author]
	OU* =	C:[Country code of country of registration of foreigner – Holder]
	OU* =	SR:[Court registration number of foreigner - Holder]
Subject Key Identifier	-	[Hash of „Subject"]

Authority Key Identifier	KeyID =	f2 37 77 e8 47 fa e9 1e 12 82 d5 b9 d7 72 70 a9 66 0f bd 8a
		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.5.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/ca5/cps [[2]Certificate Policy: Policy Identifier=0.4.0.1456.1.1]*
Enhanced Key Usage	-	Client Authentication, Secure Email, IP security (end system, tunnel termination, end user, IKE)
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5qes/crl/b-trust_ca5qes_oper.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: http://ocsp.b-trust.org
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment, Data Encipherment, Key Agreement

Qualified Statement	QStatement:	statementId = (1)
		statementInfo = 0.4.0.1862.1
		StatementId =(4)
		StatementInfo=qcSSCD (0.4.0.1862.1.4)

* Fields marked with an asterisk may not appear in the certificate

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

1. Operational procedures for issuing, renewal and management of a professional QES certificate "B-Trust Professional Certificate QES" are described in Chapter 12 of this document.

12 OPERATING PROCEDURES FOR ISSUING, RENEWAL AND MAINTENANCE/MANAGEMENT OF QES CERTIFICATES

1. Operational procedures of the Provider for issuing, renewal and maintenance/management of personal and professional QES certificates are common for three types of certificates.

12.1 Registration of an Application for Certificate

1. Applicant for a QES certificate files an application with the Registration Authority/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 ZEDEP, individualizing the Author/Holder 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 Author/Holder.
3. Application process then requires that the applicant (Author/Holder or his/her representative) or the operator of the Registration Authority/LRA generate a cryptographic (RSA) key pair and include the public key information in the certificate.
4. The pair of cryptographic keys must be generated in the B-Trust SSCD or other equivalent SSCD that meets the requirements for security level EAL 4 or higher, according to SC or other specifications defining equivalent levels of security.
5. The electronic format of the application for issuing of certificate, together with information that will be included in the certificate, is a structure and shall be signed with the private key of the key pair generated in the SSCD.
6. If the applicant does not possess a B-Trust SSCD, the application process for a certificate shall only require information identifying the Author/Holder, the type of certificate (personal or professional), and other additional information, not including the generation of a cryptographic key pair (RSA) for the certificate. Generation of the key pair as a step in the application for a certificate is executed by an operator in the LRA.
7. Upon successful registration of an application for issuing of a certificate, the operator in the LRA must establish the identity of the applicant.

12.2 Identification and Acceptance/Rejection of the Application

1. The applicant should be familiar with the list of documents required for issuing of a QES certificate selected by him, including the proposed type of contract for certification services.
2. Applicant shall properly fill in the required documents from the list.
3. Applicant must personally appear at a LRA of his choice and present the prepared documents.
4. Operator at the Registration Authority/LRA shall perform the procedure of identification and authentication of the applicant for issuing of a certificate - Author/Holder or authorized individual.
5. In accordance with the Manual - Part I (PRACTICE) and established internal procedures of the Provider, based on a received and registered the application for a QES certificate and documents submitted in the applicant's presence - Author/Holder or his/her representative, - Registration Authority/LRA confirms before the Provider:

- the identity of the Holder, respectively, of the Author;
- representative power of the Author to the Holder and of the authorized person to the Holder;
- possession of the private key corresponding to the public key given 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 of this Guide.

6. Registration Authority/LRA of the Provider, in the presence of the applicant - Author/Holder 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 certification.
7. Based on the approved application for issuance, the Certification Authority 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 with reasons for refusing the application.

12.3 Issuing and Publication of the Certificate

1. Certification Authority of the Provider identifies by electronic means the Registration Authority/LRA that has approved the electronic application for issuance of a QES certificate.
2. Certification Authority generates the requested certificate, signs it with the digital signature of the Provider and publishes it in its Public Register.

3. Notification Authority of the Provider sends notification to the Author/Holder containing the name of the Author/Holder of the QES certificate, a unique serial number and the term of validity of the certificate issued.

12.4 Acceptance of the Certificate

1. Acceptance of the certificate is an act that is performed prior to issuing and publication by the Provider through the operational Certification Authority.
2. Provider, through the operational Certification Authority, shall publish the certificate issued in the Public Register of issued certificates.
3. Following publication of the certificate, the Author/Holder is required within 3 (three) days of the publication to review the contents of the certificate and, if necessary, make objections to the Provider or the Registration Authority/LRA concerning the correctness and completeness of its contents.
4. Upon objection made under the preceding item, Provider shall immediately cease 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 the certificate, operator of the Registration Authority/LRA of the Provider may immediately record it on the B-Trust SSCD, which is transferred to the Author/Holder (or an authorized person). If the key pair is to be generated in a SSCD with the applicant, the operator notifies him/her via the e-mail address contained in his/her certificate, stating the website where it can the certificate issued can be downloaded.
2. Upon presentation of an identity document, Author/Holder (or authorized person) receives the QES kit issued on a B-Trust SSCD.

12.6 Renewal of the Certificate

1. Renewal of a QES certificate is performed by the Provider in accordance with the general operating procedure for the renewal of certificates described in the Manual - Part I (PRACTICE).

12.7 Suspending/Resuming the Certificate

1. Suspending/resuming the QES certificate is performed by the Provider, in accordance with the general operating procedure for Resuming a Certificate described in the Manual - Part I (PRACTICE).

12.8 Revocation of the Certificate

1. Revocation of a QES certificate is executed by the Provider, in accordance with the general operating procedure for revocation of a certificate described in the Manual - Part I (PRACTICE).