



CERTIFICATE POLICY

**FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE,
CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL,
AND CLOUD QUALIFIED ELECTRONIC SEAL
BY BORICA AD**

(B-Trust QCP-eIDAS QES/CQES/QESeal/CQESeal)

Version 8.0

Effective from 1 March 2026

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

Document history				
Version	Author(s)	Date	Status	Comment
4.0	Dimitar Nikolov	20.05.2018	Approved	Separating the document from the common document Policy and Practice Statement. Adding Policies on the provision of qualified certificates for qualified electronic seal and cloud qualified electronic signature.
5.0	Dimitar Nikolov	01.04.2019	Approved	Technical corrections
6.0	Dimitar Nikolov	01.03.2020	Approved	Technical corrections
6.1	Margarita Boneva	01.07.2021	Approved	Technical corrections
7.0	Margarita Boneva	10.03.2023	Approved	Additions
8.0	Margarita Boneva	01.06.2026	Approved	Additions

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

CONTENTS

LIST OF ACRONYMS AND TERMS	5
COMPLIANCE AND USE	6
INTRODUCTION	8
This Policy:	8
1 GENERAL CHARACTERISTICS OF THE CERTIFICATES	9
1.1 B-Trust Personal Qualified Certificate QES	9
1.2 B-Trust Personal Qualified Certificate Cloud QES	9
1.3 B-Trust Professional Qualified Certificate QES	10
1.4 B-Trust Professional Qualified Certificate Cloud QES	10
1.5 B-Trust Qualified Certificate QESeal	11
1.6 B-Trust Qualified Certificate Cloud QESeal	11
1.7 Policy Identifiers	12
1.7.1 B-Trust Personal QC QES and Personal QC Cloud QES – Policy identification	12
1.7.2 B-Trust Professional QC QES and Professional QC Cloud QES – Policy identification	12
1.7.3 B-Trust QC QESeal and QC Cloud QESeal – Policy identification	13
1.8 Designation and applicability of the certificates	13
1.8.1 B-Trust Personal QC QES and Personal QC Cloud QES	13
1.8.2 B-Trust Professional QC QES and Professional QC Cloud QES	13
1.8.3 B-Trust Organization QC QESeal and QC Cloud QESeal	14
1.9 Key Pair Generation	14
1.10 Limitation of authentication action	14
1.11 Use of certificates outside the scope and restrictions	15
1.12 Management of the Provider Policy	15
2 CERTIFICATE PROFILES	15
2.1 Profile of B-Trust Personal QC QES and Personal QC Cloud QES	15
2.2 Profile of B-Trust Professional QC QES and Professional QC Cloud QES	17
2.3 Profile of B-Trust Organization QC QESeal and QC Cloud QESeal	18
3 PUBLICATION AND REGISTRATION RESPONSIBILITIES	20
3.1 Public Register	20
3.2 Public Repository	20
3.3 Publication of Certification Information	20
3.4 Frequency of Publication	20
3.5 Access to the Register and Repository	20
4 IDENTIFICATION AND AUTHENTICATION	20
4.1 Naming 20	20
4.2 Initial identification and authentication	20
4.3 Identification and authentication for certificate renewal	20
4.4 Identification and authentication for suspension	20
4.5 Identification and authentication for revocation	20
4.6 Identification and authentication after revocation	20
5 OPERATIONAL REQUIREMENTS AND PROCEDURES	21
5.1 Certificate Request	21
5.2 Certificate issuance procedure	21
5.3 Certificate issuance	21
5.4 Certificate acceptance and publication	21
5.5 Key pair and certificate usage	21
5.6 Certificate renewal	21
5.7 Certificate renewal with the generation of a new key pair (re-key)	21
5.8 Certificate modification	21
5.9 Certificate suspension and revocation	22
5.10 Certificate status	22
5.11 Termination of a Certification Services Contract	22
5.12 Key recovery	22
6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	22
6.1 Physical controls	22
6.2 Procedural controls	22
6.3 Staff qualification and training	22

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

6.4	Logging procedures	22
6.5	Archiving	22
6.6	Key changeover	22
6.7	Compromise and disaster recovery	22
6.8	Compromise of a Private Key	22
6.9	Provider Termination	23
7	TECHNICAL SECURITY CONTROL AND MANAGEMENT	23
7.1	Key Pair Generation and Installation	23
7.2	Generation Procedure	23
7.3	Private Key Protection and Cryptographic Module Engineering Controls	23
7.4	Other Aspects of Key Pair Management	23
7.5	Activation Data	23
7.6	Security of Computer Systems	23
7.7	Development and Operation (Life Cycle)	23
7.8	Additional Tests	23
7.9	Network Security	23
7.10	Verification of Time	23
8	INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES	24
8.1	Periodic and Circumstantial Inspection	24
8.2	Qualifications of the Inspectors	24
8.3	Relationship of the Inspecting Persons with the Provider	24
8.4	Scope of the Inspection	24
8.5	Discussion of Results and Follow-Up Actions	24
9	BUSINESS AND LEGAL ISSUES	24
9.1	Prices and fees	24
9.2	Financial liability	24
9.3	Confidentiality of business information	24
9.4	Personal data protection	24
9.5	Intellectual property rights	24
9.6	Responsibility and warranties	24
9.7	Disclaimers of warranties	25
9.8	Limitation of liability of the Provider	25
9.9	Indemnities for the Provider	25
9.10	Term and termination	25
9.11	Notices and communication with participants	25
9.12	Amendments to the document	25
9.13	Dispute settlement (jurisdiction)	25
9.14	Governing law	25
9.15	Compliance with applicable law	25

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

LIST OF ACRONYMS AND TERMS

AES	Advanced Electronic Signature
AESeal	Advanced Electronic Seal
BG	Bulgaria
RQSCD	Server component in the cloud QES platform of B-Trust for secure remote signature creation
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRC	Communications Regulation Commission
CQES	Cloud Qualified Electronic Signature
CQESeal	Cloud Qualified Electronic Seal
EDE TSA	Electronic Document and Electronic Trust Services Act
ETSI	European Telecommunications Standards Institute
EU	European Union
HSM	Hardware Security Module
IEC	International Electro-technical Commission
ISO	International Standardization Organization
IP	Internet Protocol
LRA	Local Registration Authority
OID	Object Identifier
OCSP	On-line Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QC	Qualified Certificate
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
RA	Registration Authority
RA-VI	Registration Authority using remote video identification
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SAM	Signature Activation Module
SCT	Signature Creation Token (PKCS#12)
SSL	Secure Socket Layer
URL	Uniform Resource Locator
Website	A collection of related web pages, including multimedia content, typically identified with a common domain name (DN), and published on at least one web server.

COMPLIANCE AND USE

This Document:

- Has been prepared by "BORICA" AD (hereinafter BORICA), a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- **Is effective from 1.03.2026;**
- Is entitled: "Certificate Policy for Providing Qualified Certificates for Qualified Electronic Signature, Cloud Qualified Electronic Signature and Qualified Electronic Seal (B-Trust CP-eIDAS QES/CQES/QESeal/CQESeal)";
- Is associated with the published current version of the document „Certification Practice Statement for qualified certificates and qualified trust services of BORICA (B-Trust CPS-eIDAS)“, which contains the general conditions and requirements for the procedures of authentication, QC issuance and maintenance, and the security level requirements for generating and storing the private key for these certificates;
- The document has been developed in accordance with the formal requirements for content, structure and scope, as set out in international guideline RFC 3647, including the sections that are specific and applicable to the Qualified Certificates described in the document;
- Constitutes the General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These conditions are part of the written Certification Services Contract, which is concluded between the Provider and Users. The contract may contain special conditions that take precedence over the general conditions in this document;
- Is a public document with the purpose to establish the conformity of the activity of the Provider BORICA with the EDE TSA and the legal framework;
- is publicly available at any time on the Provider's website: <https://www.b-trust.bg/documents>;
- May be changed by the QTSP and each new version shall be published on the Provider's website.

This document is prepared in compliance with:

- Electronic Document and Electronic Trust Services Act (EDE TSA);
- Ordinance on the Activities of Trust Service Providers;
- Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature;
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183. The content and structure of this document is in accordance with Regulation (EU) No 910/2014 and refers to the information contained in the following ratified international guidelines, specifications and standards:
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1,2,3 and 5: Certificate Profiles;

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

- ETSI EN 419 241, part 2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- ETSI EN 419 241, part 3 – Trustworthy Systems Supporting Server Signing – Part 3: Protection profile for Signature Activation Data management and Signature Activation Protocol (PP-SAD+SAP);
- ETSI EN 419 221-5 - Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.
- ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates;
-

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

41 “Tsar Boris III” Blvd.
1612 Sofia
BORICA AD
Tel.: 0700 199 10
E-mail: info@b-trust.org
Official Web site: www.b-trust.bg

INTRODUCTION

This Policy:

- Refers only to the qualified certificates for qualified electronic signature, cloud qualified electronic signature, qualified electronic seal, and cloud qualified electronic seal issued by BORICA in compliance with Regulation (EU) № 910/2014 and the applicable legislation of the Republic of Bulgaria;
- Describes the specific conditions and requirements that the Provider achieves when issuing and maintaining QC for QES, QC for CQES, QC for QESeal, and QC for CQESeal, and their applicability with respect to security level and restrictions in their use;
- Determines the technical profiles and content of the QCs;
- Is implemented through common technical procedures and meets the security requirements for generating and storing the private key corresponding to a public key in the certificates specified in the Certification Practice Statement of the Provider (B-Trust CPS-eIDAS document);
- Determines the relevance and the degree of trust in the certified facts in the QCs.

It is assumed that a User who uses this document has the knowledge and understanding of public key infrastructure, website certificates and concepts, website authentication, and SSL/TLS protocol. Otherwise it is recommended that he/she become acquainted with these concepts and with the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA (B-Trust CPS-eIDAS)" before using this document. In any case, this document (Certificate Policy) should be used together with the Certification Practice Statement of the Provider.

The B-Trust® public key (PKI) infrastructure of BORICA is built and functions in compliance with the legal framework of Regulation (EU) № 910/2014, and the EDE TSA, and with the international specifications and standards ETSI EN 319 411-1/5 and ETSI EN 319 412.

The Provider uses OID in the B-Trust PKI infrastructure, formed on the basis of code 15862, assigned to BORICA by IANA in the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA Registered Private Enterprise) and in accordance with ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).

BORICA has informed the CRC about the start of activity as a QTSP under the EDE TSA and current legislation. The Provider notifies the Users of its accreditation for providing QCs specified in this document.

The accreditation of "BORICA" AD as a QTSP under the EDE TSA aims to achieve the highest security level of QCs provided and better synchronization of these activities with similar activities provided in other Member States of the European Union.

Regarding relations with Users and third parties, only the current version of the Policy at the time of using QCs for qualified electronic signature, cloud qualified electronic signature, qualified electronic seal, and cloud qualified electronic seal issued by BORICA is valid.

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

1 GENERAL CHARACTERISTICS OF THE CERTIFICATES

Pursuant to this Policy, the QTSP BORICA issues and maintains the following types of qualified certificates:

- B-Trust Personal qualified certificate QES
- B-Trust Personal qualified certificate CQES
- B-Trust Professional qualified certificate QES
- B-Trust Professional qualified certificate CQES
- B-Trust Organization qualified certificate QESeal
- B-Trust Organization qualified certificate CQESeal

These certificates have the status of qualified certificates for qualified electronic signature/seal within the meaning of Regulation 910/2014.

1.1 B-Trust Personal Qualified Certificate QES

1. The certificate for electronic signature, issued under this Policy has the status of a QC for QES within the meaning of the Regulation.
2. A Personal Qualified Certificate for QES is issued to a natural person – QES Signatory and certifies the Signatory's electronic identity and the relation of the Signatory with his public key in the certificate.
3. For the issuance of this certificate, personal presence of the Signatory or an authorized person is required at the RA/LRA for identity verification. Authentication of the Signatory's identity can also be done by means of electronic/remote identification.
4. The identification procedure includes proofs of identity of the Signatory and their verification.
5. The verification of the request for issuance of Personal qualified certificate for QES is done in the order of the above items and provides the highest level of security regarding the Signatory's identity and his relationship with the public key.
6. The Signatory may himself generate the key pair using B-Trust QSCD and the relevant software or other QSCD that is compatible with the Provider's infrastructure.
7. The private key for creating Personal QC for QES is mandatorily generated in the QSCD and cannot be taken out of it.
8. The issued Personal QC for QES certifying a public key corresponding to the private key is mandatorily recorded on a QSCD and is provided to the Signatory.
9. The Provider reserves the right to add, if necessary, additional attributes to the Personal QC for QES.

1.2 B-Trust Personal Qualified Certificate Cloud QES

1. The certificate for cloud electronic signature, issued under this Policy has the status of a QC within the meaning of the Regulation 910/2014.
2. A personal Qualified Certificate for Cloud QES is issued to a natural person – Signatory of the Cloud QES and certifies the Signatory's electronic identity and the relation of the Signatory with his public key in the certificate.
3. For the issuance of this certificate, the personal presence of the Signatory or an authorized person is required at the RA/LRA for identity verification. Authentication of the Signatory's identity can also be done by be done by means of electronic/remote identification.
4. The identification procedure includes proofs of identity of the Signatory, the ownership of the smart device with the mobile application for Cloud QES, which is registered in the user account of the Signatory, and their verification.
5. The verification of the request for issuance Personal Qualified Certificate for Cloud QES is done in the order of the above items and provides the highest level of security regarding the Signatory's identity, his relation with the public key, and his personal control on the access to the private key and the data for activation of the signature.
6. The Signatory generates the key pair at the Provider using an RQSCD in the cloud QES platform, and the relevant software supporting SAD/SAP/SAM scheme for secure remote personal control over the private

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

key of the Cloud QES.

7. The private key for creating a Personal QC for Cloud QES is secured in the Cloud QES platform via validated cryptographic schemes with security level equivalent to a B-Trust QSCD.
8. The issued Personal QC for Cloud QES certifying a public key corresponding to the private key is not provided to the Signatory, but it is published in the Public register of the Provider and is available for validity check.
9. The Provider reserves the right to add, if necessary, additional attributes to the Personal QC for Cloud QES.

1.3 B-Trust Professional Qualified Certificate QES

1. The certificate for electronic signature issued under this Policy has the status of a qualified certificate for QES within the meaning of the Regulation 910/2014.
2. A Professional Qualified Certificate for QES is issued to a Signatory – a natural person who is associated with a legal person and certifies the Signatory's electronic identity and the relationship of the Signatory with his public key in the certificate.
3. For the issuance of this certificate, personal presence of the Signatory or an authorized person is required at the RA/LRA for identity verification. Authentication of the Signatory's identity can also be done by means of electronic/remote identification.
4. The identification procedure includes proofs of the identity of the Signatory and their verification, proof that at the time of the request for issuance the legal entity exists and that the Signatory has received authorization to represent the legal entity, as well as their verification.
5. The verification of the request for issuance of Professional qualified certificate for QES is done in the order of the above items and provides the highest level of security regarding the Signatory's identity and his relationship with the public key.
6. The Signatory may himself generate the key pair using a B-Trust QSCD and the relevant software or other QSCD that is compatible with the Provider's infrastructure.
7. In the request for issuance of Professional qualified certificate for QES to a natural person associated with a legal person, the person representing the Signatory is also specified. The identity of that person is also verified.
8. The private key for creating QES is mandatorily generated in the QSCD and cannot be taken out of it.
9. The issued Professional Qualified Certificate for QES to a natural person associated with a legal person, certifying a public key corresponding to the private key, is mandatorily recorded on a QSCD and is provided to the Signatory.
10. The Provider reserves the right to add, if necessary, additional attributes to the Personal Qualified Certificate for QES.

1.4 B-Trust Professional Qualified Certificate Cloud QES

1. The certificate for cloud electronic signature, issued under this Policy has the status of a QC within the meaning of the Regulation 910/2014.
2. A Professional Qualified Certificate for Cloud QES is issued to a User- Signatory – a natural person who is associated with a legal person and certifies the Signatory's electronic identity and the relationship of the Signatory with his public key in the certificate.
3. For the issuance of this certificate, the personal presence of the Signatory or an authorized person is required at the RA/LRA for identity verification. Authentication of the Signatory's identity can also be done by be done by means of electronic/remote identification.
4. The identification procedure includes proofs of the identity of the User- Signatory, the ownership of the smartphone with the Cloud QES mobile application, which is registered in the User's account, and their verification, proof that at the time of the request for issuance the legal entity exists and that the Signatory has received authorization to represent the legal entity, as well as their verification.
5. The verification of the request for issuance of a Professional Qualified Certificate Cloud QES is done in the order of the above items and provides the highest level of security regarding the User- Signatory's identity,

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

his relation with the public key, and his personal control on the access to the private key and the data for activation of the signature.

6. The Signatory generates the key pair at the Provider using RQSCD in the Cloud QES platform, and the relevant software supporting SAD/SAP/SAM scheme for secure remote personal control over the private key of the Cloud QES.
7. In the request for issuing Professional Qualified Certificate for Cloud QES to a natural person associated with a legal person, the person representing the User- Signatory is also specified. The identity of that person is also verified.
8. The private key for creating a Professional QC for Cloud QES is secured in the Cloud QES platform via validated cryptographic schemes with security level equivalent to a B-Trust QSCD.
9. The issued Professional Qualified Certificate for Cloud QES to a natural person associated with a legal person is not provided to the Signatory, but it is published in the Public register of the Provider and is available for validity check.
10. The Provider reserves the right to add, if necessary, additional attributes to the Professional QC for Cloud QES of a natural person associated with a legal person.

1.5 B-Trust Qualified Certificate QESeal

1. The certificate for electronic seal, issued under this Policy has the status of a QC within the meaning of the Regulation 910/2014.
2. A QC for QESeal is issued only to a legal person – Creator of a seal and serves to authenticate the source and integrity of data or electronic statements and the Creator's relation with his public key.
3. For the issuance of this certificate, the personal presence of the Creator or an authorized person is required at the RA/LRA for identity verification. Authentication of the Creator's identity can also be done by be done by means of electronic/remote identification.
4. The identification procedure includes proofs of the identity of the Creator and the authorized person, proof that at the time of the request for issuance the legal entity exists and that the Signatory natural person has received authorization to represent the legal entity, as well as their verification.
5. The verification of the request for issuance of a Qualified Certificate for QESeal is done in the order of the above items and provides the highest level of security regarding the Creator's identity and his relationship with the public key.
6. In the request for issuance of a QC for QESeal, the person authorized to represent the Creator may be specified. The identity of that person is also verified.
7. The Creator may himself generate the key pair using B-Trust QSCD and the relevant software or other QSCD that is compatible with the Provider's infrastructure.
8. The private key for creating QC for QESeal is mandatorily generated on a QSCD and cannot be taken out of it.
9. The issued QC for QESeal to a legal person, certifying a public key corresponding to the private key is mandatorily recorded to the QSCD, which is provided to the Creator.
10. The Provider reserves the right to add, if necessary, additional attributes to the QC for QESeal.

1.6 B-Trust Qualified Certificate Cloud QESeal

1. The certificate for electronic seal, issued under this Policy has the status of a QC within the meaning of the Regulation 910/2014.
2. A QC for QESeal is issued only to a legal person – Creator of a seal and serves to authenticate the source and integrity of data or electronic statements and the Creator's relation with his public key.
3. For the issuance of this certificate, the personal presence of the Creator or an authorized person is required at the RA/LRA for identity verification. Authentication of the Creator's identity can also be done by be done by means of electronic/remote identification.
4. The identification procedure includes proofs of the identity of the Creator and the authorized person,

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

proof that at the time of the request for issuance the legal entity exists and that the Signatory natural person has received authorization to represent the legal entity, as well as their verification.

5. The verification of the request for issuance of a Qualified Certificate for QESeal is done in the order of the above items and provides the highest level of security regarding the Creator's identity and his relationship with the public key.
6. In the request for issuance of a QC for QESeal, the person authorized to represent the Creator may be specified. The identity of that person is also verified.
7. The private key for creating a Professional QC for Cloud QES is secured in the Cloud QES platform via validated cryptographic schemes with security level equivalent to a B-Trust QSCD.
8. The Provider reserves the right to add, if necessary, additional attributes to the QC for QESeal.

1.7 Policy Identifiers

1.7.1 B-Trust Personal QC QES and Personal QC Cloud QES – Policy identification

1. The Provider shall apply and support the common policy identified in the Personal QC for QES and QC for Cloud QES to a natural person with OID = 1.3.6.1.4.1.15862.1.6.1.1, which corresponds to the „QCP-n-qscd“ policy (OID 0.4.0.194112.1.2) based on ETSI EN 319 411-2.
2. The Provider shall enter additionally „qcp-public-with-sscd“ policy (O.I.D. = 0.4.0.1456.1.1) based on ETSI EN 101 456 in the Personal QC for QES and QC for Cloud QES, indicating that the private key has been generated and is stored and used on a QSCD.
3. The Provider shall enter an identifier „id-etsi-qcs-QcCompliance“ (OID=0.4.0.1862.1.1) in the „Qualified Statements“ attribute of the Personal QC for QES and QC for Cloud QES, indicating that the certificate is qualified.
4. The Provider shall enter an identifier „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4) in the „Qualified Statements“ attribute of the Personal QC for QES and QC for Cloud QES, indicating that the private key has been generated and is stored and used with the QSCD.
5. The Provider shall enter an identifier „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), with the value „id-etsi-qct-esign“ (OID=0.4.0.1862.1.6.1) in the „Qualified Statements“ attribute of the Personal QC for QES and QC for Cloud QES, indicating that the certificate is used for qualified electronic signature.
6. The Provider shall enter an identifier „id-etsi-qcs-QcPDS“ (OID=0.4.0.1862.1.5) in the „Qualified Statements“ attribute of the Personal QC for QES and QC for Cloud QES, with a value indicating the address (URL-link), on which the B-Trust Disclosure Statement of the Provider has been published.

1.7.2 B-Trust Professional QC QES and Professional QC Cloud QES – Policy identification

1. The Provider shall apply and support the common policy identified in the Professional QC for QES and the Professional QC for Cloud QES of a natural person associated with a legal person, with OID= 1.3.6.1.4.1.15862.1.6.1.2, which corresponds to the policy „QCP-n-qscd“ (OID 0.4.0.194112.1.2) based on ETSI EN 319 411-2.
2. The Provider shall enter additionally the policy „qcp-public-with-sscd“ (O.I.D.= 0.4.0.1456.1.1) based on ETSI EN 101 456 in the Professional QC for QES and QC for Cloud QES, indicating that the private key has been generated and is stored and used on a QSCD.
3. The Provider shall enter an identifier „id-etsi-qcs-QcCompliance“ (OID=0.4.0.1862.1.1) in the „Qualified Statements“ attribute of the Professional QC for QES and QC for Cloud QES, indicating that the certificate is qualified.
4. The Provider enters an identifier „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4) in the „Qualified Statements“ attribute of the Professional QC for QES and QC for Cloud QES, indicating that the private key has been generated and is stored and used on a QSCD.
5. The Provider enters an identifier „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6), with the value „id-etsi-qct-esign“ (OID=0.4.0.1862.1.6.1) in the „Qualified Statements“ attribute of the Professional QC for QES and QC for cloud QES, indicating that the certificate is used for electronic signature.

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

6. The Provider enters an identifier „id-etsi-qcs-QcPDS“ (OID=0.4.0.1862.1.5) in the „Qualified Statements“ attribute of the Professional QC for QES and QC for Cloud QES, with a value indicating the address (URL-link), on which the B-Trust Disclosure Statement of the Provider has been published.

1.7.3 B-Trust QC QESeal and QC Cloud QESeal – Policy identification

1. The Provider shall apply and support the common policy identified in the QC for QESeal of a legal person and QC for Cloud QESeal with OID= 1.3.6.1.4.1.15862.1.6.1.3, which corresponds to the policy „QCP-I“ (OID 0.4.0.194112.1.1) based on ETSI EN 319 411-2.
2. The Provider shall enter an identifier „id-etsi-qcs-QcCompliance“ (OID=0.4.0.1862.1.1) in the „Qualified Statements“ attribute of the qualified seal, indicating that the certificate is qualified.
3. The Provider shall enter an identifier „id-etsi-qcs-QcSSCD“ (OID=0.4.0.1862.1.4) in the „Qualified Statements“ attribute of the QC for QESeal, indicating that the private key has been generated and is stored and used on a QSCD.
4. The Provider shall enter an identifier „id-etsi-qcs-QcType“ (OID=0.4.0.1862.1.6) with the value „id-etsi-qct-eseal“ (oid=0.4.0.1862.1.6.2) in the „Qualified Statements“ attribute, indicating that the certificate is used for qualified electronic seal.
5. The Provider shall enter an identifier „id-etsi-qcs-QcPDS“ (OID=0.4.0.1862.1.5) in the „Qualified Statements“ attribute, with a value indicating the address (URL-link), on which the B-Trust Disclosure Statement of the Provider has been published.

1.8 Designation and applicability of the certificates

1.8.1 B-Trust Personal QC QES and Personal QC Cloud QES

1. The Personal QC for QES and QC for Cloud QES can be used for creating QES by the natural person specified as a Signatory in the certificate, to electronic documents and applications, which require the highest level of information security.
2. The Relying Party must perform due diligence to verify the purpose and applicability of the certificate and the software applications, with which the signature is created and verified, when trusting the electronic signature accompanied by this certificate.
3. Before trusting the electronic signature, the Relying Party should check in the Personal QC for QES and QC for Cloud QES the policy designation applicable to the certificate (Certificate Policy attribute) and the purpose and limitations of the validity of the certificate described in the Key Usage and Extended Key Usage attributes.
4. The Personal QC for QES and QC for Cloud QES have the effect of a handwritten signature to everyone within the meaning of Regulation 910/2014 and identify the User as a Signatory of QES.
5. The Personal QC for QES and QC for Cloud QES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring the highest level of security.

1.8.2 B-Trust Professional QC QES and Professional QC Cloud QES

1. The Professional QC for QES and Professional QC for Cloud QES of a natural person associated with a legal person can be used for creating QES by the natural person specified as a Signatory in the certificate, to electronic documents and applications, which require the highest level of information security.
2. The Relying Party must perform due diligence to verify the purpose and applicability of the certificate and the software applications, with which the signature is created and verified, when trusting the electronic signature accompanied by this certificate.
3. Before trusting the certificate, the Relying Party should check in the Professional QC for QES and Professional QC for Cloud QES the policy designation applicable to this certificate (Certificate Policy attribute) and the purpose and limitations of the validity of the certificate described in the Key Usage and Extended Key Usage attributes.
4. The Professional QC for QES and Professional QC for Cloud QES have the effect of a handwritten signature

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

to everyone within the meaning of Regulation 910/2014 and identify the User as a Signatory of QES.

5. The Professional QC for QES and Professional QC for Cloud QES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring the highest level of security.

1.8.3 B-Trust Organization QC QESeal and QC Cloud QESeal

1. The QC for QESeal and the QC for Cloud QESeal of a legal person is used for creating a QESeal by the Creator, specified in the certificate, to electronic documents and electronic transactions/applications, which require the highest level of information security.
2. According to Regulation 910/2014 a qualified seal should not be used and applied as an electronic signature of a legal person. The qualified seal serves only to authenticate the source and integrity of sealed electronic documents/statements (by an 'electronic' office/organization). Where a transaction requires an electronic signature of a legal person, the qualified electronic signature of the authorized representative of the legal person shall be treated as equivalent.
3. The Relying Party must perform due diligence to verify the purpose and applicability of the certificate and the software applications, with which the seal is created and verified, when trusting the electronic seal accompanied by this certificate.
4. Before trusting the electronic seal, the Relying Party should check in the qualified seal the policy designation applicable to this certificate (Certificate Policy attribute), and the purpose and limitations of the validity of the certificate described in the Key Usage, Extended Key Usage and Qualified Statements attributes.
5. In addition to the authentication of documents issued by a legal person, electronic seals may be used to authenticate the digital assets of a legal person such as software code or servers.

1.9 Key Pair Generation

The key pair of the Subject/Creator of a qualified certificate for an electronic signature or electronic seal shall be generated exclusively within a Qualified Electronic Signature/Seal Creation Device (QSCD) approved by BORICA. The device is verified for compliance with the applicable security requirements.

When the key pair is generated within the BORICA infrastructure, a QSCD is always used. The private key generated within the device remains protected and cannot be exported from it.

In cases of remote key pair generation, when the issuance of a certificate is requested through the BORICA mobile application, the key pair is generated in a hardware cryptographic module operated by BORICA, which complies with the requirements of Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS) for a secure signature creation device.

Where the key pair is generated by the Subject or Creator, BORICA recommends the use of an approved Qualified Electronic Signature/Seal Creation Device, integrated with the BORICA infrastructure, or an equivalent device that complies with the requirements of Regulation (EU) No 910/2014 (eIDAS) and is compatible with the BORICA infrastructure.

The Subject/Creator shall be responsible for the actions or omissions of any persons authorized by them to generate, store, or safeguard their private keys. The Subject/Creator shall also ensure the use of licensed software when operating a Qualified Electronic Signature/Seal Creation Device (QSCD).

The key length of the key pair used for creating a qualified electronic signature or electronic seal, when generated through the BORICA infrastructure, may be 2048, 3072, or 4096 bits

1.10 Limitation of authentication action

1. If a QC is issued with a limitation of the authentication action, the Practice Statement of the Provider allows the certificate to contain a limitation on the purposes and / or value of transactions between Users and Relying parties using a qualified electronic signature/seal.

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

2. The Provider must use the “Qualified Statements” requisite in the QC.
3. The limitation of the QCs on value of transactions that Users conclude by an electronic signature is agreed between them and each Relying Party and is outside the scope of this document.
4. In accordance with EU Regulation 910/2014, the QC for QESeal should not be used and applied as an electronic signature of a legal person. The QC for QESeal serves only to authenticate the source and integrity of automatically sealed electronic documents / statements ("electronic" office /organization).

1.11 Use of certificates outside the scope and restrictions

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

1.12 Management of the Provider Policy

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

2 CERTIFICATE PROFILES

2.1 Profile of B-Trust Personal QC QES and Personal QC Cloud QES

1. The Personal QC QES and Personal QC Cloud QES have the same profile.
2. The Provider issues B-Trust Personal qualified certificate QES and B-Trust Personal qualified certificate CQES with a profile described below:

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Common name: Name chosen by the natural person. If not specified, the full name is entered]
	G =	[First name of the natural person according to identity document]
	SN =	[Surname of the natural person according to identity document]

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

	SERIALNUMBER =	[Natural person identifier. <ul style="list-style-type: none"> • For a Bulgarian citizen - one of the following: <ul style="list-style-type: none"> ○ PNOBG-XXXXXXXXXX for Personal ID ○ PASBG-XXXXXXXXXX for passport number ○ IDCBG-XXXXXXXXXX for ID card number ○ TINBG-XXXXXXXXXX for tax number of a natural person ○ PI:BG-XXXXXXXXXX for ID number of a foreign citizen ○ BT:BG-XXXXXXXXXX for natural person number issued by B-Trust CA • For a foreign citizen – one of the following: <ul style="list-style-type: none"> ○ PNOYY- XXXXXXXXXXXX for national identity number ○ PASYY- XXXXXXXXXXXX for passport number ○ IDCYY- XXXXXXXXXXXX for national ID card number where YY is the country code of the natural person under ISO 3166]
	E =	[email address]
	C =	The two-letter country code -YY according to ISO 3166. It indicates the overall context in which other attributes of the Subject field should be understood.
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	[hash of the „Public key“]
Authority Key Identifier	KeyID =	[hash of the „Public key “ of the „Issuer“]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.1 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=0.4.0.1456.1.1 [3] Certificate Policy: Policy identifier=0.4.0.194112.1.2
Enhanced Key Usage	-	Client Authentication, Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL= http://ocsp.b-trust.org [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer
Key Usage (critical)	-	Digital Signature, Non-repudiation, Key Encipherment
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax- v2 (oid=1.3.6.1.5.5.7.11.2) id-etsi-qcs-semanticsId-Natural (oid=0.4.0.194121.1.1)

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

		id-etsi-qcs-QcCompliance (QcSSCD) (oid=0.4.0.1862.1.4)
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)
		id-etsi-qct-esign (oid=0.4.0.1862.1.6.1)
		PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf language=en

2.2 Profile of B-Trust Professional QC QES and Professional QC Cloud QES

1. The Professional QC QES and Professional QC Cloud QES have the same profile.
2. The Provider issues B-Trust Professional qualified certificate QES and B-Trust Professional qualified certificate CQES to a natural person associated with a legal person with profile described below:

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	[Start of validity period]
Validity to	-	[End of validity period]
Subject	CN =	[Common name: Name chosen by the natural person. If not specified, the full name is entered]
	G =	[First name of the natural person according to identity document]
	SN =	[Surname of the natural person according to identity document]
	SERIALNUMBER =	[Natural person identifier. <ul style="list-style-type: none"> • For a Bulgarian citizen - one of the following: <ul style="list-style-type: none"> ○ PNOBG-XXXXXXXXXX for Personal ID ○ PASBG-XXXXXXXXXX for passport number ○ IDCBG-XXXXXXXXXX for ID card number ○ TINBG-XXXXXXXXXX for VAT number of a natural person ○ PI:BG-XXXXXXXXXX for ID number of a foreign citizen ○ BT:BG-XXXXXXXXXX natural person number issued by B-Trust CA • For a foreign citizen – one of the following: <ul style="list-style-type: none"> ○ PNOYY- XXXXXXXXXXXX for national identity number ○ PASYY- XXXXXXXXXXXX for passport number ○ IDCYY- XXXXXXXXXXXX or national ID card number where YY is the country code of the natural person under ISO 3166]
	O =	[Name of the legal person]
	2.5.4.97= (organizationIdentifier)	[Identifier of a legal entity with which the individual is associated. One of the following: <ul style="list-style-type: none"> • VATBG-XXXXXXXXXX – for VAT number • NTRBG-XXXXXXXXXX – for UIC (BULSTAT)]
	E =	[email address]
C =	The two-letter country code -YY according to ISO 3166. It indicates the overall context in which other attributes of the Subject field should be	

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

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

2.3 Profile of B-Trust Organization QC QESeal and QC Cloud QESeal

- QC QESeal and QC Cloud QESeal have the same profile.
- The Provider issues QC QESeal (B-Trust Organization qualified certificate QES) and QC Cloud QESeal (B-Trust Organization qualified certificate CQES) with the profile described below:

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	[serial number]
Signature algorithm	-	Sha256RSA

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

Signature hash algorithm	-	Sha256	
Issuer	CN =	B-Trust Operational Qualified CA	
	OU =	B-Trust	
	O =	BORICA AD	
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426	
	C =	BG	
Validity from	-	[start of validity period]	
Validity to	-	[end of validity period]	
Subject	CN=	[Name of the Creator (Friendly name)]	
	O =	[Name of the Creator (Company or legal person)]	
	2.5.4.97= (organizationIdentifier)	[Creator identifier. One of the following: <ul style="list-style-type: none"> • VATBG-XXXXXXXX – for VAT number • NTRBG-XXXXXXXX – for UIC (BULSTAT)]	
	E =	[email address]	
	C =	BG or YY where YY is the country code under ISO 3166 where the Creator is registered	
Public key	-	RSA(2048 bits)	
Subject Key Identifier	-	[hash of the „Public key“]	
Authority Key Identifier	KeyID =	[hash of the „Public key“ of the „Issuer“]	
Issuer Alternative Name	URL =	http://www.b-trust.org	
Basic Constraints	Subject Type =	End Entity	
	Path length Constraint =	None	
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps	
	-	[2] Certificate Policy: Policy Identifier=0.4.0.194112.1.1	
Enhanced Key Usage	-	Client Authentication, Secure Email, Code Signing	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
	-	[1] Authority Info Access Access Method=On-line Certificate Status Protocol Alternative Name: URL= http://ocsp.b-trust.org	
Authority Information Access	-	[2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
	-	Digital Signature, Key Encipherment	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation= https://www.b-

			trust.org/documents/pds/pds_en.pdf language=en
--	--	--	--

3 PUBLICATION AND REGISTRATION RESPONSIBILITIES

3.1 Public Register

See section 2.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

3.2 Public Repository

See section 2.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

3.3 Publication of Certification Information

See section 2.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

3.4 Frequency of Publication

See section 2.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

3.5 Access to the Register and Repository

See section 2.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

4 IDENTIFICATION AND AUTHENTICATION

4.1 Naming

See section 3.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

4.2 Initial identification and authentication

See section 3.2. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

4.3 Identification and authentication for certificate renewal

See section 3.3. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS)

4.4 Identification and authentication for suspension

See section 3.4. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

4.5 Identification and authentication for revocation

See section 3.5. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

4.6 Identification and authentication after revocation

See section 3.6. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5 OPERATIONAL REQUIREMENTS AND PROCEDURES

1. The Provider, through the RA/LRA, within the framework of a QCS Agreement, performs the following QCS operating procedures applicable to the QC of this Policy:
 - registration of issuance request;
 - processing issuance request;
 - issuing;
 - handover of issued QC;
 - use of key pair and QC;
 - “Renew”;
 - “Re-key”;
 - suspension/resumption;
 - revocation;
 - QC status.
2. These operational procedures of the Provider are common for the QCs.
3. The Provider allows a User (Signatory/Creator) to terminate via RA/ LRA the Certification Services Contract between them.

5.1 Certificate Request

See 4.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.2 Certificate issuance procedure

See section 4.2. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.3 Certificate issuance

See section 4.3. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.4 Certificate acceptance and publication

See section 4.4. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.5 Key pair and certificate usage

See section 4.5. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.6 Certificate renewal

See section 4.6. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.7 Certificate renewal with the generation of a new key pair (re-key)

See section 4.7. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.8 Certificate modification

See section 4.8. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

5.9 Certificate suspension and revocation

See section 4.9. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

5.10 Certificate status

See section 4.10. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

5.11 Termination of a Certification Services Contract

See section 4.11. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

5.12 Key recovery

See section 4.12. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

6.1 Physical controls

See section 5.1. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.2 Procedural controls

See section 5.2. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.3 Staff qualification and training

See section 5.3. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.4 Logging procedures

See section 5.4. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.5 Archiving

See section 5.5. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.6 Key changeover

See section 5.6. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.7 Compromise and disaster recovery

See section 5.7. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

6.8 Compromise of a Private Key

See section 5.8. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

**CERTIFICATE POLICY FOR PROVIDING QUALIFIED CERTIFICATES
FOR QUALIFIED ELECTRONIC SIGNATURE, CLOUD QUALIFIED ELECTRONIC SIGNATURE,
QUALIFIED ELECTRONIC SEAL AND CLOUD QUALIFIED ELECTRONIC SEAL**

6.9 Provider Termination

See section 5.9. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7 TECHNICAL SECURITY CONTROL AND MANAGEMENT

7.1 Key Pair Generation and Installation

See section 6.1. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.2 Generation Procedure

See section 6.2. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.3 Private Key Protection and Cryptographic Module Engineering Controls

See section 6.3. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.4 Other Aspects of Key Pair Management

See section 6.4. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.5 Activation Data

See section 6.5. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.6 Security of Computer Systems

See section 6.6. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.7 Development and Operation (Life Cycle)

See section 6.7. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.8 Additional Tests

See section 6.8. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.9 Network Security

See section 6.9. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

7.10 Verification of Time

See section 6.10. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

8 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

8.1 Periodic and Circumstantial Inspection

See section 9.1. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

8.2 Qualifications of the Inspectors

See section 9.2. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

8.3 Relationship of the Inspecting Persons with the Provider

See section 9.3. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

8.4 Scope of the Inspection

See section 9.4. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

8.5 Discussion of Results and Follow-Up Actions

See section 9.5. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9 BUSINESS AND LEGAL ISSUES

9.1 Prices and fees

See section 10.1. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.2 Financial liability

See section 10.2. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.3 Confidentiality of business information

See section 10.3. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.4 Personal data protection

See section 10.4. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.5 Intellectual property rights

See section 10.5. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.6 Responsibility and warranties

See section 10.6. of the document "Certification Practice Statement for the provision of qualified certificates and qualified trust services" of BORICA AD (B-Trust CPS-eIDAS).

9.7 Disclaimers of warranties

See section 10.7. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.8 Limitation of liability of the Provider

See section 10.8. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.9 Indemnities for the Provider

See section 10.9. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.10 Term and termination

See section 10.10. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.11 Notices and communication with participants

See section 10.11. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.12 Amendments to the document

See section 10.12. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.13 Dispute settlement (jurisdiction)

See section 10.13. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.14 Governing law

See section 10.14. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).

9.15 Compliance with applicable law

See section 10.15. of the document “Certification Practice Statement for the provision of qualified certificates and qualified trust services” of BORICA AD (B-Trust CPS-eIDAS).