Public

# POLICY

## ON THE PROVISION OF QUALIFIED CERTIFICATES FOR ADVANCED ELECTRONIC SIGNATURE/SEAL BY BORICA AD

## (B-Trust QCP-eIDAS AES/AESeal)

Version 1.0

Effective:

July 1, 2018

| Document history | | | | |
|---|---|---|---|---|
| **Version** | **Author(s)** | **Date** | **Status** | **Comment** |
| 1.0 | Dimitar Nikolov | 20.05.2018 | Approved | Initial release |
| | | | | |

# CONTENTS:

## LIST OF TERMS AND ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Electronic Signature |
| AESeal | Advanced Electronic Seal |
| BG | Bulgaria |
| B-Trust QHSM | Qualified HSM in the cloud-based QES platform with a security profile meeting the EAL 4+ or higher security level according to CC or other specification defining equivalent security levels |
| CA | Certification Authority |
| CC | Common Criteria for Information Technology Security Evaluation – International Standard for Information Security (ISO/IEC 15408) |
| CEN | European Committee for Standardization |
| CENELEC | European Committee for Electro-technical Standardization |
| CP | Certificate Policy |
| CPS | Certificate Practice Statement |
| CRL | Certificate Revocation List |
| CRC | Communications Regulation Commission |
| CQES | Cloud Qualified Electronic Signature |
| DSA | Digital Signature Algorithm |
| DN | Distinguished Name |
| EDETSA | Electronic Document and Electronic Trusted Services Act |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| FIPS | Federal Information Processing Standard |
| 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 |
| RSA | Rivest–Shamir- Dalman |
| QSCD | Qualified Signature Creation Device |
| QTSP | Qualified Trusted Services Provider |
| SAD | Signature Activation Data |
| SAP | Signature Activation Protocol |

| | |
|---|---|
| SCT | Signature Creation Token (PKCS#12) |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| S/MIME | Secure/Multipurpose Internet Mail Extensions |
| TRM | Tamper Resistant Module |
| URL | Uniform Resource Locator |
| QCP-n-qscd | Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD |
| QCP-l-qscd | Certificate policy for EU qualified certificates issued to legal persons with Private Key related to the certified public key in a QSCD |
| QCP-w | Certificate policy for EU qualified website authentication certificates |

## COMPLIANCE AND USE

This Document:

- Has been developed by "BORICA" AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- Is effective as of 01.07.2018;
- Is entitled “Policy on the Provision of Qualified Certificates for Advanced Electronic Signature/Seal by BORICA AD (**B-Trust CP-eIDAS AES/AESeal**)”;
- Is associated with the published current version of the document „Certification Practice Statement for qualified certificates and qualified trusted services of BORICA AD (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, as far as this guideline is in line with the management policy of the Provider;
- Constitutes the General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA). These conditions are part of the written Contract for trusted services, 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 AD with the EDETSA and the legal framework;
- is publicly available at any time on the Provider's website: https://www.b-trust.bg/documents;
- May be changed by the QTSP and each new version shall be published on the Provider’s website.

This document is prepared in accordance with:

- Electronic Document And Electronic Trusted Services Act (EDETSA);
- Ordinance on the Activities of Trusted -Service-Providers;
- Ordinance on the requirements to the algorithms of creation and verification of qualified electronic signature;
- Regulation (EU) № 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The contents and structure of this document is in accordance with Regulation (EU) № 910/2014 and refers to the information contained in the following ratified international guidelines, specifications and standards:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816: ESSCertIDv2 Update for RFC 3161;
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055: Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;

- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI EN 319 412-1, 2, 3 and 5: Certificate Profiles.

Any information relating to this document may 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 the qualified certificates for advanced electronic signature/seal, issued by BORICA AD 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 QCs for AES or AESeal, 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 as specified in the Certification Practice Statement of the Provider;
- Determines the relevance and the level of trust in the certified facts in the QCs for AES or AESeal.

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 to get acquainted with these concepts and with the document „Certification Practice Statement for qualified certificates and qualified trusted services of BORICA AD (B-Trust CPS-eIDAS)" before using this document. In any case, this document (Policy) should be used together with the Certification Practice Statement of the Provider.

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

The Provider uses OIDs in the B-Trust PKI infrastructure, formed on the basis of code 15862, assigned to BORICA AD by IANA in the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA Registered Private Enterprise) and in 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 AD has informed the CRC about the start of activity as a QTSP under the EDETSA 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 EDETSA 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.

In regard to relations with Users and third parties, only the current version of the Policy at the time of using QC SSL/TLS issued by BORICA AD is valid.

# 1 GENERAL CHARACTERISTSCS OF THE CERTIFICATES

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

- B-Trust Personal qualified certificate for AES;
- B-Trust Professional qualified certificate for AES;
- B-Trust Legal qualified certificate for AESeal.

These certificates have the status of qualified certificates for AES and AESeal within the meaning of Regulation 910/2014.

## 1.1 General characteristics of B-Trust Personal qualified certificate for AES

1. The electronic signature certificate issued under this Policy has the status of a qualified certificate AES within the meaning of the Regulation 910/2014.
2. A personal qualified certificate for AES is issued to a natural person – AES Holder, and certifies the Holder's electronic identity and the relationship of the Holder with his public key in the certificate.
3. For issuing this certificate, the personal presence of the Holder or a person authorized by him is required at the RA/LRA for verification of his identity by the Provider.
4. The identification procedure includes proofs of identity of the Holder and their verification.
5. The verification of the request for issuing Personal qualified certificate for AES is done in the order of the above items and provides a high level of security regarding the Holder's identity and his relation with the public key.
6. The Holder may himself generate the key pair using approved by the Provider or other licensed software with an equivalent level of security that is compatible with the Provider's infrastructure.
7. The private key for creating Personal qualified certificate for AES is generated using the approved or licensed software, it is stored in a portable cryptographic file and can be transferred to systems of the User.
8. The issued Personal qualified certificate for AES certifying a public key corresponding to the private key is recorded to a portable software token together with the service certificates of the Provider (PKCS#12 file), when the key pair is generated at the Provider (at the LRA) and is provided to the Holder.
9. When the key pair is generated by the User, it is his responsibility to create a portable (software) token.
10. The Holder may use hardware token compatible with the B-trust infrastructure of the Provider for generating and storing the key pair for the qualified certificate for AES.
11. The Personal qualified certificate for AES is not renewed, the User-Holder may request the Provider to issue a new Personal qualified certificate for AES with a new key pair.
12. The Provider reserves the right to add additional attributes to the Personal qualified certificate for AES.

## 1.2 General characteristics of B-Trust Professional qualified certificate for AES

1. The electronic signature certificate issued under this Policy has the status of a qualified certificate for AES within the meaning of the Regulation.
2. A professional qualified certificate for AES is issued to a Holder – natural person who is associated with a legal person, and certifies the Holder's electronic identity and the relationship of the Holder with his public key in the certificate.
3. For issuing this certificate, the personal presence of the Holder or a person authorized by him is required at the RA/LRA for verifying his identity by the Provider.
4. The identification procedure includes proofs of the identity of the Holder and their verification.
5. The verification of the request for issuing Professional qualified certificate for AES is done in the order of the above items and provides a high level of security regarding the Holder's identity and his relation with the public key.
6. The Holder may himself generate the key pair using approved by the Provider or other licensed

software with an equivalent level of security that is compatible with the Provider's infrastructure.
7. In the request for issuing Professional qualified certificate for AES to a natural person associated with a legal person, the person representing the Holder is also specified. The identity of that person is also verified.
8. The private key for creating AES to a natural person associated with a legal person is generated using the approved or licensed software, it is stored in a portable cryptographic file and can be transferred to systems of the User.
9. The issued Professional qualified certificate for AES to a natural person associated with a legal person is recorded to a portable software token together with the service certificates of the Provider (PKCS#12 file), when the key pair is generated at the Provider (at the LRA) and is provided to the Holder.
10. When the key pair is generated by the User-Holder, it is his responsibility to create a portable (software) token.
11. The Holder may use hardware token compatible with the B-trust infrastructure of the Provider for generating and storing the key pair for the qualified certificate for AES.
12. The Professional qualified certificate for AES is not renewed, the User-Holder may request the Provider to issue a new Professional qualified certificate AES with a new key pair.
13. The Provider reserves the right to add additional attributes to the Professional qualified certificate for AES to an individual associated with a legal entity.

## 1.3 General characteristics of B-Trust Legal qualified certificate for AESeal

1. The electronic seal certificate issued under this Policy has the status of a Legal qualified certificate AESeal within the meaning of the Regulation.
2. A Legal qualified certificate for AESeal 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 issuing this certificate, the personal presence of the person authorized by the Creator is required at the RA/LRA for verifying his identity by the Provider.
4. The identification procedure includes proofs of the identity of the Creator and the authorized person, and their verification.
5. The verification of the request for issuing a Legal qualified certificate for AESeal is done in the order of the above items and provides a high level of security regarding the Creator’s identity and his relation with the public key.
6. In the request for issuing a Legal qualified certificate for AESeal, the person representing the Creator is specified. The identity of that person is also verified.
7. The Creator may himself generate the key pair using approved by the Provider or other licensed software with an equivalent level of security that is compatible with the Provider's infrastructure.
8. The private key for creating a Legal qualified certificate for AESeal is generated using the approved or licensed software, it is stored in a portable cryptographic file and can be transferred to systems of the User.
9. The issued Legal qualified certificate for AESeal to a legal person certifying public key corresponding to a private key is recorded to a portable software token together with the service certificates of the Provider (PKCS#12 file), when the key pair is generated at the Provider (at the LRA) and is provided to the Creator.
10. When the key pair is generated by the User-Creator, it is his responsibility to create a portable (software) token.
11. The Creator may use hardware token compatible with the B-trust infrastructure of the Provider for generating and storing the key pair for the Legal qualified certificate for AESeal.
12. The Legal qualified certificate for AESeal is not renewed, the User-Creator may request the Provider to issue a new is not renewed, the User-Holder may request the Provider to issue a new Professional qualified certificate AES with a new key pair.
13. The Provider reserves the right to add additional attributes to the Legal qualified certificate for AESeal of a legal person.

## 1.4 Policy Identifiers

### 1.4.1 B-Trust Personal qualified certificate for AES

1. The Provider shall apply and support the common policy identified in the Personal qualified certificate for AES, with OID=1.3.6.1.4.1.15862.1.7.1.1, which corresponds to „QCP-n“ (OID 0.4.0.194112.1.0) based on ETSI EN 319 411-2.
2. The Provider shall enter additionally „qcp-public“ policy (O.I.D. = 0.4.0.1456.1.2) based on ETSI EN 101 456 in the Personal qualified certificate for AES, indicating that the private key has not been generated and is not stored and used in 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 qualified certificate for AES, indicating that the certificate is qualified.
4. 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 qualified certificate for AES, with a value indicating the address on which the B-Trust Disclosure Statement of the Provider has been published.

### 1.4.2 B-Trust Professional qualified certificate for AES

1. The Provider shall apply and support the common policy identified in the Professional qualified certificate for AES to an individual associated with a legal entity, with OID= 1.3.6.1.4.1.15862.1.7.1.2, which corresponds to „QCP-n“ (OID 0.4.0.194112.1.0) based on ETSI EN 319 411-2.
2. The Provider shall enter additionally „qcp-public“ policy (O.I.D. = 0.4.0.1456.1.2) based on ETSI EN 101 456 in the Professional qualified certificate for AES, indicating that the private key has not been generated and is not stored and used in 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 qualified certificate for AES, indicating that the certificate is qualified.
4. 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 qualified certificate for AES, with a value indicating the address on which the B-Trust Disclosure Statement of the Provider has been published.

### 1.4.3 B-Trust Legal qualified certificate for AESeal

1. The Provider shall apply and support the common policy identified in the Legal qualified certificate for AESeal, with OID=1.3.6.1.4.1.15862.1.7.1.3, which corresponds to „ncp“ (OID 0.4.0.2042.1.1) based on ETSI EN 319 411-2.
2. The Provider shall enter additionally „qcp-public“ policy (O.I.D. = 0.4.0.1456.1.2) based on ETSI EN 101 456 in the Legal qualified certificate for AESeal, indicating that the private key has not been generated and is not stored and used in 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 qualified certificate for AES, indicating that the certificate is qualified.
4. The Provider shall enter an identifier „id-etsi-qcs-QcPDS“ (OID=0.4.0.1862.1.5) in the „Qualified Statements" attribute of the Legal qualified certificate for AESeal, with a value indicating the address on which the B-Trust Disclosure Statement of the Provider has been published.

## 1.5 Designation and use of the certificates

### 1.5.1 B-Trust Personal qualified certificate for AES

1. The Personal qualified certificate for AES can be used for creating AES by the natural person specified as a Holder in the certificate, to electronic documents and applications, which require a significant level of information security.
2. It is the Relying Party's duty, when trusting the electronic signature accompanied by this certificate, to verify the purpose and applicability of the certificate and the software applications, with which the signature is created and verified.
3. Before trusting the certificate, the Relying Party should check 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 Personal qualified certificate for AES does not have the effect of a handwritten signature to everyone within the meaning of Regulation 910/2014 and art. 13 of the EDESCA, and identifies the person as a Holder of the AES.
5. The Personal qualified certificate for AES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring a significant level of security.

### 1.5.2 B-Trust Professional qualified certificate for AES

1. The Professional qualified certificate for AES of a natural person associated with a legal person can be used for creating AES by the natural person specified as a Holder in the certificate, to electronic documents and applications, which require a significant level of information security.
2. It is the Relying Party's duty, when trusting the electronic signature accompanied by this certificate, to verify the purpose and applicability of the certificate and the software applications, with which the signature is created and verified.
3. Before trusting the certificate, the Relying Party should check 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 qualified certificate for AES does not have the effect of a handwritten signature to everyone within the meaning of Regulation 910/2014 and art. 13 of the EDESCA, and identifies the person as a Holder of the AES.
5. The Professional qualified certificate for AES can also be used for sending secure and encrypted electronic messages and for secure and encrypted communications, access to information, and online transactions requiring a significant level of security.

### 1.5.3 B-Trust Legal qualified certificate for AESeal

1. The qualified certificate for AESeal of a legal person is used for creating an AESeal by the Creator specified in the certificate, to electronic documents and applications, which require a significant level of information security.
2. According to Regulation 910/2014 a qualified certificate for AESeal should not be used and applied as an electronic signature of a legal person. The qualified certificate for AESeal 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 or advanced electronic signature of the authorized representative of the legal person shall be treated as equivalent.
3. It is the Relying Party's duty, when trusting the qualified electronic seal accompanied by this certificate, to verify the purpose and applicability of the certificate and the software applications, with which the signature is created and verified.
4. Before trusting the electronic seal, the Relying Party should check in the qualified certificate for AESeal 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.

## 1.6 Limitation of the authentication action

1. If a QC is issued with a limitation of the authentication action, the Practice Statement of the Provider allows the certificate to contain a limitation on the purposes and / or value of transactions between Users and Relying parties using a qualified electronic signature/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 through the use of an electronic signature is agreed between them and Relying Parties, and is outside the scope of this document.

4. In accordance with EU Regulation 910/2014, the QC for AESeal should not be used and applied as an electronic signature of a legal entity. The QC for AESeal serves only to authenticate the source and integrity of automatically sealed electronic documents / statements ("electronic" office /organization).

### 1.7 Use of certificates outside the scope and restrictions

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

### 1.8 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 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 qualified certificate for AES

1. The Provider issues B-Trust Personal qualified certificate for AES to a natural person 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 Advanced 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.<br>• For a Bulgarian citizen - one of the following:<br>○ PNOBG-XXXXXXXXXX for EGN<br>○ PASSBG-XXXXXXXX for passport number<br>○ IDCBG-XXXXXXXXX for ID card number<br>○ TINBG-XXXXXXXXX for tax number of a natural person<br>○ PI:BG-XXXXXXXXXX for ID number of a foreign citizen<br>○ BT:BG-XXXXXXXXXX natural person number issued by B-Trust CA<br>• For a foreign citizen – one of the following:<br>○ PNOYY- XXXXXXXXXX for national identity number<br>○ PASSYY- XXXXXXXX for passport number<br>○ IDCYY- XXXXXXXXX for national ID card number<br>where YY is the country code of the natural person under ISO 3166<br>] |
| | E = | [email address] |
| | C = | BG |
| 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 =<br>Path length Constraint = | End Entity<br>None |
| Certificate Policy | - | [1] Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.7.1.1<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier ID=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2] Certificate Policy:<br>Policy Identifier=0.4.0.1456.1.2<br>[3] Certificate Policy:<br>Policy identifier=0.4.0.194112.1.0 |
| Enhanced Key Usage | - | Client Authentication, Secure Email |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl |
| Authority Information Access | - | [1] Authority Info Access<br>Access Method=On-line Certificate Status Protocol<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2] Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer |
| Key Usage (critical) | - | 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-Natural (oid=0.4.0.194121.1.0)<br>id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) |

| | | | |
|---|---|---|---|
| | | 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 |

## 2.2 B-Trust Professional qualified certificate for AES

1. The Provider issues B-Trust Professional qualified certificate for AES to a natural person associated with a legal person 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 Advanced 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.<br>• For a Bulgarian citizen - one of the following:<br>○ PNOBG-XXXXXXXXXX for EGN<br>○ PASSBG-XXXXXXXX for passport number<br>○ IDCBG-XXXXXXXXX for ID card number<br>○ TINBG-XXXXXXXXX for tax number of a natural person<br>○ PI:BG-XXXXXXXXXX for ID number of a foreign citizen<br>○ BT:BG-XXXXXXXXXX natural person number issued by B-Trust CA<br>• For a foreign citizen – one of the following:<br>○ PNOYY- XXXXXXXXXX for national identity number<br>○ PASSYY- XXXXXXXX for passport number<br>○ IDCYY- XXXXXXXXX for national ID card number<br>where YY is the country code of the natural person under ISO 3166<br>] |
| | E = | [email address] |
| | C = | BG |
| 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 =<br>Path length Constraint = | End Entity<br>None |

| | | | |
|---|---|---|---|
| Certificate Policy | - | [1] Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.7.1.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier ID=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2] Certificate Policy:<br>Policy Identifier=0.4.0.1456.1.2<br>[3] Certificate Policy:<br>Policy identifier=0.4.0.194112.1.0 | |
| Enhanced Key Usage | - | Client Authentication, Secure Email | |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl | |
| Authority Information Access | - | [1] Authority Info Access<br>Access Method=On-line Certificate Status Protocol<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2] Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer | |
| Key Usage (critical) | - | 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-Natural (oid=0.4.0.194121.1.0) |
| | | id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) | |
| | | id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) | PdsLocations<br>PdsLocation=https://www.b-trust.org/documents/pds/pds_en.pdf<br>language=en |

## 2.3 Profile of B-Trust Legal qualified certificate for AESeal

1. The Provider issues B-Trust Organization qualified certificate for AESeal 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 Advanced 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:<br>• VATBG-XXXXXXXXX – for VAT number |

| | | |
|---|---|---|
| | | • NTRBG-XXXXXXXXX – for UIC (BULSTAT)<br>] |
| | E = | [email address] |
| | C = | BG or YY<br>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 =<br>Path length Constraint = | End Entity<br>None |
| Certificate Policy | - | [1] Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.15862.1.7.1.3<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier ID=CPS<br>Qualifier:<br>http://www.b-trust.org/documents/cps<br>[2] Certificate Policy:<br>Policy Identifier=0.4.0.2042.1.1 |
| Enhanced Key Usage | - | Client Authentication, Secure Email |
| CRL Distribution Points | - | [1] CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.crl |
| Authority Information Access | - | [1] Authority Info Access<br>Access Method=On-line Certificate Status Protocol<br>Alternative Name:<br>URL=http://ocsp.b-trust.org<br>[2] Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ca.b-trust.org/repository/B-TrustOperationalACAOCSP.cer |
| Key Usage (critical) | - | 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-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

As described in section 2.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 3.2 Public Repository

As described in section 2.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 3.3 Publication of Certification Information

As described in section 2.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 3.4 Frequency of Publication

As described in section 2.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 3.5 Access to the Register and Repository

As described in section 2.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 4 IDENTIFICATION AND AUTHENTICATION

### 4.1 Naming

As described in section 3.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 4.2 Initial identification and authentication

As described in section 3.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 4.3 Identification and authentication for certificate renewal

Under this Policy, the Provider does not renew Qualified Certificates for Advanced Electronic Signature/Seal. Please see section 3.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 4.4 Identification and authentication for suspension

As described in section 3.4. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 4.5 Identification and authentication for termination

As described in section 3.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 4.6 Identification and authentication after termination

As described in section 3.6. of the document „Certification Practice Statement for qualified certificates and qualified trusted 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 application;
   - processing issuance application;
   - issuing;
   - use of key pair and QC;
   - suspension / resumption;
   - termination;
   - QC status.
2. These operational procedures of the Provider are common for the QCs for AES and AESeal.
3. The Provider allows a User (Holder/Creator) to terminate via RA/ LRA the Trusted Services

Contract between them.

## 5.1 Certificate Application

As described in section 4.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.2 Certificate issuance procedure

As described in section 4.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.3 Certificate issuance

As described in section 4.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.4 Certificate acceptance and publication

As described in section 4.4. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.5 Key pair and certificate usage

As described in section 4.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.6 Certificate renewal

Under this Policy, the Provider does not renew Qualified Certificates for Advanced Electronic Signature / Seal. As described in section 4.6. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

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

As described in section 4.7. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.8 Certificate modification

As described in section 4.8. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.9 Certificate revocation and suspension

As described in section 4.9. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.10 Certificate status

As described in section 4.10. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.11 Termination of a Contract for Trusted Services

As described in section 4.11. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 5.12 Key recovery

As described in section 4.12. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

# 6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 6.1 Physical controls

As described in section 5.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.2 Procedural controls

As described in section 5.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.3 Staff qualification and training

As described in section 5.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.4 Logging procedures

As described in section 5.4. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.5 Archiving

As described in section 5.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.6 Key changeover

As described in section 5.6. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.7 Compromise and disaster recovery

As described in section 5.7. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.8 Compromise of a Private Key

As described in section 5.8. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 6.9 Provider Termination

As described in section 5.9. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

# 7 TECHNICAL SECURITY CONTROL AND MANAGEMENT

## 7.1 Key Pair Generation and Installation

As described in section 6.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 7.2 Generation Procedure

As described in section 6.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 7.3 Private Key Protection and Cryptographic Module Engineering Controls

As described in section 6.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 7.4 Other Aspects of Key Pair Management

As described in section 6.4. of the document „Certification Practice Statement for qualified certificates

and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.5 Activation Data

As described in section 6.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.6 Security of Computer Systems

As described in section 6.6. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.7 Development and Operation (Life Cycle)

As described in section 6.7. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.8 Additional Tests

As described in section 6.8. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.9 Network Security

As described in section 6.9. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 7.10 Verification of Time

As described in section 6.10. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 8 INSPECTION AND CONTROL OF PROVIDER'S ACTIVITIES

### 8.1 Periodic and Circumstantial Inspection

As described in section 9.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 8.2 Qualifications of the Inspectors

As described in section 9.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 8.3 Relationship of the Inspecting Persons with the Provider

As described in section 9.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 8.4 Scope of the Inspection

As described in section 9.4. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

### 8.5 Discussion of Results and Follow-Up Actions

As described in section 9.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

# 9 BUSINESS AND LEGAL ISSUES

## 9.1 Prices and fees

As described in section 10.1. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.2 Financial liability

As described in section 10.2. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.3 Confidentiality of business information

As described in section 10.3. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.4 Personal data protection

As described in section 10.4. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.5 Intellectual property rights

As described in section 10.5. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.6 Responsibility and warranties

As described in section 10.6. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.7 Disclaimer

As described in section 10.7. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.8 Limitation of liability of the Provider

As described in section 10.8. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.9 Indemnities for the Provider

As described in section 10.9. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.10 Term and termination

As described in section 10.10. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.11 Notices and communication with participants

As described in section 10.11. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.12 Amendments to the document

As described in section 10.12. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.13 Dispute settlement (jurisdiction)

As described in section 10.13. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.14 Governing law

As described in section 10.14. of the document „Certification Practice Statement for qualified

certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).

## 9.15 Compliance with applicable law

As described in section 10.15. of the document „Certification Practice Statement for qualified certificates and qualified trusted services" of BORICA AD (B-Trust CPS-eIDAS).