Public

POLICY

ON THE PROVISION OF CERTIFICATES FOR WEBSITE AUTHENTICATION BY BORICA AD

(B-Trust QCP-eIDAS Web SSL)

Version 1.0

Effective date:

July 1, 2018

Document history				
Version	**Author (s)**	**Date**	**Status**	**Comment**
1.0	Dimitar Nikolov	25.05.2018	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 website authentication certificates
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 developed by "BORICA" AD, a legal entity registered in the Commercial Register of the Registry Agency under UIC 201230426;
- Becomes effective as of 01.07.2018;
- Is entitled “Policy on the Provision of Certificates for Website Authentication by BORICA AD (B-Trust QCP-eIDAS Web SSL)”;
- 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 Certification-Service-Providers;
- 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 content 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;
- CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

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 to the website authentication certificates (Certificates SSL/TLS), 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 Certificates SSL/TLS, 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;
- Determines the relevance and the level of trust in the certified facts in Certificates SSL/TLS.

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 Domain Validation SSL certificate/B-Trust DVC SSL;
- B-Trust Organization Validation SSL certificate/B-Trust OVC SSL.

1.1 B-Trust Domain Validation SSL certificate/B-Trust DVC SSL – General characteristics

1. The B-Trust Domain Validation SSL certificate/B-Trust DVC SSL issued under this Policy has the status of a Certificate within the meaning of the Regulation only if it is used for validation of the domain.
2. This certificate is issued to a User - a legal entity or an individual - and it authenticates the electronic identity of the domain owner hosting a website with a high degree of certainty for the browser client.
3. Wild card (*) in the hostname is accepted (for example, * .b-trust.bg).
4. For issuing this certificate, the personal presence of the User or a person authorized by him is required at the RA/LRA for the identification procedure by the Provider.
5. The identification procedure includes submission of evidence of ownership of the domain hosting website and of the identity of the User and the authorized person and their verification.
6. The verification of the request for issuing Domain Validation SSL certificate is done in the order of the above items and provides a high level of security regarding the ownership of the domain by the User (legal entity) specified in the certificate.
7. Regarding the use of the TLS/SSL protocol, the policy for this certificate allows a sufficient level of security for the browser client accessing a website in the domain - generating and storing the private key corresponding to the public key in the certificate by validated or licensed software and cryptographic software token.
8. The User 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.
9. In the request for issuing website (domain) validation certificate the person representing the User is specified. The identity of that person is also verified.
10. The private key for creating website (domain) validation certificate 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.
11. The issued certificate 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 User.
12. When the key pair is generated by the User, it is his responsibility to create a portable (software) Token.
13. The Provider reserves the right to add additional attributes to the website (domain) validation certificate.

1.2 B-Trust Organization Validation SSL certificate/B-Trust OVC SSL – General characteristics

1. The B-Trust Organization Validation SSL certificate/B-Trust OVC SSL, issued under this Policy has the status of Certificate only if it is used for validation.
2. This certificate is issued to a User - a legal entity or an individual - and it authenticates the electronic identity and accreditation of the User with a high degree of certainty for the browser client that the website accessed is owned by the organization identified in the certificate.
3. Wild card (*) in the hostname is accepted (for example, * .b-trust.bg).
4. For issuing this certificate, the personal presence of the User or a person authorized by him is required at the RA/LRA for the identification procedure by the Provider.
5. The identification procedure includes submission of evidence of ownership of the domain hosting website and of the identity of the User and the authorized person and their verification.

6. The verification of the request for issuing organization validation certificate of a website (domain) is done in the order of the above items and provides a high level of security regarding the ownership of the domain by the User (legal entity) specified in the certificate.
7. Regarding the use of the TLS/SSL protocol, the policy for this certificate allows a sufficient level of security for the browser client accessing a website in the domain - generating and storing the private key corresponding to the public key in the certificate by validated or licensed software and cryptographic software token.
8. The User 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.
9. The private key for creating organization validation certificate 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.
10. The issued certificate is recorded to a portable software token together with the service certificates of the Provider (PKCS#12 file), when the pair of keys is generated at the Provider (at LRA) and is provided to the User.
11. When the pair of keys is generated at the User, it is his responsibility to create a portable (Software) Token.
12. The Provider reserves the right to add additional attributes to the organization validation certificate.

1.3 Policy Identifiers

1.3.1 B-Trust Domain Validation SSL certificate/B-Trust DVC SSL – Policy indication

1. The Provider shall apply and support the common policy identified in the Domain Validation SSL certificate, with OID = 1.3.6.1.4.1.15862.1.7.1.5, which corresponds to DVC (OID = 0.4.0.2042.1.6) based on ETSI TS 102 042.
2. The Provider shall enter in the „Certificate policy" attribute a certificate policy with OID = 2.23.140.1.2.1, corresponding to CA/B Forum SSL DV if the certificate performs only domain validation (Compliant with Baseline Requirements – No entity identity asserted).

1.3.2 B-Trust Organization Validation SSL qualified certificate/B-Trust OVC SSL - Policy indication

1. The Provider shall apply and support the common policy identified in the Organization Validation SSL certificate with OID = 1.3.6.1.4.1.15862.1.7.1.6, which corresponds to "OVC" (OID = 0.4.0.2042.1.7) based on ETSI TS 102 042.
2. The Provider shall enter in the „Certificate policy" attribute a certificate policy with OID = 2.23.140.1.2.2, corresponding to CA/B Forum SSL OV of the User is legal entity (organization/institution) (Compliant with Baseline Requirements – Organization identity asserted).

1.4 Designation and use of the certificates

1.4.1 B-Trust Domain Validation SSL certificate

1. B-Trust DVC SSL is manly used to establish exchange of data through TLS/SSL protocols for the following services and applications:
   - To identify the organization owner of the domain (DNS), providing an adequate level of certainty for the browser client that the website he is accessing is the property of the organization identified in the certificate with its name and address;
   - Encryption of communications between a client and website facilitating the exchange of crypto keys for Internet data protection.
2. The Relying Party's duty is to verify the purpose and applicability of the certificate and software applications that use the certificate.
3. 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, Extended Key Usage and Qualified Statements attributes, before trusting the certificate.

4. The validity of B-Trust Domain Validation SSL qualified certificate is one year or 825 days. The certificate is not subject to renewal. The Provider shall issue a new certificate.

1.4.2 B-Trust Organization Validation SSL certificate/B-Trust OVC SSL

1. The Organization Validation SSL certificate is used to identify the domain owner and the accreditation of the person (User) with an adequate level of certainty for the browser client that the website he is accessing is the property of the person identified in the certificate.
2. The Relying Party's duty is to verify the purpose and applicability of the certificate and software applications that use the certificate.
3. 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, Extended Key Usage and Qualified Statements attributes, before trusting the certificate.
4. The validity of the Organization Validation SSL qualified certificate is one year or 825 days. The certificate is not subject to renewal. The Provider shall issue a new certificate.

1.5 Limitation of authentication action

1. The certification action when using website authentication certificates is regulated only within the scope of their application in accordance with section 1.5 of this Policy. Any other use of the certificates is unauthorized and invalidates their authentication.
2. Website Authentication Certificates should not apply to activities subject to restrictions and prohibitions under the legislation of the Republic of Bulgaria as well as the applicable EU Regulations and Directives.
3. If a QC is issued with a limitation of the authentication action, the Practice Statement of the Provider shall not allow the certificate to contain a limitation on the purposes and/or value of transactions between Users and Relying parties using a website authentication certificate.
4. The limitation of the website authentication certificate on value of transactions in online electronic transactions between Users and Relying Parties is outside the scope of this document.

1.6 Use of certificates outside the scope and restrictions

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.

1.7 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 Domain Validation SSL certificate/B-Trust DVC SSL

1. The Provider issues Domain Validation certificate with the 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	-	[Validity from]	
Validity to	-	[Validity to]	
Subject	CN =	[Name of User's domain (DNS name)]	
	OU =	[DV SSL]	
	E =	[User's email]	
	L =	[User's locality]	
	C =	BG or YY where YY is the country code under ISO 3166 where the User is registered	
Public key	-	RSA(2048 bits)	
SubjectAlternativeName	-	[DNS name]	
Subject Key Identifier	-	[hash of „Public key "]	
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer"]	
Issuer Alternative Name	URL =	http://www.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.5 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=2.23.140.1.2.1 [3] Certificate Policy: Policy Identifier=0.4.0.2042.1.6	
Enhanced Key Usage	-	Server Authentication, Client Authentication, Secure Email	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.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-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-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/pds_e

			n.pdf language=en

2.2 Profile of B-Trust Organization Validation SSL certificate/B-Trust OVC SSL

1. The Provider issues Organization Validation certificate with the 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	-	[Validity from]
Validity to	-	[Validity to]
Subject	CN =	[Name of User's domain (DNS name)]
	OU =	[OV SSL]
	E =	[User's email]
	O =	[User's name (company)]
	2.5.4.97= (organizationIdentifier)	[Company identifier: • VATBG-XXXXXXXXX • NTRBG-XXXXXXXXX]
	L =	[User's locality]
	C =	BG or YY where YY is the country code under ISO 3166 where the User is registered
Public key	-	RSA(2048 bits)
SubjectAlternativeName	-	[DNS name]
Subject Key Identifier	-	[hash of „Public key "]
Authority Key Identifier	KeyID =	[hash of „Public key " of „Issuer"]
Issuer Alternative Name	URL =	http://www.b-trust.org
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.7.1.6 [1,1]Policy Qualifier Info: Policy Qualifier ID=CPS Qualifier: http://www.b-trust.org/documents/cps [2] Certificate Policy: Policy Identifier=2.23.140.1.2.2 [3] Certificate Policy: Policy Identifier=0.4.0.2042.1.7
Enhanced Key Usage	-	Server Authentication, Client Authentication, Secure Email
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.b-trust.org/repository/B-TrustOperationalACA.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-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-QcType (oid=0.4.0.1862.1.6)	id-etsi-qct-web (oid=0.4.0.1862.1.6.3)
		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 3.1. 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).
Under this policy, the Provider will identify the User under whose domain the domain (DNS) is registered. It also identifies the authorized person representing the User in front of the Provider and, if applicable, the domain user of the User.
The legal instrument in the authentication procedure prior to the issuance of a website certificate of authenticity to both parties - Supplier and User - includes compliance with ETSI and CA / B Forum requirements.

The Provider, through the its Registration Authorities, will perform all appropriate and authorized means to verify the information that will be certified by the issuance of a certificate of authenticity to a website (server, domain or organization), including through the use of national public registers - the Commercial Register, the BULSTAT register, other public registers of non-profit organizations / associations, and the existence of the domain and its affiliation to the User.
The Provider may request from the User additional information and documents for the purpose of secure identification / authentication and compliance.

4.3 Identification and authentication for certificate renewal

Under this Policy, the Provider does not renew Website Authentication Certificates. 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 revocation

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 revocation

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).

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 are common for the Organization Validation certificate.
3. The Provider, through the RA / LRA, admits a User to terminate a QCS Agreement.

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).
In addition to checking the User's existence, the RA / LRA checks the existence of the domain and its affiliation to the User. Checking is done in some of the following sites:

- for domains .bg – www.nic.bg
- for domains .eu – www.euric.eu
- for domains .eus – whois.nic.eus
- for other domains – whois.icann.org

for B-Trust DVC SSL and B-Trust OVC SSL certificates „wildcard" (*) is not admissible (i.e.TLD/Top Level Domains).

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 Website Authentication Certificates. Please see 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

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

Ad 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 Disclaimers of warranties

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).