



**B-TRUST® DISCLOSURE STATEMENT
OF THE QUALIFIED TRUSTED SERVICE PROVIDER
BORICA AD**

Version 2.0

20 May 2018

B-TRUST® DISCLOSURE STATEMENT

Document history				
Version	Author(s)	Date	Status	Comment
1.0	Dimitar Nikolov	13.01.2017	Approved	Initial release.
2.0	Dimitar Nikolov	20.05.2018	Approved	Added Electronic Seal information.

CONTENTS

1	Contact Information	5
2	Certificate type, Validation/Identification procedures and Usage	5
2.1	Types of certificate	5
2.2	Validation/Identification procedures	5
2.3	Usage.....	5
3	Reliance limits	5
4	Obligations of Users	6
5	Certificate Status Checking Obligations of Relying Parties	6
6	Limited Warranty and Disclaimer/Limitation of Liability	7
7	Applicable Agreements, CPS, CP	8
8	Privacy Policy/Statement	8
9	Refund Policy	8
10	Applicable Law, Complaints and Dispute Resolution	8
11	Conformity assessments, trust marks/logos, and audit	8
12	Document Identification	8
13	Registration and identity verification points.....	9

B-TRUST® DISCLOSURE STATEMENT

This document is a PKI Disclosure Statement/PDS of the Qualified Trusted Services Provider BORICA AD. This document is not intended to replace a B-Trust Certificate Policy or Certification Practice Statement, according to which qualified certificates are issued.

This statement, which follows the structure of Annex A of the document ETSI TS 319-411-1, is informative only and in no way substitutes the content of B-Trust Policy and Practice.

B-TRUST® DISCLOSURE STATEMENT

1 Contact Information

Any inquiries regarding this document can be addressed to:

Republic of Bulgaria
1612 Sofia, 41 "Tsar Boris III" Blvd.
Tel.: 0700 199 10
Fax: 02/ 981 45 18
E-mail: info@b-trust.org
Official web site of the Provider: www.b-trust.bg

2 Certificate type, Validation/Identification procedures and Usage**2.1 Types of certificate**

This statement applies only to qualified trusted services provided by B-Trust. Public key qualified certificates are issued by the B-Trust Operational Qualified CA and B-Trust Operational Advanced CA. The profile and any other constraints of the qualified public key certificate issued by these authorities are in compliance with ETSI EN 319 411-2.

2.2 Validation/Identification procedures

Qualified certificate are issued to after validation of the identity of the User. The validation process is performed by a Registration Authority/ Local Registration Authority (RA/LRA) of B-Trust or other person who is authorized to confirm the identity of the Holder/Creator of the certificate. A natural person, who requested issuance of a qualified certificate, is identified by his/her national identity document. In case of a person representing an organization, an authorization by the Holder/Creator to sign/seal and use the qualified certificate is required or a record of powers from an official state or commercial register.

The identification and authentication of an Applicant for a qualified certificate must meet the requirements specified in Section 3.2 (Initial Identification) of the B-Trust Certification Practice Statement. The RA/LRA shall identify and authenticate the information provided in the Application pursuant to Section 3.2 of the above document.

2.3 Usage

Qualified certificates issued by B-Trust Operational Qualified CA и B-Trust Operational Advanced CA must be used only in accordance with REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and in accordance with the document EN ETSI TS 319 411-2.

3 Reliance limits

The financial guarantee for qualified certificates issued by B-Trust Operational Qualified CA of Borica AD in relation to an individual event is BGN 600 000, and the total amount of the financial guarantees in relation to all such events cannot exceed the amount of BGN 600 000 BGN. Financial liability refers to 12-month periods, which is equivalent to the calendar year.

In order to manage the B-Trust operation and supervise the B-Trust users and personnel efficiently, all events registered in the system and having essential impact on the B-Trust security shall be recorded in logs.

In particular, B-Trust event logs include operations of registration, issuance, revocation and suspension of certificates, renewal procedures, issuance of qualified electronic time-stamps, validation of certificate status, key generation and other events having significant impact on the security and normal operation of B-Trust.

B-TRUST® DISCLOSURE STATEMENT

4 Obligations of Users

The Users are required to act in accordance with the B-Trust CP/CPS (B-Trust Policy and Practice) and the relevant Trusted Services Contract, concluded between them and Borica AD. In this context, the Users are responsible for:

- having basic knowledge and understanding of the proper use of public key cryptography and certificates;
- providing only correct information without errors, omissions or misuse;
- providing a properly filled and personally signed registration form;
- submitting an identity document and/or other document providing the information;
- verifying the content of the issued certificate prior to initial use and refrain from using it if it contains misleading or incorrect information;
- getting acquainted and accepting the terms and conditions of the B-Trust CPS (B-Trust Certification Practice Statement) and other relevant requirements and agreements;
- providing complete control over the private key by not sharing private codes and/or passwords;
- notifying the Registration Authority of any change in the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;
- suspending the use of the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances makes the information in the certificate misleading or inaccurate;
- notifying the Registration Authority immediately of any suspected or actual compromise of the private key and requesting the certificate to be suspended/revoked;
- immediately cease using the certificate upon:
 - (a) expiration or revocation of the certificate, or
 - (b) any suspicion or actual disclosure of the private key corresponding to the public key in this certificate, and immediately removing the certificate from the devices and/or software on which it has been installed;
- using the private key corresponding to the public key certificate to sign/seal other certificates;
- protecting the private key from unauthorized access.

The private keys for qualified certificates issued by the B-Trust Operational Qualified CA are generated on a Qualified Signature/Seal Creation Device (QSCD) in the presence of the Holder/Creator, who alone has control over the QSCD.

5 Certificate Status Checking Obligations of Relying Parties

The Relying parties are entitled to use qualified certificates only in accordance with the terms and conditions set forth in the B-Trust CPS (B-Trust Certification Practice Statement). It is their responsibility to verify the legal validity and the applicable law of these certificates. Before trusting information from the certificate, the Relying party must check the validity of the certificate, i.e. whether it is revoked/suspended, using the response from the B-Trust CRL or OCSP.

A relying party is committed to:

- verify that the electronic signature/seal is created using the private key corresponding to the public key in the Holder/Creator issued by B-Trust Operational Qualified CA or B-Trust Operational Advanced CA;
- verify that a signed/sealed message/document or certificate has not been changed after its signing/sealing;
- verify accurately and correctly (using application software/devices) the compliance of the level of trust of the received certificates with the security level of the cryptographic operations for the electronic signature/seal;

B-TRUST® DISCLOSURE STATEMENT

- consider invalid an electronic signature or certificate if it is not possible to determine the validity of the signature or of the certificate by means of application software and/or devices, or if the result of the verification is negative;
- trust only the qualified certificates that are used in accordance with the declared policy and the appropriate applicability specified by the Relying party, and their valid status was verified based on an effective Certificate Revocation List or B-Trust OCSP service.

6 Limited Warranty and Disclaimer/Limitation of Liability

B-Trust Operational Qualified CA and B-Trust Operational Advanced CA of Borica AD declares and guarantees to:

- provide services related to certificates issuance and repository services consistent with the B-Trust CPS (B-Trust Certification Practice Statement) and with the other operation policies and procedures of the Qualified Trusted Services Provider (QTSP);
- at the time of certificate issuance, implement procedure for verification of the accuracy of the information contained in it before issuing and initial use;
- apply a procedure to reduce the probability that the information contained in the certificate is misleading/inaccurate;
- support 24x7 publicly accessible and up-to-date document information;
- perform authentication and identification procedures in accordance with the CP/CPS and the internal policies, procedures and operations;
- provide certificate and key management services including certificate issuance, publication, renewal and revocation in accordance with the CP/CPS;

Borica AD shall not be liable for any absence/loss of B-Trust PKI service in the case of:

- natural disasters, war, telecommunications/energy disturbance, etc.;
- unauthorized use of the certificates or their use outside the appropriate use specified in the B-Trust QCA CP/CPS.

Limitations of Liability:

- B-Trust Operational Qualified CA and B-Trust Operational Advanced CA shall not be liable to Holders/Creators or any person in cases when this liability results from their negligence, fraud or intentional damage;
- B-Trust Operational Qualified CA and B-Trust Operational Advanced CA assume no liability in the cases of using certificates or associated public key/private key pairs for other purposes outside the appropriate use specified in the Policy of the certificate unless the use is in accordance with this Policy. The Holders/Creators will indemnify the B-Trust Operational Qualified CA and B-Trust Operational Advanced CA from and against any such liability and costs and any resulting costs and claims;
- B-Trust Operational Qualified CA and B-Trust Operational Advanced CA shall not be liable for any direct or indirect damages to any party caused as a result of uncontrolled breach of the provided trusted services;
- end-users shall be liable for any form of invalid information contained in the certificates, to Relying parties even though the information has been accepted by B-Trust;
- Holders/Creators shall compensate a Relying Party that has suffered losses as a result of breach on their part of the Trusted Services Contract.

B-TRUST® DISCLOSURE STATEMENT

7 Applicable Agreements, CPS, CP

The B-Trust CPS can be found in the B-Trust repository of documents at <https://www.b-trust.bg/documents>.

Accordingly, Trusted Services Contract related to Holders/Creators and an optional Contract for qualified validation of certificates regarding Relying parties can be found on the above B-Trust website.

8 Privacy Policy/Statement

B-Trust Operational Qualified CA and B-Trust Operational Advanced CA of Borica AD fully complies with the Personal Data Protection Act and other applicable legislation of the Republic of Bulgaria.

Any information about Users that is not disclosed through the qualified certificates issued by B-Trust or the through the CRLs is considered personal information. All the information contained in a qualified certificate, issued by B-Trust, in B-Trust CRLs, or provided by a publicly available service, shall not be considered confidential.

B-Trust keeps all events relating to the life cycle of keys managed by the B-Trust Operational Qualified CA and B-Trust Operational Advanced CA for ten years, then any certificate based on these records cease to be stored.

9 Refund Policy

B-Trust Operational Qualified CA and B-Trust Operational Advanced CA strives to provide the highest level of quality of the trusted services it offers and provides. Any User or Relying party may request revocation/termination of a certificate or service and refund, if the respective party is not satisfied with the B-Trust services, but only if B-Trust Operational Qualified CA and B-Trust Operational Advanced CA fails to fulfill its obligations and the obligations defined in the User Contract and in this document.

10 Applicable Law, Complaints and Dispute Resolution

The operational activity of B-Trust Operational Qualified CA and B-Trust Operational Advanced CA follows the general rules set out in the CPS (B-Trust Practice) and is in line with the applicable regulatory framework of the Republic of Bulgaria and applicable international acts. Disputes related to qualified services of B-Trust Operational Qualified CA and B-Trust Operational Advanced CA shall be settled initially through a conciliation procedure. If the complaint is not settled within 30 days of the commencement of the conciliatory process, the parties may refer the dispute to the appropriate court. In the event of disputes and complaints arising from the use of a certificate or services provided by B-Trust, Users shall undertake to notify Borica AD of the cause of the dispute.

11 Conformity assessments, trust marks/logos, and audit

Audits to verify the conformity with procedural and legal provisions, particularly the conformity with B-Trust CPS (B-Trust Certification Practice Statement) are performed every 24 months by an Authority for Conformity Assessment, based on Art. 20 of REGULATION 910/2014 EU (eIDAS).

12 Document Identification

This document has been registered by B-Trust and has an Object Identifier (OID) assigned: 1.3.6.1.4.1.15862.1.6.2.

B-TRUST® DISCLOSURE STATEMENT

13 Registration and identity verification points

B-Trust offices for registration and identification (verification of the identity) register Users/Applicants and verify their identity. The list of B-Trust offices can be found on the B-Trust website at <https://www.b-trust.bg/contacts>.