



B-TRUST® DISCLOSURE STATEMENT
of
THE QUALIFIED TRUSTED SERVICES PROVIDER (QTSP)
BORICA AD

Version: 1.0

July 2017

B-TRUST PUBLIC DISCLOSURE STATEMENT

TABLE OF CONTENTS

1. Contact Information 3

2. Certificate types, Validation/Identification procedures and Usage 3

3. Reliance limits..... 4

4. Obligations of Users 4

5. Certificate status checking obligations of relying parties 5

6. Limited warranty and disclaimer of liability 5

7. Applicable agreements/contracts, Policies and Practices of QTSP..... 6

8. Privacy Policy 6

9. Refund Policy 6

10. Applicable law, complaints and dispute resolution..... 6

11. Conformity assessment, trust mark/logo and audit 7

12. Identification of this document 7

13. Registration points, points of the identity confirmation..... 7

B-TRUST PUBLIC DISCLOSURE STATEMENT

This document is the PKI Disclosure Statement/PDS of the Qualified Trusted Services Provider (QTSP) Borica AD (referred to as B-Trust®). This document does not substitute or replace the B-Trust Certificate Policy/Certification Practice Statement (CP/CPS) under which qualified certificates are issued.

This statement, which follows the structure of Annex A of the document ETSI TS 319-411-1, is merely informative and in no way replaces the provisions of the aforementioned documents.

1. Contact Information

Queries regarding this document (PDS) shall be addressed to:

Republic of BULGARIA
1612 Sofia
41 "Tsar Boris III" Blvd.
BORICA AD
Official Web site: www.b-trust.org
E-mail: info@b-trust.org
Tel.: 02/ 92 15 115
Fax: 02/ 981 45 18

2. Certificate types, Validation/Identification procedures and Usage

Certificate Types

This statement applies only to qualified certification services provided by B-Trust. Public key qualified certificates are issued by the B-Trust PKI QCA. Profile and any other limitation of certified public key certificate issued by B-Trust QCA shall be compliant with the ETSI EN 319 411-2.

Validation/identification procedure

Qualified certificate shall be issued to an individual after verification of their identity. Verification of the individual shall be carried out by a Registration Authority/ Local Registration Authority (RA/LRA) of B-Trust or other person who is authorized to confirm the identity of the Titular of the certificate. The individual, requesting issuance of a qualified certificate shall be identified by their national identity document. In case of individuals associated or acting on behalf of an organization, an authorization of the Titular is required in order to sign and use the qualified certificate or the official government or trade register record of the powers is required.

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 CP/CPS (B-Trust Certification Practice Statement and Certification Policy). The RA/LRA shall identify and authenticate information provided by the Applicant in the Application pursuant to Section 3.2 of the above document.

Usage

Qualified certificates issued by B-Trust PKI QCA 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.

B-TRUST PUBLIC DISCLOSURE STATEMENT

3. Reliance limits

The financial guarantee of Borica AD in relation to an individual event amounts to 600 000 BGN, where the total financial guarantees in relation to all such events cannot exceed the amount of 600 000 BGN. Financial liability applies 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 associated with registration, issuance, revocation/termination and temporary suspension of certificates, renewal procedures, issuance of time stamps (qualified electronic time stamps), validation of a certificate's status, key generation and others event having significant importance on the security and normal operation of B-Trust.

4. Obligations of Users

Users are required to act in compliance with the B-Trust CP/CPS and the relevant Contract for certification services, concluded between them and Borica AD. In this context, 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 (Application);
- supplementing such information with a proof of identity and/or document for provision of information;
- verifying the content of the issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information;
- reading and agreeing to all terms and conditions of the B-Trust CP/CPS (Certification Practice Statement and Certification Policy) and other relevant regulations and agreements;
- ensuring complete control over the private key by not sharing private keys 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;
- invalidating 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 that the certificate be revoked/terminated;
- 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, as well immediately removing the certificate from the devices and/or software on which it has been installed;
- refraining to use the private key that corresponds to the public key to sign other certificates;
- protecting the private key from unauthorized access.

B-TRUST PUBLIC DISCLOSURE STATEMENT

Private keys for qualified certificates shall be generated on a Qualified Signature Creation Device (QSCD) in the presence of the Titular, who alone has control to the QSCD.

5. Certificate status checking obligations of relying parties

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

A relying party is committed to:

- verify that an electronic signature has been created by means of a private key corresponding to a public key in the Titular's certificate issued by B-Trust QCA;
- verify that a signed message/document or a certificate have not been modified after signing it,
- 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;
- consider an electronic signature or certificate as invalid if by means of applied software and/or devices it is not possible to determine the validity of the signature or of the certificate or if the result of the verification is negative;
- trust only these qualified certificates that are used in accordance with the declared policy and are appropriate for applicability ranges that were specified by the relying party, and their valid status was verified on the basis of the actual Certificate Revocation List or B-Trust OCSP service.

6. Limited warranty and disclaimer of liability

B-Trust QCA of Borica AD declares and guarantees to:

- Provide services related to certificates issuance and repository services consistent with the B-Trust CP/CPS and other operation policies and procedures of the Qualified Certification 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 first use;
- Implement a procedure for reducing the possibility for misleading/incorrect information contained in the certificate;
- Maintain 24 x 7 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/termination of a certificate in accordance with the CP/CPS;

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

- Due to natural disasters, war, telecommunications/energy disturbance, etc.
- Due to unauthorized use of certificates or their use outside the scope of the B-Trust QCA CP/CPS.

B-TRUST PUBLIC DISCLOSURE STATEMENT

Limitations of Liability:

- B-Trust QCA shall not be liable for Titulars or any person in cases when this liability results from their negligence, fraud or willful misconduct;
- B-Trust QCA assumes no liability in the cases of using certificates or associated public key/private key pairs for other purposes outside the scope of the Policy stated in the certificate unless the use is in accordance with this Policy. Titulars will indemnify the B-Trust QCA from and against any such liability and costs and claims arising there from;
- B-Trust QCA shall not be liable to any direct or indirect damages to any party caused as a result of uncontrolled breach of the provided certification services;
- End-Users shall be liable for any form of invalid information contained in the certificate to relying parties even though the information has been accepted by B-Trust;
- Titulars shall compensate a Relying Party that suffered losses as a result of breach of the Certification Services Contract by them.

7. Applicable agreements/contracts, Policies and Practices of QTSP

B-Trust Certification Practice Statement and Certification Policy can be found in the B-Trust repository of documents and at: <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

Accordingly, Certification Services Contract related to Titulars and an optional contract for qualified validation of certificates regarding Relying parties can be found on the abovementioned B-Trust website.

8. Privacy Policy

B-Trust QCA of Borica AD fully complies with the Personal Data Protection Act and other applicable legislation in the Republic of Bulgaria.

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

B-Trust stores all events relating to the life cycle of keys managed by the B-Trust QCA for ten years. After this period any certificate based on these records shall not be stored.

9. Refund Policy

B-Trust QCA makes efforts to provide the highest level of quality of the certification services it offers. Any User or Relying party may request revocation/termination of a certificate or service and a refund, if the relevant party is not satisfied with the B-Trust services, but only if B-Trust QCA fails to fulfill its obligations and the obligations defined in the User Contract and the present document.

10. Applicable law, complaints and dispute resolution

The operational activity of B-Trust QCA shall follow the general rules set out in the CPS (B-Trust Certification Practice Statement and Certification Policy) and shall be in compliance with the applicable regulatory framework in the Republic of Bulgaria and the applicable

B-TRUST PUBLIC DISCLOSURE STATEMENT

supranational acts. Disputes related to B-Trust QCA qualified services 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 following the usage of an issued certificate or services delivered by B-Trust, Users shall notify Borica AD about the cause of the dispute or complaint.

11. Conformity assessment, trust mark/logo and audit

Audits checking the conformity with procedural and legal regulations, particularly the conformity with B-Trust CP/CPS (B-Trust Certification Practice Statement and Certification Policy) shall be carried out at every 24 month by a Conformity Assessment Body based on Art.20 of eIDAS.

12. Identification of this document

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

13. Registration points, points of the identity confirmation

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