



**BORIKA AD**

**B-TRUST® QTSA DISCLOSURE STATEMENT**

Version: 1.0

July 2017

**TABLE OF CONTENTS**

1 Entire agreement ..... 3

2 Contact Information ..... 3

3 Electronic time-stamp types and usage ..... 3

4 Reliance limits..... 4

5 Obligations of subscribers ..... 4

6 TSU public key certificate status checking obligations of relying parties..... 4

7 Limited warranty and disclaimer/Limitation of liability ..... 5

8 Applicable agreements and practice statement..... 5

9 Privacy Policy ..... 5

10 Refund Policy ..... 6

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

12 TSA and Repository licenses, trust marks and audit..... 6

13 Identification of this document ..... 6

**B-TRUST PUBLIC DISCLOSURE STATEMENT**

---

**1 Entire agreement**

This document is the QTSA Disclosure Statement, hereinafter referred to as the TDS, of the Borica AD Qualified Time Stamp Authority (referred to as B-Trust® QTSA). This document does not substitute or replace Policy and security requirements of B-Trust QTSA (B-Trust TP/TPS) under which qualified time-stamps are issued.

This statement, which follows the structure of Annex B of the document ETSI TS 319-421, is merely informative and in no way replaces the provisions of the aforementioned documents.

**2 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](http://www.b-trust.org)  
E-mail: [info@b-trust.org](mailto:info@b-trust.org)  
Tel.: 02/ 92 15 115  
Fax: 02/ 981 45 18

**3 Electronic time-stamp types and usage**

B-Trust QTSA offers a single class of time-stamp token under the policy identifier 0.4.0.2023.1.1. Time-stamps tokens produced under 0.4.0.2023.1.1 are in the form prescribed by RFC 3161 and subsequent standards. Time stamping protocol and time-stamp token profile are in compliance with ETSI EN 319 2422. TSA qualified trust service accepts the following hash algorithms:

- SHA-256 (recommended)
- SHA-384
- SHA-512

B-Trust time-stamp token signatures are encrypted using RSA 2048. Each time-stamp token includes the public keys necessary for verification, and can be verified against B-Trust QTSA's certificate or the known and published audit public key certificate of the source time-stamping unit (TSU) of QTSA. Certificates can be retrieved from B-Trust Repository at: <https://www.b-trust.org/bg/elektronni-podpisi/udostoveritelni-verigi>.

Borica AD preserves the time stamps in an Archive for five (5) years. The Archive will provide B-Trust QTSA the ability to extend validity of all constituent time-stamps through the application of newer signatures with greater strength.

Qualified time-stamp tokens issued by B-Trust QTSA 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*, in accordance the document EN ETSI TS 319 421 and other applicable legislation in Republic of Bulgaria. These time-stamp tokens can be used for any purpose –

## **B-TRUST PUBLIC DISCLOSURE STATEMENT**

extended electronic signature formats, Archives, registers, electronic forms, etc., except the protection (e.g. time-stamping) of a timestamp produced by a TSA other than B-Trust QTSA.

### **4 Reliance limits**

The time signal in B-Trust QTSA is provided via GPS-NTP. The time-stamping service uses this time signal and a set of NTP servers as time sources. With that setup the time-stamping service reaches an accuracy of the time of (+/-500ms) or better with respect to UTC.

For more information see Section 7.2.2 of the complete document B-Trust QTSA Policy and security requirements (TP/TPS) at <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

QTSA's Event Logs are maintained for 5 years.

### **5 Obligations of subscribers**

Subscribers are required to act in accordance with the B-Trust QTSA TP/TPS (Policy and security requirements) and the relevant Subscriber Agreement. In this context, Subscribers are responsible for:

- having a basic understanding of the proper use of time-stamps;
- providing only correct information without errors, omissions or misrepresentations;
- verifying the content of a newly issued time-stamp 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 QTSA TP/TPS and other relevant regulations and agreements;
- invalidating the time-stamp immediately if any information included in the time-stamp is misleading or inaccurate, or if any change of circumstances, makes the information in the time-stamp misleading or inaccurate.

For more information see Section 6.2 of the complete document TP/TPS and security requirements at <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

### **6 TSU public key certificate status checking obligations of relying parties**

Before placing any reliance on a Time-Stamp, Relying Parties must verify that the time-stamp token has been correctly signed and that the associated TSU certificate is valid (not listed on the B-Trust PKI Certificate Revocation List/CRL at <https://www.b-trust.org/bg/spravki-i-uslugi/info/prekrateni-i-spreni-podpisi>). If this verification takes place after the end of the validity period of the certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.

For more information see Section 6.4 of the complete document TSA TP/TPS and security requirements at <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

**B-TRUST PUBLIC DISCLOSURE STATEMENT**

---

**7 Limited warranty and disclaimer/Limitation of liability**

B-Trust QTSA of Borica AD warrants and promises to:

- Provide time-stamp tokens issuance and repository services consistent with the Policy and security requirements and other Operations Policies and Procedures;
- At the time of time-stamp token issuance, implement procedure for verifying accuracy of the information contained within it before installation and first use;
- Maintain 24 x 7 publicly-accessible repositories with current information;
- Provide QTSA/TSU certificate(s) and key management services including certificate issuance, publication, renew and revocation in accordance with the B-Trust CP/CPS;

The B-Trust QTSA does not liable for any loss of the Time Stamp service:

- Due to war, natural disasters, telecommunications/energy disturbance, etc.
- Due to unauthorized use of time-stamp tokens or using it beyond the prescribed use (TP/TSP) defined for the tokens.

Limitations on Liability:

- B-Trust QTSA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- B-Trust QTSA assumes no liability whatsoever in relation to the use of time-stamp tokens issued under TSA TP/TPS for any use other than in accordance with that Policy. Relying Party will immediately indemnify the B-Trust QTSA from and against any such liability and costs and claims arising there from;
- B-Trust QTSA will not be liable to any party whatsoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Subscribers are liable for any form of misrepresentation of information contained in the time-stamp token to relying parties even though the information has been accepted by B-Trust QTSA.

**8 Applicable agreements and practice statement**

Relevant content can be found in B-Trust Repository at <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

In particular, applicable agreements include Obligations of Subscribers and Obligations of Relying Parties described in B-Trust QTSA TP/TPS available at <https://www.b-trust.org/bg/elektronni-podpisi/dokumenti>.

**9 Privacy Policy**

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

## **B-TRUST PUBLIC DISCLOSURE STATEMENT**

Any and all information made public in a qualified time-stamp token issued by B-Trust QTSA or its Repository, or by a publicly available service shall not be considered confidential.

B-Trust retain all events relating to the life cycle of time-stamp tokens issued by the QTSA for at least five (5) years after any time-stamp token based on these records ceases to be valid. Relations between Subscriber, Relying Party and B-Trust QTSA are based on trust.

### **10 Refund Policy**

For the QTSA with SLA the service is paid according to the contractual terms for delivery and use of the service. The Refund Policy for QTSA is described in the relevant Service Level Contracts. In addition to that, a Corporate TSP may charge fees for its services.

B-Trust QTSA makes efforts to secure the highest level of quality of its services. If a Subscriber or a Relying Party is not satisfied with the QTSA services, they can stop using Time Stamp service.

### **11 Applicable law, complaints and dispute resolution**

Operating of B-Trust QTSA is based on the general rules stated in the document Policy and security requirements and it is in accordance with the legal acts in force in the Republic of Bulgaria and the applicable supranational acts. Disputes related to B-Trust's qualified services will be first settled through conciliation. If the complaint is not settled within 30 days of the commencement of conciliatory process, the parties can hand over the dispute to appropriate court. In the instance of the occurrence of arguments or complaints following the usage of an issued time-stamp token(s) or services delivered by B-Trust, subscribers commit themselves to notify Borica AD of the reason for the argument or complaint.

### **12 TSA and Repository licenses, trust marks and audit**

Audits checking the consistency with procedural and legal regulations particularly the consistency with B-Trust QTSA Policy and security requirements (TS/TSP) is carried out at every 24 month by a conformity assessment body on a basis of art. 20 of eIDAS.

### **13 Identification of this document**

This document has been registered with B-Trust of Borica AD and has been assigned an Object Identifier 1.3.6.1.4.1.15862.1.6.4.