POLICY AND PRACTICE STATEMENT ON THE PROVISION OF QUALIFIED SERVICES BY BORICA AD FOR ISSUING QUALIFIED TIME-STAMP TOKENS OF B-TRUST® QUALIFIED TIME-STAMPING AUTHORITY

Version 2.0

March 1, 2020

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.2	Dimitar Nikolov	13.01.2017	Approved	Amendments to the document related to the implementation of Regulation 910/2014.

Document history				
Version	**Author(s)**	**Date**	**Status**	**Comment**
1.3	Dimitar Nikolov	01.07.2018	Approved	Change of the profile of the Time-stamp certificate. Legislative update.
2.0	Dimitar Nikolov	01.03.2020	Approved	Technical corrections

CONTENTS

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;
- Specifies the requirements on the provision of Qualified Time-Stamps to Users by the Qualified Trust Services Provider (QTSP) BORICA AD through its administratively separate unit - Qualified Time-Stamping Authority;
- Constitutes the General Conditions within the meaning of Art. 16 of the Obligations and Contracts Act (OCA);
- Includes a detailed description of the policy and practice in providing qualified electronic time- stamps by the Provider and is a public document with the purpose to establish the conformity of the activity of the Provider BORICA AD with the legal framework;
- May be changed by the QTSP and each new version of the “Timestamp Policy and Timestamp Practice Statement on the Provision of Qualified Services by BORICA AD in Issuing Qualified Time-Stamp Tokens” shall be published on the Provider’s website.

This document is prepared in accordance with:

- Regulation (EU) № 910/2014 of the European Parliament and of the Council on Trust Services and refers to information contained in the internationally ratified recommendations, specifications and standards prepared in accordance with this Regulation;
- Electronic Document And Electronic Certification Services Act;

The content and structure of this document refers to the information contained in the following ratified international guidelines, specifications and standards:

- RFC 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- EN 319 422: Time-stamping protocol and time-stamp token 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

1 INTRODUCTION

The Qualified Trust Service Provider "BORICA" AD, hereinafter referred to as "QTSP", under the terms of The Electronic Document and Electronic Trust Services Act (EDETSA), issues Qualified Time-Stamp Tokens (QTST).

The Qualified Time-Stamp Tokens provide calibrated official time to certify in a reliable and traceable manner the availability of digital data, including contents of an electronic document before a particular moment. When attached to a QES, the QTST verifies that the electronic signature is created before the time indicated in the QTST.

This document sets out the general terms and conditions that the QTSP follows when issuing Qualified Time-Stamp Tokens, and in operation and maintenance of this service.

The authority through which the QTSP issues and maintains QTST strictly observes the Policy and Practice contained herein. This Policy and Practice mainly address the above-described scenario of applicability of the QTST to QES, but they are also applicable to other scenarios.

Considering that the QTST provided by B-Trust Qualified Time-Stamping Authority (QTSA) are applicable to different scenarios, the QTSP "BORICA" AD has published general Policy and Practice, which form this document.

The QTSP "BORICA" AD operates the B-Trust QTSA and publicly provides QTST services at the following web address: „http://tsa.b-trust.org".

2 SCOPE

This document sets out the requirements to the QTSP Policy regarding the issued QTST and defines the Practice for the operation and management of B-Trust QTSA, in order to let the users and the relying parties, who have concluded Contract for the use of the B-Trust trust services or have signed Service Level Agreement to such Contract, have description and assessment of security of the provided qualified service for issuing QTST.

The B-Trust Qualified Time-Stamping Services (TSS) use the common infrastructure of B-Trust of "BORICA" AD as a Qualified Trust Service Provider under the EDETSA and Regulation 910/2014.

The requirements and conditions contained in the document mainly address B-Trust Qualified TSS in the use and maintenance of QES. They are based on the use of PKI cryptography, public key certificates and source of accurate (official) time, but they could also be used for other purposes.

Users and relying parties should use this document to obtain complete description and assessment of security of the provided QTST.

3 Terms and definitions

B-Trust QTSA (B-Trust Qualified Time-Stamping Authority) – Certification Authority in the infrastructure of B-Trust that provides QTST.

TST (Time-Stamp Token) – electronically signed Time-Stamp Token by B-Trust QTSA for the existence of digital content of an electronic document before particular time, specified in the certificate and for the lack of any changes to this content after that moment. When attached to an electronic signature, the certificate creates irrevocability of the signature in time.

Qualified ***TSS (***Qualified ***Time-Stamping Services)*** – qualified trust services for generating secure QTST, keeping records of issued and delivered QTST, verification and validation of the QTST.

TSA-system – combination of organized IT products and components, via which B-Trust QTSA provides QTST.

Coordinated Universal Time (UTC) – timeframe based on seconds, as per ITU-R Recommendation

TF.460-5.

UTC(k) – timeframe according to laboratory "k", which resembles UTC, for the purpose of achieving accuracy of plus/minus 100 ns (ITU-R Recommendation TF.536-1 [TF.536-1]).

Service Level Agreement (SLA) – Negotiated agreement for the level of services in the provision of Qualified TSS.

GPS – *Global Positioning System* - Global system for satellite positioning

NTP – *Network Time Protocol* is a protocol for synchronization of clocks in computer systems

NTP Stratum – Stratum in NTP hierarchical order of time sources, determining the shifting of the server compared to a referent time source (Stratum 0).

The other specific terms used in this document follow the definitions given in the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD" (B-Trust CPS-eIDAS), which is published and available at the website of the QTSP "BORICA" AD (https://www.b-trust.bg/documents).

4 Concept

4.1 Qualified Time-Stamping Services (Qualified TSS)

The infrastructure of B-Trust used for the provision, servicing and maintenance of Qualified TSS, includes:

- B-Trust Qualified Time-Stamping Authority - operates Qualified TSS, generates QTST, maintains the register and the archive of issued QTST and manages the service;
- System logistics – accepting online orders and delivery of QTST, verification and validation of issued QTST.

The system logistics includes access to a source of accurate time (UTC(k)).

This separation is conditional for the purpose of the document and imposes no restrictions for the use of QTST.

4.2 B-Trust Qualified Time-Stamping Authority (B-Trust QTSA)

„B-Trust Qualified Time-Stamping Authority" is the certification authority in the infrastructure of B-Trust, as described in section 4.1, which provides QTST in accordance with the Policy and Practice of QTSP, described in this document, and builds trust with the QTST users.

4.3 Users

The users of QTST are subscribers or relying parties of B-Trust, in accordance with the "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD" (B-Trust CPS-eIDAS), as well as any other individual or legal entity, who has concluded individual contract with BORICA AD for Qualified TSS, and respective Service Level Agreement (SLA).

4.4 Policy and Practice

This document defines the general elements of the policy and practice of the QTSP in providing QTST in its capacity as general conditions.

The Policy sets out the conditions and rules, to which the QTSP adheres. The Practice describes how the QTSP implements the described Policy, and the procedures it follows when providing QTST.

B-Trust QTSA issues QTST to each interested party, following standard (non-guaranteed) service level. A rule in the B-Trust QTSA Policy is to issue QTST following the practice and procedures included in this document.

Any user who needs guaranteed service level for QTST has to conclude an Agreement for B-Trust Qualified TSS and SLA.

The payment for the "Qualified Electronic Time-Stamping" service with Service Level Agreement is according to the contractual terms of delivery and use of the service.

The Provider's practice in the provision of QTST is performed by the B-Trust Qualified Time-Stamping Authority and is identified by:

Certification Authority	OID
B-Trust Qualified Time-Stamping Authority	O.I.D. = 1.3.6.1.4.1.15862.1.6.3

The Provider's policy in the provision of QTST is identified by the following identifiers:

Qualified Certificate	Name	OID
QTST	B-Trust Qualified Time-Stamp Policy	O.I.D. = 1.3.6.1.4.1.15862.1.6.3 O.I.D. = 0.4.0.2023.1.1

4.5 Management of the Provider's Policy and Practice

1. The Provider's Policy and Practice are subject to administrative management and supervision by the Board of Directors of BORICA AD.
2. Changes, modifications and additions are admissible, which do not affect the rights and obligations arising from this document and the standard contract between the Provider and the Users, after concordance and approval by the Board of Directors.
3. Each new version or edition of this document, submitted and approved, shall be immediately published on the Provider's website.
4. Any comments, inquiries and clarifications regarding this document may be addressed to:
   - E-mail address of the Certification Authority: info@b-trust.org;
   - E-mail address of the Provider: info@borica.bg;
   - tel.: (02) 9215 115 and fax: (02) 981 45 18

5 Policy of B-Trust Qualified Time-Stamping Authority

5.1 General overview

The Policy of B-Trust QTSA is the set of rules, which denote the applicability of QTST for a particular application or application class with common requirements to the security level.

B-Trust issues QTSTs in accordance with "ETSI TS 102 023 Policy Requirements for time-stamping authorities" and the present Policy.

The provided accurate calibrated time per UTC (Coordinated Universal Time) is accurate to 0.5 seconds. When applying one-second adjustment to UTC (leap second) B-Trust QTSA does not issue QTST within this second.

The System logistics of B-Trust QTSA uses GPS source of accurate time for ensuring maximum accuracy.

The service certificate of the Provider's B-Trust QTSA is a public key certificate, electronically stamped with the Provider's root private key. With the private key of B-Trust QTSA, QTST are electronically stamped on the submission of contents of an electronic document by a User and/or by a Relying party.

This certificate of the B-Trust QTSA, certifying the belonging of the public RSA key (2048 bits), used to verify QESeal in the issued QTST, has a profile in accordance with the document "ETSI EN 319 422 Time-Stamping Protocol and time-stamp token profiles"

The electronic time stamps of the Provider, which are accompanied by the official certificate of B-Trust Qualified Time-Stamping Authority, are qualified.

The profile of the B-Trust Qualified Time-Stamping Authority certificate is specified below.

Field	Attributes	Value/Meaning
Version	-	V3
Serial number	-	00 ae c4 79 46 76 d5 0e d1
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2018-06-01T14:33:23Z
Validity to	-	2023-05-31T14:33:23Z
Subject	CN =	B-Trust Qualified Time-Stamping Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(2048 Bits)
Subject Key Identifier		57 96 93 11 a2 5c 92 ce fb 23 9e 6a d8 85 0c 50 b7 b0 3a a4
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0
Issuer Alternative Name	URL=	http://www.b-trust.org
Subject Alternative Name	URL=	http://tsa.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) 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-TrustOperationalQCAOCSP.cer
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage (critical)	-	Time-Stamping (1.3.6.1.5.5.7.3.8)
Thumbprint (Sha1)		f9 c0 c3 9a 43 77 73 b0 bc 72 22 df ee 1d a7 92 cf aa 8a d9
Thumbprint (Sha256)		00 35 5f ce 1b ee ae 61 e8 6e 79 a6 83 64 f4 b5 23 4a 1a df ea b6 f0 97 14 0b 12 03 39 8c 08 36
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-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf language=en

B-Trust uses the following algorithms for electronic signature and data protection:

Algorithm	Name
Hash algorithm:	SHA256
Asymmetric algorithms:	RSA

5.2 Identifier

B-Trust QTSA issues QTST for two types of data contents:

- of QES;
- of random electronic document/statement.

The requirements to the above-mentioned QTST are identical and consistent with those with arbitrary use of QTST, according to “ETSI EX 319 421” with policy “OID = 0.4.0.2023.1.1“

Generally, B-Trust QTSA issues QTST with Policy identifier:

Provider’ s policy	Identifier (OID)
B-Trust TST (QTST)	O.I.D. = 0.4.0.2023.1.1

With a negotiated SLA, B-Trust QTSA issues QTST with an identifier described in the particular agreement.

5.3 Applicability

The policy according to this document does not restrict the applicability of the provided QTST by B-Trust Qualified Time-Stamping Authority.

QTST may be used when creating extended formats of QES (XAdES, CAdES, PAdES), in making archives, registers, electronic forms, etc., at the discretion of users.

5.4 Conformity

If required, B-Trust QTSA may use the Policy identifier specified in section 5.2.

The QTST issued are electronically signed by B-Trust QTSA in the capacity of certification authority, identified with its certificate.

The certificate of B-Trust QTSA is used by user/relying party for validity verification of the QES in the provided QTST.

6 Obligations of B-Trust QTSA

6.1 General obligations:

- To meet all requirements specified in section 7 of the document for implementation of the Policy;
- To ensure conformity with the requirements specified herein of the Policy, even when the functionality of B-Trust QTSA or a part thereof is provided under an agreement;

- To ensure conformity of the provided QTST with the procedures documented in the Practice Statement.

6.2 Obligations to users

- To observe the general obligations;
- To ensure constant access to the QTST, without the planned technical interruptions and preventive maintenance activities;
- To implement and operate adequate and secure communication infrastructure;
- To provide calibrated time (UTC);
- To indicate in the QTST certified time with accuracy to 500 milliseconds;
- To maintain the QTST in accordance with conventional international recommendations and specifications;
- To maintain simultaneously multiple sessions of orders for issuance of QTST;
- Option to scale the productivity (QTST/sec.);
- To use technical equipment corresponding to the general requirements for reliability and security of technical means of the QTSP pursuant to the legal provisions of the EDETSA;
- To not violate any licenses, intellectual property or other rights in the issued QTST;
- To not allow modifications of digital data after the issuance of QTST, without this be proven.

6.3 User Obligations

Users who obtain QTST should verify the electronic signature of B-Trust QTSA and check the validity of the certificate of the authority.

B-Trust QTSA does not require electronic authentication and does not impose any other restriction on the QTST users.

6.4 Relying Party Obligations

General obligation of any third relying party is to verify the qualified electronic stamp in the QTST. They should check the validity of the certificate of B-Trust QTSA. If the period of validity of the certificate has not expired, the relying party should:

- verify that this certificate is not in the CRL;
- verify the degree/level of security of the used hash function for the QTST;
- verify the degree/ level of security of used algorithms, as well as the length of the pair key for QES in the QTST.

6.5 Responsibility of B-Trust QTSA

B-Trust QTSA operates TSS in complete accordance with the Policy and Practice of QTSP according to the document “Certification practice statement for the provision of qualified certificates and trust services by BORICA AD” and the present document. B-Trust QTSA shall not publish/present additional information regarding the provided QTST, unless a user/third relying party has concluded an Agreement for use of B-Trust QTS and SLA with the QTSP.

B-Trust QTSA shall not be held responsible of any problems occurred during the provision of QTS, resulting from events and causes falling beyond the competence and scope of the QTSP activity.

“BORICA” AD, in the capacity of QTSP under the EDETSA, is responsible under this Act and its legal provisions. The QTS is a type of trust service with “irrevocability” profile and requires efficient control on all elements and events in the work of B-Trust QTSA – procedures, QTS-transactions, key material, personnel, etc.

7 Practice and procedures of B-Trust QTSA

All procedures, control mechanisms and technical characteristics of B-Trust QTSA, specified herein, supplement those specified in the document “Certification practice statement for the provision of

qualified certificates and trust services by BORICA AD" (B-Trust CPS-eIDAS), especially in the parts regulating the activity of "BORICA" AD in the capacity of QTSP providing qualified trust services.

The present terms and procedures form the basis of the operative work of B-Trust QTSA.

7.1 Key management

7.1.1 Generating key pairs

The pair of RSA keys is generated in a crypto module with a certified security level FIPS 140-2 Level 3 of the personnel of the QTSP that has the right to perform this function. The generated pair of RSA keys has length of 2048 bits.

The description and the roles of the QTSP personnel are specified in the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD". The environment for generating key pair by a QTSP Certification authority is described in the same document.

7.1.2 Private Key protection

The generated private key of B-Trust QTSA is stored in a crypto module (HSM) with a certified level of security FIPS 140-2 Level 3.

A special safe keeps the relevant copies of smart cards together with parts of the private key of B-Trust QTSA.

7.1.3 Distribution of the public key

The public key of B-Trust QTSA is certified for QESeal, issued from the Root Certification Authority (B-Trust Root Qualified CA) in the PKI hierarchy for issuance of certificates for qualified electronic signature.

This certificate with public key of B-Trust QTSA is entered in the qualified TSS system. In addition, the certificate of B-Trust QTSA is published on the website of the QTSP and may be freely delivered to the personal computers of users who use a B-Trust QTS.

7.1.4 Extending the duration and/or re-issue of certificates

The period of validity of the certificate of B-Trust QTSA is 5 years. After expiry of this period, the term of validity of the certificate is extended for a period of 1 year. After this period, a new pair of keys is generated, the private key of which is stored in the crypto module (HSM), while the public key is certified through the issue of a new certificate of B-Trust QTSA. The pair of keys with expired term of validity is stored as follows:

- private key – stored for a period of 10 years;
- public key – stored for a period of 10 years.

7.2 Timestamping

The server software of B-Trust QTSA implements the technical certification of "ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles".

The communication software of the B-Trust QTSA system maintains the communication with customers of the Qualified TSS with protocols: TCP/IP, HTTP/HTTPS.

7.2.1 TST

The profile of requests/responses of B-Trust QTSA system conforms to the above-mentioned technical specifications and includes the following attributes/parameters:

1. The request for issuance of QTS includes:

Attribute name	Value	Description
Version	1	version

Message Imprint	Hash Algorithm: […]	hash algorithm used (Sha256)
	Hash Value: […]	hash value of electronic signature of signed electronic document or other digital data
Requested Policy	[option]	identifier of policy to be certified in QTST
Nonce	[option]	additional data to be included in QTST
Certificate Request	[option]	option if QTST should contain certificate of B-Trust QTSA
Extensions	[option]	additional extensions

2. The response (TSR) includes:

Attribute name	Value	Description
Version	1	version
Policy	[Policy OID]	identifier of the policy on Time-Stamp issuance
Message Imprint	Hash Algorithm: […]	hash algorithm used (Sha256)
	Hash Value: […]	hash value of the electronic signature of signed electronic document or other digital data supplied to the provider
Serial Number	[…]	unique identification number
Generated Time	[…]	time of submission of electronic signature (certified time under UTC)
Accuracy	500	accuracy in milliseconds = 0.5 seconds
Ordering	true	
Nonce	[option]	additional data required in TSQ;;
Tsa	CN = B-Trust Qualified Time-Stamping Authority OU = B-Trust O = BORICA AD OrganizationIdentifier(2.5.4.97) = NTRBG-201230426 C = BG	
Extensions	[option]	additional extensions
Digital Signature	[…]	identifiers of the algorithms used for the creation of electronic signature (Sha256RSA)
	Signature Value: […]	electronic signature of QTST
	[Certificate of B-Trust TSA]	the certificate of qualified electronic seal of the Trust Service Provider

7.2.2 UTC synchronization

B-Trust QTSA uses hardware source of accurate calibrated time with high accuracy. The synchronization of UTC with the time source is automatic, based on NTP protocol, after establishment of a difference between the source and the time in the system.

In the event of any problems occurred in the hardware time source and until replacement of the same with a spare source, web-based timeservers shall be used as source of accurate time. Synchronization is the basis of at least two web-sources of time via NTP protocol.

The accuracy of the certified time is with deviation up to 0.5 seconds from UTC. B-Trust QTSA does not issue time certificates in a case of larger deviation, lack of UTC synchronization or when applying one-second adjustment to the accurate time (leap second).

7.3 Management and operation

7.3.1 Security management

All aspects of security management of B-Trust QTSA are in accordance with the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD".

In the event of a break in the security of the B-Trust QTSA service or loss of data authenticity, all registered users of the service shall be notified at the earliest opportunity.

7.3.2 Risk evaluation

All aspects of risk evaluation are in accordance with the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD".

7.3.3 Personnel controls

The features of the QTSP personnel and the appointed positions are in accordance with the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD".

7.3.4 Access control

Physical control to the environment of the QTSP and of B-Trust QTSA is in accordance with the document "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD".

7.3.5 Secure environment

The crypto module (HSM) with certified security level FIPS 140-2 Level 3 is the operational environment for storing the private key and for electronic signing of QTSTs, which are delivered to users.

7.3.6 Termination of TSA

In the event of termination of B-Trust QTSA the relevant procedures from "Certification practice statement for the provision of qualified certificates and trust services by BORICA AD" shall be performed.