POLICY AND PRACTICE

OF

B-TRUST TIME STAMP AUTHORITY

Version 1.1

1 September 2015

1 Introduction

Certification Service Provider "BORICA – BANKSERVICE" AD, hereinafter referred to as "CSP", by virtue of Art. 19 of the Law on Electronic Document and Electronic Signature (LEDES) issues and maintains certificates of Qualified Electronic Signature (QES) and Time Stamp Tokens (TST).

Time Stamp Tokens provide calibrated official time to certify in a reliable and traceable manner the availability of digital data, including the contents of electronic document before particular moment. When attached to QES in accordance with Art. 40 of the LEDES, TST verifies that the electronic signature is created before the time indicated in TST.

This document sets out the general terms and conditions that CSP adheres to for the issuance of Time Stamp Tokens in accordance with Art. 40 of LEDES and during the operation and maintenance of this service.

The authority through which CSP issues and maintains Time Stamp Tokens strictly observes the Policy and Practice contained herein. This Policy and Practice mainly address the above-mentioned scenario of applicability of the Time Stamp Token to QES, but they are applicable to other scenarios as well.

With a view to the fact that Time Stamp Tokens provided by B-Trust TSA are applicable to different scenarios, CSP "BORICA - BANKSERVICE" AD published a general Policy and Practice, which form this document.

CSP "BORICA - BANKSERVICE" AD operates B-Trust TSA and publicly provides TSS services at the following web address „http://tss.b-trust.org".

2 Scope

This document sets out the requirements to the CSP Policy regarding the issued TST and defines the Practice for the operation and management of B-Trust TSA, in order to allow the users and trusting parties who have concluded Agreement for using certification services of B-Trust or signed Service Level Agreement to such Agreement, to obtain description and assessment of security of provided B-Trust TSS.

B-Trust TSS uses the common infrastructure of B-Trust of "BORICA - BANKSERVICE" AD as a regulated Certification Service Provider as per LEDES.

The structure and the content of the document adhere to and correspond to document ETSI TS 102 023 v.1.2.1 (2003-01) Policy Requirements for time-stamping authorities.

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

Users and trusting parties should use this document to obtain complete description and assessment of security of provided TSS services.

3 Terms and definitions

B-Trust TSA (Time Stamp Authority) – Certification Authority in the infrastructure of B-Trust, that provides TSS services.

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

TSS (Time Stamp Services) – certification services to generate secure TST, keeping records of issued and delivered TST, examination and verification of the validity of TST.

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

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 upon the provision of 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 the document follow the definitions given in B-Trust's User Manual, published in and available at the website of CSP "BORICA - BANKSERVICE" AD (http://www.b-trust.org).

4 Concept

4.1 Time Stamp Service (TSS)

The infrastructure of B-Trust, which provides, serves and maintains TSS, includes:

- B-Trust TSA - operates TSS, generates TST, maintains journal and archive of issued TST and manages the service;
- System logistics – accepting online orders and delivery of TST, examination and verification of issued TST.

System logistics includes access to an source of accurate time (UTC(k)).

This division is conditional for the purpose of the document and imposes no restrictions for the use of TSS.

4.2 B-Trust TSA

"B-Trust TSA" is the certification authority in the infrastructure of B-Trust according to item 4.1, which provides TSS in accordance with the Policy and Practice of CSP, described in this document and forms the trust of TST users.

4.3 Users

The users of TSS are subscribers or trusting parties of B-Trust certification services as per B-Trust's User Manual, as well as any other individual or legal entity, who has concluded individual contract with "BORICA – BANKSERVICE" AD for TSS and Service Level Agreement (SLA), respectively.

4.4 Policy and practice

The present document defines the general elements of the policy and practice of CSP and provides TSS in the capacity of general conditions.

The Policy sets out the conditions and rules which CSP adheres to. The Practice describes how CSP implements the described Policy and the procedures that it adheres to in the provision of TSS.

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

Any user who needs guaranteed service level for TSS, concludes an Agreement for use of B-Trust TSS and SLA.

5 Policy of B-Trust TSA

5.1 General overview

The Policy of B-Trust TSA is the set of rules, which mean the applicability of TST for particular application or application class with general requirements to the security level.

B-Trust issues TST in accordance with "ETSI TS 102 023 Policy Requirements for time-stamping authorities" and the present Policy. The content of "ETSI TS 102 023" is technically equivalent to "IETF RFC 3628: Requirements for Time-Stamping Authorities".

The presented accurate calibrated time per UTC (Coordinated Universal Time) is accurate to 0.5 seconds.

System logistics of B-Trust TSA uses GPS source of accurate time, as well as alternative time sources for the purpose of ensuring maximum accuracy.

The certificate of B-Trust TSA, certifying the belonging of the public RSA key (2048 bits), used to verify QES in the issued TST, has profile according to the document "IETF RFC 3161, Internet x.509 PKI Time Stamp Protocol (TSP)".

The profile of B-Trust TSA certificate is specified below.

Field	Attribute	Meaning/Value
Version	-	V3
Serial number	-	0b
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Root CA
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD
	L =	Sofia
	C =	BG
Validity from	-	16 April 2015 09:34:16 UTC
Validity to	-	15 April 2020 09:34:16 UTC
Subject	Phone =	+359 2 9 215 100
	E =	ca5tss@b-trust.org
	PostalCode =	1784
	STREET=	bul. Tsarigradsko shose No 117.
	CN =	B-Trust Time Stamp Authority
	OU =	B-Trust
	O =	BORICA - BANKSERVICE AD, EIK 201230426
	L =	Sofia
	C =	BG
Public key	-	RSA(2048 bits)
Subject Key Identifier	-	2d 79 0e 96 e8 dc 9d c2 40 fd 08 71 da ae 06 67 4e 49 e6 2e
Authority Key	KeyID =	9b a6 48 3a 23 1f 3a a9 a8 88 28 57 64 ed 04 96 1c 30 c8 9d

Identifier		Certificate Issuer:
		Directory Address:
		CN=B-Trust Root CA
		OU=B-Trust
		O=BORICA - BANKSERVICE AD
		L=Sofia
		C=BG
		Certificate SerialNumber=01

Issuer Alternative Name	URL =	http://www.b-trust.org
Subject Alternative Name	URL=	http://tss.b-trust.org
Basic Constraints	Subject Type = Path length Constrain =	End Entity None
CRL Distribution Points		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.b-trust.org/repository/ca5root/crl/b-trust_ca5_root.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
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)		17 8e 35 12 63 06 b2 eb 74 a9 e5 c7 72 e6 9d 7a ee a8 0a 8c
Thumbprint (Sha256)		4f a4 8f 10 1b a9 69 db 32 b3 1f d9 00 3b 74 4a fa 97 91 c2 20 5a 37 10 a4 94 5b 94 a7 7b e7 0d

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

Algorithm	Designation
Hash algorithm:	SHA1, SHA256
Asymmetric algorithms:	RSA

5.2 Identifier

B-Trust TSA issues TST for two types of content:

- Qualified TST for QES;
- Qualified TST for digital content of random electronic document/statement.

The requirements to the above-mentioned TST are identical and consistent with those with random use of TST, according to “ETSI TS 102 023“ with policy “OID = 0.4.0.2023.1.1“.

In the majority of cases, B-Trust TSA issues TST, which contains Policy identifier:

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

With negotiated SLA, B-Trust TSA issues TST, which contain identifier described in the particular agreement.

5.3 Applicability

The policy according to this document does not restrict the applicability of the provided TST of B-Trust TSA.

TST 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 TSA may use the Policy identifier specified in item 5.2.

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

The certificate of B-Trust TSA is used by user/trusting party for examination and validity of QES in the provided TST.

6 Obligations of B-Trust TSA

6.1 General obligations:

- To meet all requirements specified in item 7 of the document for implementation of the Policy;
- To ensure conformity with the requirements specified in this Policy, even when the functionality of B-Trust TSA or a part thereof is provided under an agreement;
- To ensure conformity of provided TSS with the documented procedures in Practice.

6.2 Obligations to users:

- To observe general obligations;
- To ensure constant access to TSS, 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 TST certified time with accuracy to 500 milliseconds;
- To maintain TSS in accordance with recognized international recommendations and specifications;
- To maintain simultaneously a number of sessions of orders for the issuance of TST;
- Option to scale the productivity (TST/sec.);
- To use technical equipment corresponding to the general requirements for reliability and security of technical means of CSP pursuant to the legal provisions of LEDES;
- To not violate any licenses, intellectual property or other rights in the issued TST;
- To not allow modifications of digital data after the issuance of TST, without this be proven.

6.3 Obligations of users

Users who receive TST should verify the electronic signature of B-Trust TSA and check the validity of the certificate of this authority.

B-Trust TSA does not require electronic authentication and does not impose any other restriction on TSS users.

6.4 Obligations of third trusted parties

General obligation of any third trusted party is to verify QES in TST. It should check the validity of the certificate of B-Trust TSA. In the event that the period of validity of that certificate has not expired, the third trusted party should:

- check whether this certificate is included in CRL list;
- check the extent/ level of security of used hash function for TST;
- check the extent/ level of security of used algorithms, as well as the length of the pair keys for QES in TST.

6.5 Responsibility of B-Trust TSA

B-Trust TSA operates TSS in complete accordance with the Policy and Practice of CSP according to the document "B-Trust – User Manual" and the present Policy and Practice. B-Trust TSA shall not publish/present additional information regarding the provided TSS, unless user/third trusted party has concluded Agreement for use of B-Trust TSS and SLA with CSP.

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

"BORICA – BANKSERVICE" AD, in the capacity of CSP under LEDES, is responsible under this law and its legal provisions. TSS is a type of certification service with "irrevocability" profile and requires efficient control on all elements and events in the work of B-Trust TSA – procedures, TSS transactions, key material, personnel, etc.

7 Practice and procedures of B-Trust TSA

All procedures, control mechanisms and technical characteristics of B-Trust TSA, specified herein, supplement those specified in the document "B-Trust User Manual", especially in the parts regulating the activity of "BORICA – BANKSERVICE" AD in the capacity of CSP providing certification services.

The present conditions and procedures form the basis of the operative work of B-Trust TSA.

7.1 Key management

7.1.1 Generation of a pair of keys

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 CSP that has the right to occupy that position. The generated pair of RSA keys has length of 2048 bits.

The description and the role of the CSP personnel are specified in the document "B-Trust User Manual". The generation environment for a pair of keys by a Certification authority of CSP is listed in the same document.

7.1.2 Protection of a private key

The generated private key of B-Trust TSA 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 and chips together with the private key of B-Trust TSA.

7.1.3 Distribution of the public key

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

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

7.1.4 Extension of term and/or re-issue of certificates

The period of validity of the certificate of B-Trust TSA is 5 years. After the expiry of this period, the term of validity of the certificate is extended for a period of 3 years. After this period expires a new pair of keys is generated, the private key from which is stored in the crypto module (HSM), while the public key is certified through the issue of a new certificate of B-Trust TSA. 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 Certification of time

Server software of B-Trust TSA implements the technical certification of "ETSI TS 101 861 v.1.3.1 (2006-01) Time Stamp Profile". This specification is equivalent to the international recommendation of IETF RFC 3161 (Time Stamp Protocol).

Communication software of TSA system maintains communication with customers of TSS with protocols: TCP/IP, HTTP/HTTPS.

7.2.1 TST

The profile of orders/responses of TSA system conforms with the above-mentioned technical specifications and includes the following attributes/parameters:

1. The order for the issue of TST (TSQ) includes:

Attribute name	**Value**	**Description**
Version	1	version
Message Imprint	Hash Algorithm: […]	used hash algorithm (Sha1/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 TST
Nonce	[option]	additional data to include in TST
Certificate Request	[option]	option if TST should contain certificate of B-Trust TSA
Extensions	[option]	additional extensions

2. TST response of the request (TSR) includes:

Attribute name	Value	Description
Version	1	version
Policy	[Policy OID]	identifier of policy for the issue of Time Stamp Tokens
Message Imprint	Hash Algorithm: […]	used hash algorithm (Sha1/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 code
Generated Time	[…]	time for the 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	Phone = +359 2 9 215 100
	E = ca5tss@b-trust.org
	PostalCode = 1784
	STREET = bul. Tsarigradsko shose No 117
	CN = B-Trust Time Stamp Authority
	OU = B-Trust
	O = BORICA - BANKSERVICE AD, EIK 201230426
	L = Sofia	

	C = BG	
Extensions	[option]	additional extensions
Digital Signature	[…]	identifiers of algorithms used for the creation of electronic signature (Sha1RSA/Sha256RSA)
	Signature Value: […]	electronic signature of TST
	[Certificate of B-Trust TSA]	certificate of qualified electronic signature of the Certification Service Provider

7.2.2 Time synchronization with UTC

B-Trust TSA uses hardware source of accurate calibrated time with high accuracy. 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, the source of accurate time shall be found in web-based time servers. Synchronization is the basis of at least two web-sources of time via NTP protocol.

7.3 Management and operation

7.3.1 Security management

All aspects of security management for B-Trust TSA are in accordance with the document “B-Trust - User Manual” of CSP „BORICA – BANKSERVICE” AD.

7.3.2 Risk evaluation

All aspects of risk evaluation are in accordance with the document “B-Trust - User Manual” of CSP „BORICA – BANKSERVICE” AD.

7.3.3 Personnel security

The characteristics of the CSP personnel and the appointed positions are in accordance with the document “B-Trust - User Manual” of CSP „BORICA – BANKSERVICE” AD.

7.3.4 Access control

Physical control to the environment of CSP and of B-Trust TSA is in accordance with the document “B-Trust - User Manual” “BORICA – BANKSERVICE” AD .

7.3.5 Secure environment

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

7.3.6 Termination of TSA

In the event of termination of B-Trust TSA the relevant procedures from “B-Trust - User Manual” of CSP “BORICA – BANKSERVICE” AD shall be performed.