BALTSTAMP
TIME-STAMPING PRACTICE STATEMENT

Unique object ID (OID): **1.3.6.1.4.1.38424.1.4.4**
Version: 4.0

Valid since 2020-10-30

2020

TABLE OF CONTENTS

The history of the BalTstamp time-stamping practice statement:

Version	Date	Description
Version 0.1	2011-04-11	The draft first version
Version 1.0	2011-04-20	The first version
Version 1.1	2013-02-01	The corrected first version
Version 1.2	2014-07-23	The corrected first version
Version 1.3	2016-07-01	The corrected first version
Version 2.0	2016-12-01	The second draft version
Version 2.1	2017-03-31	The corrected second version
Version 3.0	2019-08-01	The third version
Version 4.0	2020-10-30	The fourth version

Approval of the BalTstamp time-stamping practice statement:

Preparation of the document	Name	Date	Signature
The document was prepared by	Emilis Urba	2020-09-30	
The document was verified by	Rimantas Miškinis	2020-10-15	
The document was approved by	Vincentas Vitkauskas	2020-10-30	

1 INTRODUCTION

The joint stock company "BalTstamp" (further – the BalTstamp) was established on January 31, 2011, for the purpose of provision of the qualified time-stamping service to both legal and natural persons to ensure the validity of qualified electronic signatures throughout the whole life time of the electronic documents in which the qualified electronic signatures are used. Information about the BalTstamp is available on the website https://www.baltstamp.lt/

1.1 Overview

The standard ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" specifies a best practices time-stamp policy (BTSP) for time-stamping authorities (further – TSA) issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better. The requirements specified in the BTSP are related neither to concrete technological solutions nor to the organizational structure of the TSA. Technical solutions, procedures, and personnel policy for the implementation of BTSP's requirements are described in the present BalTstamp Time-stamping practice statement (further – TSPS) of the TSA.

The present TSPS is based upon the following legal acts and normative documents:

a) The Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [eIDAS].

b) The standard ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", previously published as ETSI TS 102 023 "Policy requirements for time-stamping authorities" [EN 319 421].

c) The standard ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles", previously published as ETSI TS 101 861 "Time stamping profile" [EN 319 422].

While providing the service of time-stamping, TSA carries out the functions of generation and management of the time stamps.

Note regarding the definitions. Hereafter TSA means BalTstamp TSA; TSP means BTSP; TSPS means BalTstamp TSPS, and so on, i.e. everything that is said applies solely to the BalTstamp TSA.

1.2 Identification

The unique identifier (OID) of the TSPS is **1.3.6.1.4.1.38424.1.4.3**; the values of its fields are given in the Table ***No. 1:***

Table No. 1. The values of the fields of the unique identifier of the TSPS

Name	Value
ISO	1
Organization recognized by ISO	3
U.S. Department of Defence	6
Internet	1
Private company	4
Private company registered by IANA	1
Joint stock company "BalTstamp"	38424
Subdivision BalTstamp	1
Document type (time-stamping practice statement)	4
Document version	3

The version of the TSPS in effect is available on the website https://www.baltstamp.lt/

1.3 Users and fields of application of the time stamps

A time stamp issued by the TSA can be used to time-stamp an advanced electronic signature created using a qualified electronic signature creation device and confirmed with a valid qualified certificate, together with the data signed. This allows to prove that the electronic signature has been created before the time indicated in the time stamp. However, it is possible to time-stamp unsigned data too. Such a time stamp

confirms that the data have been created before the time indicated in the time stamp. The users of the time stamps provided by the TSA can be legal or natural persons needing the services provided by the TSA.

Neither BTSP nor TSPS imposes any limitations for using the time stamps. They can be used when signing and implementing electronic transactions, submitting applications and proposals, archiving electronic documents, etc.

TSA may provide public services; however, it can also serve closed user groups.

1.4 Conformance. Its confirmation and verification

By including in a time stamp issued a unique identifier of BTSP, TSA confirms that the time stamp conforms to the BTSP and the TSPS. In this way, TSA undertakes all the obligations defined in the BTSP and fulfils all the defined requirements for its activities.

The compliance of the TSA's activities with the BTSP and TSPS is verified as defined by the TSA, at least every two years.

1.5 Contact information

The TSPS is managed by the joint stock company "BalTstamp", which contact information is given in the *Table* ***No. 2:***

Table No. 2. Contact information of the TSA

TSA:	The joint stock company "BalTstamp"
Address:	Dariaus ir Girėno st. 40, LT-02189 Vilnius
Phone:	+370-5-216 72 11
Fax:	+370-5-216 72 12
URL:	https://www.baltstamp.lt/
E-mail:	info@baltstamp.lt

2 POLICIES AND PRACTICES

2.1 Risk assessment

The TSA carries out a risk assessment to identify, analyse and evaluate threats to the business assets taking into account business and technical issues. Based on the risk assessment results, the appropriate risk treatment measures are selected, which ensure that the level of security is commensurate to the degree of risk.

The TSA determines all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the present Time-stamping practice statement (TSPS).

The risk assessment is approved and the residual risks are accepted by the director of the BalTstamp TSA.

2.2 TSA practice statement

The TSA ensures that it demonstrates the reliability necessary for providing time-stamping services. In particular:

a) The practices and procedures used to address all the requirements identified in the Time-stamp policy (TSP) are described in the present Time-stamping practice statement (TSPS).

b) The TSPS identifies the obligations of all external organizations supporting the TSA services including the applicable policies and practices.

c) The TSPS and other relevant documentation, as necessary to assess conformance to the TSP, are available to subscribers and relying parties on the website of the BalTstamp TSA, or provided upon request.

d) The director of the BalTstamp TSA has overall responsibility for the TSA with final authority for approving the TSPS.

e) The director of the BalTstamp TSA ensures the implementation of the practices by communicating them to the personnel as appropriate.

f) The review process for maintaining the TSPS is defined in the section 2.12 Procedures for changes to the TSPS.

g) The TSA gives a due notice of changes it intends to make in its TSPS and, following approval as in (d) above, makes the revised TSPS immediately available as required under (c) above.

h) The provisions made for termination of service are stated in the section 3.14 TSA termination and termination plans.

BTSP is the only time-stamp policy supported by the TSA:

a) Hashing algorithms that can be used to represent the datum being time-stamped are specified in the section 3.7.1 Time-stamp issuance.

b) The accuracy of the time in the time-stamps with respect to UTC is specified in the section 3.7.1 Time-stamp issuance.

c) The TSA does not set any limitations on the use of its time-stamps. They can be used when signing and carrying out electronic transactions, submitting applications and proposals, archiving electronic documents, etc.

d) The subscriber obligations are specified in the section 2.6 Subscriber obligations.

e) The relying party obligations are specified in the section 2.7 Relying party obligations.

f) Information on how to verify the time-stamps is provided in the section 2.7 Relying party obligations.

g) The time-stamps issued are qualified electronic time-stamps as per Regulation (EU) No 910/2014 [eIDAS].

2.3 Terms and conditions

The TSA discloses to all subscribers and potential relying parties the terms and conditions regarding the provision of its time-stamping services.

These terms and conditions specify the following:

a) The TSP being applied.
b) The expected life-time of public key certificates.
c) The subscriber's obligations, if any.
d) Information on how to verify the time-stamp, and any possible limitations on the validity period associated with it.
e) The period of time during which TSA event logs are retained.
f) Limitations of liability.
g) Limitations on the use of the services provided including the limitation for damages arising from the use of services exceeding such limitations.
h) The applicable legal system.
i) Procedures for settlement of complaints and disputes.
j) Whether the time-stamping service has been assessed to be conformant with the TSP, and if so through which conformity assessment scheme.
k) The TSA contact information.
l) Any undertaking regarding availability.

This information is available on the website https://www.baltstamp.lt/ in a readily understandable language, and may be complemented by the contracts between the TSA and the subscribers.

2.4 Information security policy

The TSA has an information security policy which is approved by the director of the BalTstamp TSA and which sets out the organization's approach to managing its information security.

The TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practice.

The TSA retains responsibility for all aspects of the provision of time-stamping services within the scope of the TSP, whether or not functions are outsourced to subcontractors. TSA uses the services provided by the Time and Frequency Standard Laboratory (LDEL) of the Metrology Department of the Center for Physical Sciences and Technology (FTMC) to generate time stamp components for the time stamps to be provided, and to ensure the metrological traceability of the time stamps to the universal coordinated time UTC according to the requirements of the present Time-stamping practice statement. The TSA retains responsibility for the disclosure of relevant practices of all the parties participating in the provision of time stamps.

The responsibility for defining the guidelines for information security, continuous maintaining of infrastructure, documentation, management, and implementation of security measures and operational procedures for the TSA equipment, premises, systems and information assets as well as protection of information and other assets is undertaken by the director of the BalTstamp TSA. The TSA ensures the communication of security guidelines and rules to all related personnel who need them in their work.

Security measures and operational procedures for the equipment, premises, systems and information assets required for provision of time stamps are documented, managed, and followed.

Information security infrastructure necessary for ensuring security is maintained permanently. Any changes affecting security are approved by the director of the BalTstamp TSA.

2.5 TSA obligations

2.5.1 General

The TSA ensures that all requirements on TSA are implemented as applicable to the TSP. TSA ensures implementation of the following:

a) Procedures defined in the present TSPS, including the service of generation of time-stamp components and metrological traceability of the time-stamps generated to the universal coordinated time UTC provided by the Time and Frequency Standard Laboratory of Metrology Department of the Center for Physical Sciences and Technology according to the requirements of the TSPS.
b) Adherence to any additional obligations either indicated in the time-stamp directly or incorporated by reference.

c) Validity of TSU certificates is ensured by CA's obligation to update their CRL at least every 7 days. This is specified in CA's Certificate Policy.

d) To ensure operability and reliability of the service vulnerability scans are performed once a year and penetration test are performed once in five years.

2.5.2 TSA obligations towards subscribers

The TSA meets its claims as given in its published terms and conditions including the availability and accuracy of its service.

2.6 Subscriber obligations

When relying upon a time-stamp token, the subscriber shall verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp token has not been compromised (for details, see the section 2.7 Relying party obligations).

2.7 Relying party obligations

The relying party, when relying upon a time-stamp token, shall verify that the time-stamp token has been correctly signed and that the private key used to sign the time stamp token has not been compromised (disclosed to third-parties or unusable for other reasons) until the time of verification.

If the time-stamp is verified during the TSU's certificate validity period, the validity of the signing key can be checked by making sure that the TSU's certificate has not been revoked. But, if the time of verification is beyond the end of the validity period of the corresponding certificate, time-stamp verification may be impossible because certification authorities are not obliged to publish revocation data of expired certificates, including the revocation due to key compromise. However, the time-stamp can be verified even when the validity period of the certificate is expired provided that at the moment of verification it can be known that:

a) The TSU private key has not been compromised at any time up to the time that a relying party verifies a time-stamp token.

b) The hash algorithms used in the time-stamp token exhibit no collisions at the time of verification.

c) The signature algorithm and signature key size under which the time-stamp token has been signed are still technologically reliable and beyond the reach of cryptographic attacks at the time of verification.

Note concerning the terms: TSA uses the private key for signing the time-stamps and for nothing else; time-stamps are signed in the time-stamping unit (further – TSU). Thus, the terms adopted from [EN 319 421] and used here and further: *private key*, *signing (signature) key*, *TSU signing key*, *TSU private signing key* are equivalent.

Besides that, the relying party shall comply with the constraints on the use of the time stamp defined in the TSP and take any other measures of precaution.

2.8 Liability

TSA liability and obligations are defined in the contracts for provision of service in effect.

2.9 Legal provisions and interpretations

2.9.1 The main legal acts

Generation of time stamps, their provision, requirements for the providers, and liability is regulated by:

a) The Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

b) The Law on electronic identification and trust services for electronic transactions of the Republic of Lithuania issued on April 26, 2018.

c) The Procedure for granting qualified status to trust services providers and trust services they provide and for provision of qualified trust service provider reports to supervisory body, established by the order No. 1V-588 of the director of Communications Regulatory Authority of the Republic of Lithuania issued on April 21, 2018.

d) The procedure for reporting security and/or integrity incidents in the trust services, established by the order No. 1V-594 of the director of Communications Regulatory Authority of the Republic of Lithuania issued on June 4, 2019.

2.9.2 Dispute settlement

Any disputes between the TSA and its end-users are resolved by positive-minded negotiations. In a case of failing to settle the dispute, it is addressed to the institutions of law enforcement.

2.10 Charges

TSA may set the prices for its time-stamping services.

2.11 Intellectual property rights

When citing any documentation of the TSA, it is required to provide a reference to its source.

2.12 Procedures for changes to the TSPS

The TSPS can be changed in the case a mistake is detected, the need in updating arises, or proposals for changes come from related parties.

Changes to the TSPS are subdivided into the two categories:

a) Essential changes about which the users shall be informed and, after the changes are implemented, the TSPS OID shall be changed.

b) Inessential changes about which the TSA is not obliged to inform other parties and, after the changes are implemented, the TSPS OID is not changed.

Inessential changes are possible when the information of explanatory, recommendation character is updated or contact data of the persons responsible for TSPS management changes.

All other changes (including all those affecting the security level of the time-stamping service) are essential.

TSPS is reviewed, changed and approved by the following procedure:

a) TSA's personnel responsible for security once a year, starting with the last edition of TSPS, review the TSPS and make sure that the TSPS is still suitable. If the changes are needed, the personnel initiate changes.

b) Changes can also be initiated by other personnel of the TSA or the users of the time-stamps. The solution on whether a change to the TSPS shall be prepared is adopted by the director of the BalTstamp TSA; preparation is assigned to the personnel whose field of activity is affected by the intended change.

c) The personnel to whom the work is assigned prepare a new edition of the TSPS.

d) The decision on the approval of the new edition of the TSPS is adopted by the director of the BalTstamp TSA; if the change is essential, the first digit in the TSPS's version and, correspondingly, an element of the OID version (the last digit) are changed. Having made an inessential change, the second and the further digits in the TSPS's version are changed.

e) The approved new edition of the TSPS is published on the website of the BalTstamp TSA.

f) The supervisory body is informed of the updated TSPS no later than 3 working days.

3 TSA MANAGEMENT AND OPERATION

3.1 Introduction

The TSA follows all the practices indicated in the following clauses.

The provision of a time-stamp in response to a request is at the discretion of the TSA depending on the agreements with the subscriber.

3.2 Internal organization

3.2.1 Organization reliability

The TSA ensures that its organization is reliable. In particular:

a) The TSA is a legal entity according to the law of the Republic of Lithuania, registered in the Register of Legal Entities as UAB BalTstamp; entity's code is 302608545.

b) The TSA has a system for quality and information security management appropriate for the time-stamping services it is providing.

c) It employs a sufficient number of personnel having the education, training, technical knowledge and experience adequate to provision of the time-stamping services.

d) Policies and practices under which the TSA operates are based on international standards and are non-discriminatory.

e) TSA's services are accessible to all applicants whose activities fall within its declared field of operation, and that agree to abide by their obligations as specified by the TSA.

f) The TSA has adequate arrangements and resources, in accordance with national law, to cover liabilities arising from its operations and activities.

g) The TSA has the financial stability and resources required to operate in conformity with the TSP, including the requirements for TSA termination.

h) The policies and procedures for the resolution of complaints and disputes about the provisioning of the time-stamping services or any other related matters are specified as defined in the section 2.3 Terms and conditions.

i) The TSA has a documented agreement and contractual relationship in place where the provisioning of services involves third parties.

3.2.2 Segregation of duties

Conflicting duties and areas of responsibility are segregated as defined in the TSA's information security policy (see the section 2.4 Information security policy) to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP assets.

3.3 Personnel security

The TSA ensures that personnel and hiring practices enhance and support the trustworthiness of the TSA's operations. In particular:

a) The TSA employs personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.

b) Appropriate disciplinary sanctions are applied to personnel violating TSA's policies or procedures.

c) Personnel's security roles and responsibilities, as specified in the TSA's information security policy, are documented in their job descriptions. Trusted roles, on which the security of the TSA's operation is dependent, are clearly identified.

d) TSA personnel (both temporary and permanent) have job descriptions defined from the point of view of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. The job descriptions include skills and experience requirements.

e) Personnel exercise administrative and management procedures and processes that are in line with the TSA's information security management procedures.

f) TSA employs managerial personnel who possess:
   - Knowledge of time-stamping technology.
   - Knowledge of digital signature technology.
   - Knowledge of mechanisms for synchronization of the TSU clocks with UTC.
   - Familiarity with security procedures for personnel with security responsibilities.
   - Experience with information security and risk assessment.

g) All TSA personnel in trusted roles are free from conflict of interest that might prejudice the impartiality of the TSA operations.

h) Trusted roles are defined in the TSA's information security policy and include roles that involve the following responsibilities:
   - Security officers: overall responsibility for administering the implementation of the security practices.
   - System administrators: authorized to install, configure and maintain the TSA trustworthy systems for time-stamping management.
   - System operators: responsible for operating the TSA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
   - System auditors: authorized to view archives and audit logs of the TSA trustworthy systems.

i) TSA personnel are formally appointed to trusted roles by the senior management responsible for security.

j) The TSA does not appoint to trusted roles or management any person who is known to have committed a serious crime or other offence that affects his/her suitability for the position. Personnel have no access to the trusted functions until any necessary checks are completed.

The director of the BalTstamp TSA is responsible for employing the personnel complying with these requirements as well as testing their skills and reliability, defining and describing the roles of personnel (including the trusted functions) in their job descriptions.

All the personnel can perform the operations defined by their roles only.

3.4 Asset management

The TSA ensures that its information and other assets receive an appropriate level of protection. In particular, the TSA maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

All media are handled securely in accordance with the requirements of the information classification scheme. Media containing sensitive data are securely disposed of when no longer required.

3.5 Access control

The TSA ensures that TSA system access is limited to properly authorized individuals. In particular:

a) A firewall is implemented to protect the TSA's internal network domains from unauthorized access, including access by subscribers and third parties. The firewall is configured to prevent all protocols and accesses not required for the operation of the TSA.

b) The TSA ensures effective administration of user access required for the work of operators, administrators and auditors. In this way, the system security, including user account management, auditing, and timely modification or removal of access, is maintained.

c) Access to information and application system functions is restricted in accordance with the access control policy, and the TSA system provides sufficient computer security controls for the separation of trusted roles identified in the TSPS, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled.

d) TSA personnel are properly identified and authenticated before using critical applications related to the time-stamping.

e) TSA personnel are accountable for their activities; to this end, event logs are retained (see the section 3.12 Collection of evidence).

The following additional controls are applied to time-stamping management:

f) The local network components (e.g. routers) are kept in a physically secure environment, and their configurations are periodically audited for compliance with the requirements specified by the TSA.

g) Continuous monitoring and alarm facilities are provided to enable the TSA to detect, register, and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

3.6 Cryptographic controls

3.6.1 General

The TSA ensures the security of cryptographic keys and cryptographic devices throughout their lifecycle as detailed in the following clauses.

3.6.2 TSU key generation

The TSA generates its cryptographic keys under controlled circumstances. In particular:

a) The generation of the TSU's signing key(s) is undertaken in a physically secured environment by personnel in trusted roles (see clause 7.3 of [EN 319 421]) under, at least, dual control. The personnel authorized to carry out this function are limited to those required to do so under the TSA's practices.

b) The generation of the TSU's signing key(s) is carried out within a cryptographic module that meets the requirements identified in the standard [FIPS 140] level 3.

c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time stamp tokens key are recognized as being fit for the purposes of time stamp tokens as issued by the TSA: the key length is 2048 bits, the signing algorithm is RSA.

d) A TSU's signing key is not imported into different active cryptographic modules.

e) A TSU has a single time-stamp signing key active at a time.

3.6.3 TSU private key protection

The TSA ensures that TSU private keys remain confidential and maintain their integrity. In particular:

a) TSU's private signing keys are held and used within a cryptographic module that meets the requirements identified in the standard [FIPS 140] level 3.

b) If TSU’s private keys are backed up, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment, in a room protected from unattended access (see clause 7.8 of [EN 319 421]). The personnel authorized to carry out this function are limited to those who are required to do so under the TSA's practices.

c) The confidentiality of any backup copies of the TSU private signing keys is protected cryptographically before being stored outside the cryptographic module.

3.6.4 TSU public key certificate

The TSA ensures that the integrity and authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties. In particular:

a) TSU signature verification (public) keys are made available to relying parties in public key certificates.

b) The signature verification (public) key certificate used by TSU is issued either by a certification authority which provides a level of security equivalent to, or higher than, the TSP which is implemented by the present TSPS, or a TSA itself.

c) The TSU cannot issue time-stamps before the corresponding signature verification (public key) certificate is loaded into it.

3.6.5 Rekeying TSU's key

The validity period of TSU's certificate is set not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose:

- for RSA 2048-bit keys – until the end of year 2029.

Renewal of the TSU's certificate while maintaining the same key pair is not done.

3.6.6 Life cycle management of signing cryptographic hardware

The TSA ensures the security of cryptographic hardware throughout its lifecycle. In particular, the TSA ensures that:

a) Time-stamp token signing cryptographic hardware is not tampered with during shipment and while stored. Prior to installation, the hardware is checked by security officers in accordance with the information security policy, and the results are documented in the journal of the hardware unit.

b) Generation and activation of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment. These events are recorded in the journal of the hardware unit. Duplication of keys is not performed.

c) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement using the secure zeroization procedure described in the documentation of the device so that it is practically impossible to recover them.

3.6.7 End of TSU key life cycle

The expiration date of a TSU key is equal to the expiration date of the associated public key certificate. The TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular:

a) TSA maintains procedures to ensure that a new key is put in place when a TSU's key expires; i.e., personnel whose duties require doing so supervise and ensure that the keys, which, according to the data of a journal, have expired, are no longer used. Before the time of expiry, the personnel irreversibly delete the key from the cryptographic module as well as all its copies from the media specified in the journal. Then, they generate and install a new key pair as described in the section 3.6.2 TSU key generation.

b) The TSU private signing keys, or any key part, including any copies is destroyed such that the private keys cannot be retrieved.

3.7 Time-stamping

3.7.1 Time-stamp issuance

The TSA ensures that time-stamps are issued securely and include the correct date and time. In particular:

a) The time values the TSU uses in the time-stamps are traceable to UTC(LT).

b) The value of time included in the time-stamp does not differ from UTC more than the accuracy defined in the TSP and in the time-stamp itself.

c) If the time-stamp provider's clock is detected (see the section 3.7.2 Clock synchronization with UTC) as being out of the stated accuracy, then time-stamps are not issued.

d) The time-stamps are signed using a key generated exclusively for this purpose.

e) The time-stamp generation system rejects any attempt to issue a time-stamp if the signing private key has expired.

The time-stamps issued conform to the time-stamp profile defined in [EN 319 422]. The structure of a time-stamp request accepted by the BalTstamp TSA is given in the *Table* ***No. 3***; the structure of a time-stamp issued by the BalTstamp TSA is given in the *Table* ***No. 4***.

Table No. 3. The structure of a time-stamp request

Field	Value
version	1
messageImprint	A hash algorithm OID and the hash value of the data to be time-stamped; the following algorithms can be used: - SHA-1 (OID: 1.3.14.3.2.26), though not recommended - SHA-256 (OID: 2.16.840.1.101.3.4.2.1) - SHA-384 (OID: 2.16.840.1.101.3.4.2.2) - SHA-512 (OID: 2.16.840.1.101.3.4.2.3)

reqPolicy	If specified, shall be 0.4.0.2023.1.1
nonce	If specified, the same value will be included in the time-stamp
certReq	If present and set to *true*, the certificate of the corresponding TSU will be included in the time-stamp
extensions	Shall not be specified

Table No. 4. The structure of a time-stamp

Field	Value
version	1
policy	0.4.0.2023.1.1
messageImprint	Equals to the value of the corresponding field of request (*TimeStampReq*)
serialNumber	An integer (up to 160 bits long), unique for every time-stamp issued by the TSU
genTime	UTC time indicating the time when the time stamp was created
accuracy	1 s or better (up to 200 ms), depending on an agreement
nonce	Equals to the value of the corresponding field of request (*TimeStampReq*), if included
tsa	Corresponds to the value of the *Subject* field of the certificate used for signing the time stamp: C = LT L = Vilnius organizationIdentifier = NTRLT-302608545 O = BalTstamp UAB CN = BalTstamp QTSA TSU1 or C = LT L = Vilnius O = BalTstamp UAB CN = BalTstamp QTSA TSU2
extensions	May contain *qcStatements* extension with the *esi4-qtstStatement-1* statement

3.7.2 Clock synchronization with UTC

The TSA ensures that its clock is synchronized with UTC within the declared accuracy. In particular:

a) The TSU clocks are continuously synchronized with the State Standard of Time and Frequency, which realizes the Lithuanian scale of the universal coordinated time UTC(LT), which traceability to UTC is ensured by means of continuous comparison; the characteristics of the traceability are published in the "Circular T" of the Bureau International des Poids et Mesures (BIPM). Therefore, the TSU clocks cannot deviate more than two tenths of a second.

b) The TSU clocks are protected against threats that could result in an undetected change to a clock that could take it outside its calibration. Threats include tampering by unauthorized personnel, radio or electrical shocks, etc.

c) The systems used by the TSA are capable to detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

d) If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the time-stamp issuance is stopped.

e) The TSU clocks maintain synchronization when a leap second occurs as notified by the appropriate body. The change to take account of the leap second occurs during the last minute of the day when the leap second is scheduled to occur. The systems record the exact time of this change. If a leap second is inserted, to prevent ambiguity and problems for the systems that cannot handle 61 seconds per minute, time stamps are not issued during the leap second and the second before it.

3.8 Physical and environmental security

The TSA ensures that physical access to critical services is controlled and physical risks to its assets minimized. In particular:

a) For both the time-stamping provision and the time-stamping management:
   - Physical access to facilities concerned with time-stamping services is limited to properly authorized individuals.
   - Controls are implemented to avoid loss, damage or compromise of assets, theft or leak of information, interruption to business activities.
   - Controls are implemented to avoid compromise or theft of information and information processing facilities.

b) TSA applies access controls to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clauses 7.6.2 and 7.6.3 of [EN 319 421].

c) The following additional controls are applied to time-stamping management:
   - The time-stamping management facilities are operated in an environment that physically protects the services from compromise through unauthorized access to systems or data.
   - Physical protection is achieved through the creation of a clearly defined security perimeter around the time-stamping management. Inside this perimeter, there are no parts of the premises shared with other organizations.
   - Physical and environmental security controls are implemented to protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.
   - Controls are implemented to protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

TSA’s time-stamping equipment operates in the Time and Frequency Standard Laboratory (LDEL), which personnel are authorized to supervise the equipment and operate it, in the premises controlled according to the requirements of the quality management system. The boundaries of the LDEL, at the same time, define the security perimeter, unauthorized access to the inside area of which is not possible. The building of the Center for Physical Sciences and Technology (FTMC) which houses the LDEL is protected by the watchers and security service. In this way, the assets (including media) are protected against being taken off-site without authorization or compromise.

LDEL operates a modern air conditioning system, which is maintaining the air temperature necessary and cleaning the air of the dust. If the power supply fails, UPS and the diesel electric power generator maintains normal operation of the system for 4 hours.

To prevent compromise and theft of information and information processing facilities, the following measures are taken: in the TSA’s equipment, internet connection is limited – only the connections necessary for the provision of time stamps are allowed. Firewalls and intrusion protection systems are implemented.

3.9 Operation security

For critical services, as identified by the risk analysis, the TSA uses trustworthy systems and products that are protected against modification. The TSA ensures that the TSA system components are secure and correctly operated, with minimal risk of failure.

In particular:

a) An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the TSA or on behalf of the TSA to ensure that security is built into IT systems.

b) Change control procedures are applied for releases, modifications, and emergency software fixes of any operational software.

c) The integrity of TSA system components and information is protected against viruses, malicious and unauthorized software.

d) Media used within the TSA trustworthy systems are securely handled to protect media from damage, theft, unauthorized access, and obsolescence.

e) Media management procedures are employed to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

f) Procedures are established and implemented for all trusted and administrative roles that have impact on the provision of time-stamping services.

g) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

3.10 Network security

The TSA maintains and protects TSU systems in a secure zone, accessible by the personnel in trusted roles only. The configuration of TSU systems is hardened so that only the necessary accounts, applications, services, protocols and ports are used. The information security policy of the TSA identifies the trusted roles and assigns the corresponding responsibilities in order to implement this practice.

3.11 Incident management

The TSA is constantly monitoring system activities concerning access to and use of the TSA's systems.

Abnormal system activities that indicate potential security violations, including possible intrusions, are detected and reported as alarms.

The TSA acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. Incidents are reported in line with the incident management procedures.

Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions be minimized.

3.12 Collection of evidence

The TSA ensures that all relevant information concerning the operation of time-stamping services is recorded and stored for an appropriate period of time, for the purpose of providing evidence for the purposes of legal proceedings. In particular:

General

a) The specific events and data to be logged are documented in the TSA's information security policy.

b) The confidentiality and integrity of current and archived records concerning operation of time-stamping services is maintained.

c) Records concerning the operation of time-stamping services are completely and confidentially archived in accordance with disclosed TSA practices.

d) Records concerning the operation of time-stamping services are made available if required for the purposes of providing evidence of the correct operation of the time-stamping services for the purpose of legal proceedings.

e) The precise time of environmental, key management, and clock synchronization events of the TSA is recorded.

f) Records concerning time-stamping services are held for a period of time after the expiration of the validity of the TSU's signing keys as appropriate for providing necessary legal evidence and as notified in the TSA disclosure statement (see clause 6.3 of [EN 319 421]).

g) The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

h) Any information recorded about subscribers are kept confidential except as where agreement is obtained from the subscriber for its wider publication.

Management of TSU keys

i) Records concerning all events relating to the lifecycle of TSU keys are logged.

j) Records concerning all events relating to the lifecycle of TSU certificates are logged.

Clock synchronization

k) Records concerning all events relating to synchronization of a TSU's clock to UTC are logged.

l) Records concerning all events relating to detection of loss of synchronization are logged.

3.13 Business continuity management

The TSA ensure that in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of traceability to UTC(LT), relevant information is made available to subscribers and relying parties. In particular:

a) The TSA's disaster recovery plan addresses the compromise or suspected compromise of TSU's private signing keys or loss of traceability of a TSU clock, which may have affected time-stamps which have been issued.

b) In the case of a compromise, or suspected compromise or loss of traceability, the TSA makes available to all subscribers and relying parties a description of compromise that occurred.

c) In the case of a compromise to a TSU's operation (e.g. TSU key compromise), suspected compromise or loss of traceability, the TSU does not issue time stamp tokens until the compromise has been recovered from.

d) In the case of a major compromise of the TSA's operation or loss of traceability, wherever possible, the TSA makes available to all subscribers and relying parties information which may be used to identify the time stamp tokens which may have been affected, unless this breaches the privacy of the TSA’s users or the security of the TSA services.

3.14 TSA termination and termination plans

The TSA ensures that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and continued maintenance of information required to verify the correctness of time-stamps is provided. In particular:

a) The TSA has an up-to-date termination plan.

b) Before the TSA terminates its time-stamping services, the following procedures are executed as a minimum:

- The TSA makes available to all subscribers, relying parties and the supervisory body information concerning its termination at least 3 months in advance, by using the available contact data.
- TSA terminates authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time-stamps.
- The TSA transfers obligations to a reliable party for maintaining event log and audit archives (see clause 7.14 of [EN 319 421]) necessary to demonstrate the correct operation of the TSA for a reasonable period.
- The TSA maintains or transfers to a reliable party its obligations to make available its public key or its certificate to relying parties for a reasonable period.
- TSU private keys, including backup copies, are destroyed in a manner such that the private keys cannot be retrieved.

c) The TSA has an arrangement to cover the costs to fulfil these minimum requirements in case the TSA becomes bankrupt or for other reasons is unable to cover the costs by itself.

d) The TSA states in its practices the provisions made for termination of service. Those include:

- Notification of all affected entities.
- Transferring the TSA obligations to other parties.

e) The TSA takes steps to have the TSU's certificates revoked.

3.15 Compliance

The TSA ensures compliance with legal requirements. In particular:

a) Compliance with the requirements of the Regulation (EU) No 910/2014 [eIDAS] is confirmed at least every 24 months by an audit performed by an accredited conformity assessment body.

b) The TSA has no specific requirements for use of the services which could prevent access for persons with disabilities.

c) The TSA ensures that the requirements of the European Data Protection Directive 95/46/EC, as it is

implemented through Lithuanian legislation, are met:

- For the purpose of provision of the time-stamping services, the TSA requires to provide a time-stamping request as defined in [EN 319 422], together with authentication data if appropriate for the authentication method chosen.
- The TSA processes the data together with the communication level attributes as necessary to issue a time-stamp and to fulfil the requirements of the applicable standards, including monitoring for security, accounting and capacity planning.
- No other data, including personal data, is collected or processed during the provision of the services.
- Appropriate technical and organizational measures are taken against unauthorized or unlawful processing, disclosure, accidental loss or destruction of, or damage to, the data received.

4 DEFINITIONS AND ABBREVIATIONS

Compromise: a loss, theft, modification, illegal use, or any other security violation of the confidential data.

Hardware security module (HSM), or cryptographic security module: hardware and software used to generate cryptographic key pairs – private and public keys, to store private keys and/or to create electronic signatures.

Repository: an internet place where information of the time-stamping authority is made available for the users.

Subscriber: an entity requiring services provided by a TSA and which has explicitly or implicitly agreed to its terms and conditions.

Time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time-stamp policy (TSP): a set of rules for generation, management, and verification of time stamps, which defines the rights and obligations of the provider and the users of the service. The service provider defines and implements the time stamp policy, while the user of the time stamps chooses the service provider with acceptable rules as well as other terms and conditions.

Time-stamp token: data object defined in IETF RFC 3161, representing a time-stamp.

Time-stamp users: recipients (including subscribers) of the time stamps who rely upon them.

Time-stamping authority (TSA): a certification service provider which provides the time-stamping service.

Time-stamping practice statement (TSPS): statement of the practices that a TSA employs in issuing time-stamp tokens, by fulfilling which the time stamp policy is implemented.

BIPM – International Bureau of Weights and Measures (fr. *Bureau International des Poids et Mesures*)
BTSP – Best practices Time-Stamp Policy
CA – Certificate authority
ETSI – European Telecommunications Standards Institute
FTMC – Center for Physical Sciences and Technology
LDEL – Time and Frequency Standard Laboratory
OID – Object identifier
RRT – Communications Regulatory Authority of the Republic of Lithuania
TSA – Time-stamping authority
TSP – Time stamp policy
TSPS – Time-stamping practice statement
TSU – Time-stamping unit
UTC – Universal coordinated time (fr. *universel temps coordonné*)

5 REFERENCES

[eIDAS] – Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[EN 319 401] – ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[EN 319 421] – ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[EN 319 422] – ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[FIPS 140] – The standard FIPS PUB 140-2 "Security Requirements for Cryptographic Modules" (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).