BALTSTAMP
TIME STAMP POLICY

Unique object ID (OID): **1.3.6.1.4.1.38424.1.3.1**
Version: 1.1

Valid since 2014-07-25

2014

TABLE OF CONTENTS

The history of the BalTstamp time stamp policy:

Version	Date	Description
Version 0.1	2011-04-11	The draft first version
Version 1.0	2011-04-15	The first version
Version 1.1	2014-07-23	The first version with editorial corrections

Approval of the BalTstamp time stamp policy:

Preparation of the document	Name	Date	Signature
The document was prepared by	Emilis Urba	2014-07-01	
The document was verified by	Rimantas Miškinis	2014-07-21	
The document was approved by	Vincentas Vitkauskas	2014-07-23	

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 http://www.baltstamp.lt/

1.1 Overview

The BalTstamp time stamp policy (further – TSP) defines the operation of the BalTstamp time-stamping authority (further – TSA) and the requirements, including the security requirements, for generation of the time stamps with a precision not worse than two tenths of a second and confirmed with public key certificates. In order to justify the confidence of the users in the time stamps provided by the TSA, TSP is declared publicly.

The requirements specified in the TSP are related neither to concrete technological solutions nor the organizational structure of the TSA. Technical solutions, procedures, and personnel policy for the implementation of TSP's requirements are described in the BalTstamp time-stamping practice statement (further – TSPS).

TSP is based upon the following legal acts and normative documents:

a) the order No. 1V-407 "The order of provision of time-stamping services" (Official Gazette, 2011, No. 48-2349) issued by the director of the Communications Regulatory Authority of the Republic of Lithuania on April 19, 2011;

b) the standard LST ETSI TS 102 023 "Policy requirements for time-stamping authorities";

c) the standard LST ETSI TS 101 861 "Time stamping profile".

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

1.2 Identification

The unique identifier (OID) of the TSP is **1.3.6.1.4.1.38424.1.3.1**; 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 TSP

Name	**Value**
ISO	1
Organization recognized by the 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 stamp policy)	3
Document version	1

The version of TSP in effect is available on the website http://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 a secure electronic signature created using a secure 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.

TSP does not impose 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 the unique identifier defined in Section 1.2 in a time stamp issued, TSA confirms that the time stamp conforms to the TSP. In this way, TSA undertakes all the obligations defined in the TSP and fulfils all the defined requirements for its activities.

The compliance of the TSA's activities with the TSP and TSPS is verified as defined by the TSA.

1.5 Contact information

The TSP 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:	http://www.baltstamp.lt/
E-mail:	info@baltstamp.lt

2 OBLIGATIONS AND LIABILITY

2.1 Obligations of the TSA

2.1.1 General

The TSA shall ensure that all requirements on TSA are implemented as applicable to the TSP (selected trusted time stamp policy). TSA shall ensure implementation of the following:

a) procedures defined in the TSP, even if the TSA's functions are outsourced to subcontractors;

b) adherence to any additional obligations indicated in the time stamp either directly or incorporated by reference.

TSA shall provide all the time-stamping services complying with its TSPS.

2.1.2 TSA obligations towards subscribers

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

2.2 Subscriber obligations

Having obtained 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 (disclosed to third-parties or unusable for other reasons).

The subscriber shall comply with the limitations on the use of the time stamp (if any) and follow measures of precaution defined in the TSP as well as in the contracts completed with the service provider. Besides that, the subscriber shall follow the obligations specified in the TSA's terms and conditions.

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 [ETSI 1] and used here and further: *private key*, *signing (signature) key*, *TSU signing key*, *TSU private signing key* are equivalent.

2.3 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.

Note: 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 part 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.

Besides that, the relying party shall comply with the limitations on the use of the time stamp and follow measures of precaution defined in the TSP as well as in the contracts completed with the service provider.

2.4 Liability

TSA is liable for its illegal operation and reimburses the harm incurred by the subscriber as compelled by the law of the Republic of Lithuania. TSA undertakes no additional obligations, except for those determined in the contracts for provision of service in effect.

2.5 Legal provisions and interpretations

2.5.1 The main legal acts

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

a) the Law on electronic signature of the Republic of Lithuania [ELP] (Official Gazette, 2000, No. 61-1827; Official Gazette, 2002, No. 64-2572);

b) the order No. 1V-407 "The order of provision of time-stamping services" (Official Gazette, 2011, No. 48-2349) issued by the director of the Communications Regulatory Authority of the Republic of Lithuania on April 19, 2011.

2.5.2 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 confided to the institutions of law enforcement.

2.6 Charges

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

2.7 Intellectual property rights

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

3 REQUIREMENTS ON TSA PRACTICES

3.1 Practice and disclosure statements

3.1.1 TSA Practice statement

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

a) the TSA shall have a risk assessment carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures;

b) the TSA shall have a statement of the practices and procedures used to address all the requirements identified in the present TSP;

c) the TSA's practice statement shall identify the obligations of all external organizations supporting the TSA services including the applicable policies and practices;

d) the TSA shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the TSP;

e) the TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services as specified in clause 7.1.2 of [ETSI 1];

f) the TSA shall have a high level management body with final authority for approving the TSA practice statement;

g) the senior management of the TSA shall ensure that the practices are properly implemented;

h) the TSA shall define a review process for the practices including responsibilities for maintaining the TSA practice statement;

i) the TSA shall give due notice of changes it intends to make in its practice statement and shall, following approval as in (f) above, make the revised TSA practice statement immediately available to subscribers and relying parties as required under (d) above.

3.1.2 TSA Disclosure statement

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services. This statement shall specify the following:

a) the TSA contact information;

b) the time stamp policy being applied;

c) at least one hashing algorithm which may be used to represent the data being time-stamped;

d) the expected life-time of the signature used to sign the time stamp token (depends on the hashing algorithm being used, the signature algorithm being used and the private key length);

e) the accuracy of the time in the time stamp tokens with respect to UTC;

f) any limitations on the use of the time-stamping service;

g) the subscriber's obligations as defined in clause 6.2 of [ETSI 1], if any;

h) the relying party's obligations as defined in clause 6.3 of [ETSI 1];

i) information on how to verify the time stamp token such that the relying party is considered to "reasonably rely" on the time stamp token (see clause 6.3 of [ETSI 1]) and any possible limitations on the validity period;

j) the period of time during which TSA event logs are retained;

k) reference to the applicable legal system, including the claim to meet the requirements on time-stamping services under the Lithuanian law;

l) limitations of liability;

m) procedures for complaints and dispute settlement;

n) whether the TSA has been assessed to be conformant with its time stamp policy, and if so, by which independent body.

This information shall be available at the website http://www.baltstamp.lt/ in a language understandable by the subscriber. In the case of any change, the content of the website shall be updated immediately.

3.2 Key management life cycle

3.2.1 TSA key generation

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

a) the generation of the TSU's signing key(s) shall be undertaken in a physically secured environment by personnel in trusted roles (see clause 7.4.3 of [ETSI 1]) under, at least, dual control. The personnel authorized to carry out this function shall be limited to those requiring to do so under the TSA's practices;

b) the generation of the TSU's signing key(s) shall be carried out within a cryptographic module(s) which either meets the requirements identified in the standard [FIPS 1] level 3 or higher or meets the requirements identified in [CWA 1], or is a trustworthy system which is assured to EAL 4 or higher in accordance to [ISO/IEC 1], or equivalent;

c) the TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time stamp tokens key shall be recognized by any national supervisory body, or in accordance with existing current state of art, as being fit for the purposes of time stamp tokens as issued by the TSA.

3.2.2 TSU private key protection

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

a) TSU's private signing key(s) shall be held and used within a cryptographic module which either meets the requirements identified in the standard [FIPS 1] level 3 or higher or meets the requirements identified in [CWA 1], or is a trustworthy system which is assured to EAL 4 or higher in accordance to [ISO/IEC 1], or equivalent;

b) if TSU’s private keys are backed up, they shall be 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 7.4.4 of [ETSI 1]). The personnel authorized to carry out this function shall be limited to those who are required to do so under the TSA's practices;

c) any backup copies of the TSU private signing keys shall be stored in the media protected cryptographically in a room other than that in which the cryptographic module is held. The level of the room protection is adequate to the terms specified in the TSPS. The term for validity of the TSU certificate and the appropriate signature creation data (private key) shall be set taking into account the algorithms used for hashing and signature creation as well as the length of the key of the signature which confirms the time stamps.

3.2.3 Distribution of the TSU public key

The TSA shall ensure 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) key shall be made available to relying parties in a public key certificate;

b) the TSU's signature verification (public) key certificate shall be issued by a certification authority which provides a level of security equivalent to, or higher than, the present TSP.

3.2.4 Rekeying TSU's key

The life-time of TSU's certificate shall be not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose. The life-time of TSU's certificate shall be not longer than that of the TSU’s key pair. Renewal of the TSU's certificate while maintaining the same key pair is not done.

3.2.5 The end of the life cycle of the TSU’s cryptographic key pair

The TSA shall ensure that TSU private signing keys are not used beyond the end of their life cycle. In particular:

a) operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires;

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

c) the time stamp generation system SHALL reject any attempt to issue a time stamp if the signing private key has expired.

3.2.6 Managing the life cycle of cryptographic module used to sign time stamps

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

a) time stamp token signing cryptographic hardware is not tampered with during shipment;

b) time stamp token signing cryptographic hardware is not tampered with while stored;

c) installation, activation and duplication of TSU's signing keys in cryptographic hardware shall be done only by personnel in trusted roles using, at least, dual control in a physically secured environment;

d) time stamp token signing cryptographic hardware is functioning correctly;

e) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement.

3.3 Time-stamping

3.3.1 Time stamp token

The TSA shall ensure that time stamp tokens are issued securely and include the correct date and time. In particular:

a) the time stamp token shall include an identifier for the time stamp policy;

b) each time stamp token shall have a unique identifier;

c) the time values the TSU uses in the time stamp token shall be traceable to UTC(LT);

d) the time included in the time stamp token shall not differ from UTC more than the accuracy defined in this policy;

e) if the time stamp provider's clock is detected (see clause 7.3.2 c) of [ETSI 1]) as being out of the stated accuracy, then time stamp tokens shall not be issued;

f) the time stamp token shall include a representation (e.g. hash value) of the data being time-stamped as provided by the requestor;

g) the time stamp token shall be signed using a key generated exclusively for this purpose;

h) the time stamp token shall include:

- an identifier for the country in which the TSA is established, i.e. Lithuania;
- an identifier for the TSA;
- an identifier for the unit which has issued the time stamp.

The structure of the time stamp token shall comply with the requirements of [ETSI 2].

3.3.2 Clock synchronization with UTC

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

- the TSU clocks shall be 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 International Bureau of Weights and Measures (fr. *Bureau International des Poids et Mesures*, BIPM). Therefore, the TSU clocks cannot deviate more than two tenths of the second;
- the TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration. Threats may include tampering by unauthorized personnel, radio or electrical shocks;
- the TSA shall ensure that clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time when this change occurred.

3.4 TSA operation and its management

3.4.1 Security management

The TSA shall ensure that administrative and management procedures are applied which are adequate

and correspond to recognized best practice. In particular:

General

a) the TSA shall retain responsibility for all aspects of the provision of time-stamping services within the scope of this TSP, whether or not functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the TSA and appropriate arrangements made to ensure that subcontractors are bound to implement any controls required by the TSA. The TSA shall retain responsibility for the disclosure of relevant practices of all parties;

b) the TSA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the TSA's information security policy. The TSA shall ensure publication and communication of this policy to all employees who are impacted by it;

c) the information security infrastructure necessary to manage the security within the TSA shall be maintained at all times. Any changes that will impact on the level of security shall be approved by the TSA management;

d) the security controls and operating procedures for TSA facilities, systems, and information assets providing the time-stamping services shall be documented, implemented and maintained;

e) TSA shall ensure that the security of information is maintained when the responsibility for TSA functions has been outsourced to another organization or entity.

3.4.2 Asset classification and management

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

3.4.3 Security of the service with respect to personnel

The TSA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the TSA's operations. In particular (general):

a) the TSA shall employ personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;

b) personnel's security roles and responsibilities, as specified in the TSA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the TSA's operation is dependent, shall be clearly identified;

c) TSA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and TSA specific functions. These should include skills and experience requirements;

d) personnel shall exercise administrative and management procedures and processes that are in line with the TSA's information security management procedures;

The following additional controls shall be applied to time-stamping management:

e) managerial personnel shall be employed 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;

f) all TSA personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA operations;

g) trusted roles 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;

h) TSA personnel shall be formally appointed to trusted roles by senior management responsible for security;

i) the TSA shall not appoint to trusted roles or management any person who is known to have committed a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

3.4.4 Physical and environmental security

The TSA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized. In particular (general):

a) For both the time-stamping provision and the time-stamping management:

- physical access to facilities concerned with time-stamping services shall be limited to properly authorized individuals;
- controls shall be implemented to avoid loss, damage or compromise of assets, leak or theft of information, and interruption to business activities;
- controls shall be implemented to avoid compromise or theft of information and information processing facilities;

b) TSA shall apply access controls to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clauses 7.2.1 and 7.2.2 of [ETSI 1];

c) the following additional controls shall be applied to time-stamping management:

- the time-stamping management facilities shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data;
- physical protection shall be achieved through the creation of a clearly defined security perimeter (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations shall be outside this perimeter;
- physical and environmental security controls shall be 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 shall be implemented to protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

3.4.5 Operations management

The TSA shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure. In particular (general):

a) the integrity of TSA system components and information shall be protected against viruses, malicious and unauthorized software;

b) incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions shall be minimized;

c) media used within the TSA trustworthy systems shall be securely handled to protect media from damage, theft, unauthorized access, and obsolescence;

d) procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of time-stamping services;

Media handling and security

e) all media shall be handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2 of [ETSI 1]). Media containing sensitive data shall be securely disposed of when no longer required;

System planning

f) capacity demands shall be monitored and projections of future capacity requirements made to ensure

that adequate processing power and storage are available;

Incident reporting and response

g) the TSA shall act in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

The following additional controls shall be applied to time-stamping management:

Operating procedures and responsibilities

h) TSA security operations shall be separated from other operations. TSA security operations' responsibilities include:

- operational procedures and responsibilities;
- secure systems planning and acceptance;
- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange.

These operations shall be managed by TSA trusted personnel, but, may actually be performed by, non-specialist, operational personnel, as defined within the appropriate security policy, and, roles and responsibility documents.

3.4.6 System access management

The TSA shall ensure that TSA system access is limited to properly authorized individuals. In particular (general):

a) controls (e.g. firewalls) shall be implemented to protect the TSA's internal network domains from unauthorized access, including access by subscribers and third parties. Firewalls shall be configured to prevent all protocols and accesses not required for the operation of the TSA;

b) the TSA shall ensure effective administration of user (this includes operators, administrators, and auditors) access to maintain system security, including user account management, auditing, and timely modification or removal of access;

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

d) TSA personnel shall be properly identified and authenticated before using critical applications related to time-stamping;

e) TSA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.10 of [ETSI 1]);

The following additional controls shall be applied to time-stamping management:

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

g) continuous monitoring and alarm facilities shall be 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.

3.4.7 Deployment and maintenance of the trustworthy systems

The TSA shall use trustworthy systems and products that are protected against modification.

Note: The risk analysis carried out on the TSA's services (see clause 7.1.1 of [ETSI 1]) identifies its critical services requiring trustworthy systems and the levels of assurance required.

In particular:

a) an analysis of security requirements shall be 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 shall be applied for releases, modifications and emergency software fixes of any operational software.

3.4.8 Compromise of the TSA services

The TSA shall ensure 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), that relevant information is made available to subscribers and relying parties. In particular:

a) the TSA's disaster recovery plan shall address the compromise or suspected compromise of TSU's private signing keys or loss of traceability of a TSU clock, which may have affected time stamp tokens which have been issued;

b) in the case of a compromise, or suspected compromise or loss of calibration, the TSA shall make 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 shall 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 calibration, wherever possible, the TSA shall make 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.

3.4.9 TSA termination

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time stamp tokens. In particular:

a) before the TSA terminates its time-stamping services the following procedures shall be executed as a minimum:

- the TSA shall make available to all subscribers and relying parties information concerning its termination;
- TSA shall terminate authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time stamp tokens;
- the TSA shall transfer obligations to a reliable party for maintaining event log and audit archives (see clause 7.4.10 of [ETSI 1]) necessary to demonstrate the correct operation of the TSA for a reasonable period;
- the TSA shall maintain or transfer to a reliable party its obligations to make available its public key or its certificates to relying parties for a reasonable period;
- TSU private keys, including backup copies, shall be destroyed in a manner such that the private keys cannot be retrieved;

b) the TSA shall have 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;

c) the TSA shall state in its practices the provisions made for termination of service. This shall include:

- notification of affected entities;
- transferring the TSA obligations to other parties;

d) the TSA shall take steps to have the TSU's certificates revoked.

3.4.10 Compliance with legal requirements

The TSA shall ensure compliance with legal requirements. In particular:

a) the TSA shall ensure that the requirements of the European Data Protection Directive, as it is implemented through Lithuanian legislation, and the requirements of [ADA] are met;

b) appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

c) the information contributed by users to the TSA shall be completely protected from disclosure unless with their agreement or by court order or other legal requirement.

3.4.11 Recording of information concerning operation of the TSA

The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings. In particular:

General

a) the specific events and data to be logged shall be documented by the TSA;

b) the confidentiality and integrity of current and archived records concerning operation of time-stamping services shall be maintained;

c) records concerning the operation of time-stamping services shall be completely and confidentially archived in accordance with disclosed business practices;

d) records concerning the operation of time-stamping services shall be 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 significant TSA environmental, key management and clock synchronization events shall be recorded;

f) records concerning time-stamping services shall be 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 7.1.2 of [ETSI 1]);

g) the events shall be 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 shall be 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 life-cycle of TSU keys shall be logged;

j) records concerning all events relating to the life-cycle of TSU certificates shall be logged;

Clock Synchronization

k) records concerning all events relating to synchronization of a TSU's clock to UTC shall be logged;

l) records concerning all events relating to detection of loss of synchronization shall be logged.

3.5 Organizational issues

The TSA shall ensure that its organization is reliable. In particular that:

a) policies and procedures under which the TSA operates shall be non-discriminatory;

b) the TSA shall make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSA disclosure statement;

c) the TSA is a legal entity according to national law;

d) the TSA has a system or systems for quality and information security management appropriate for the time-stamping services it is providing;

e) the TSA has adequate arrangements and possibilities to cover liabilities arising from its operations and/or activities;

f) it has the financial stability and resources required to operate in conformity with this policy. This includes requirements for TSA termination identified in the present TSP;

g) it employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services;

h) it has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of the time-stamping services or any other related matters;

i) it has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

3.6 Procedures for changes to the TSP

TSP 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 TSP are subdivided into the two categories:

a) essential changes about which the users shall be informed and, after the changes are implemented, the TSP 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 TSP 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 TSP management changes.

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

TSP 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 TSP, review the TSP and make sure that the TSP is still suitable. If the changes are needed, the personnel initiate changes;

b) changes can be initiated also by other personnel of the TSA or the users of the time stamps. The solution on whether a change to the TSP shall be prepared is adopted by the TSA's management; 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 TSP;

d) if the change is essential, the draft new edition of the TSP is published in the TSA's repository for 30 days. Having taken into account the remarks received (if any), the new edition of the TSP is submitted for approval. In a case of inessential changes, the new edition of the TSP is submitted for approval immediately after its preparation;

e) the decision on the approval of the new edition of the TSP is adopted by the TSA's management; if the change is essential, the first digit in the TSP'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 TSP's version are changed;

f) the new edition of the TSP is approved by the director of the BalTstamp;

g) the approved new edition of the TSP is published in the TSA's repository.

4 DEFINITIONS AND ABBREVIATIONS

Certificate: electronic certificate which relates the public key (the data for verifying a signature) to the signatory and confirms its identity or enables its determining.

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

Cryptographic module: see hardware security module (HSM).

Electronic signature (signature): the data which are embedded, attached, or associated logically with other data to prove their authenticity ant to identify the signatory.

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.

Key pair: a pair of two mathematically-related cryptographic keys – private and public.

Private key: a unique set of data which is used by a signatory for electronic signature creation (signature creation data).

Public key: a unique set of data used for electronic signature verification (signature verification data).

Qualified certificate: a certificate created by the certification service provider, meeting the requirements set by the Government of the Republic of Lithuania or its authorized institution.

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

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-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.

Time stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time. An electronic signature time stamp is the evidence that the signature has been created before the time specified in the time stamp token.

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

BIPM – International Bureau of Weights and Measures (fr. *Bureau International des Poids et Mesures*)
CA – Certificate authority
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

[ADA] – The Law on legal protection of personal data of the Republic of Lithuania;

[ELP] – The Law on electronic signature of the Republic of Lithuania and the Law on amendment of the clauses 4, 8, 14, 16 of the Law on electronic signature;

[ETSI 1] – The standard LST ETSI TS 102 023 "Policy requirements for time-stamping authorities";

[ETSI 2] – The standard LST ETSI TS 101 861 "Time stamping profile";

[FIPS 1] – The standard FIPS PUB 140-2 "Security Requirements for Cryptographic Modules";

[CWA 1] – Common Workshop Agreement 14167-2;

[ISO/IEC 1] – The standard ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security". Part 1 – Introduction and general model; Part 2 – Security functional components; Part 3 – Security assurance components.