BALTSTAMP
TIME-STAMPING PRACTICE STATEMENT

Unique object ID (OID): **1.3.6.1.4.1.38424.1.4.1**
Version: 1.2

Valid since 2014-07-25

2014

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

Approval of the BalTstamp time-stamping practice statement:

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.

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 present BalTstamp Time-stamping practice statement (further – TSPS) of the TSA.

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.

Note regarding the definitions. Hereafter TSA means BalTstamp TSA; TSP means BalTstamp TSP; 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 TSP is **1.3.6.1.4.1.38424.1.4.1**; 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 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	1

The version of the TSPS 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.

Neither TSP 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, TSA confirms that the time stamp conforms to the TSP and the TSPS. 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 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:	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 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 indicated in the time stamp either directly or incorporated by reference.

2.1.2 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.

2.2 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.

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.

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.

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.

2.4 Liability

TSA liability and obligations are defined 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 addressed 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 TSA PRACTICES

3.1 Practice and disclosure statements

3.1.1 TSA Practice statement

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

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

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

c) the TSPS identifies the obligations of all external organizations supporting the TSA services including the applicable policies and practices;

d) the TSPS and other relevant documentation are available to subscribers and relying parties, as necessary to assess conformance to the TSP;

e) the TSA discloses 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 has a high level management body with final authority for approving TSPS;

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

h) the TSA has defined a review process for the practices including responsibilities for maintaining TSPS;

i) the TSA gives a due notice of changes it intends to make in its TSPS and makes the revised TSPS immediately available to subscribers and relying parties.

3.1.2 TSA Disclosure statement

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

This statement specifies the following:

a) the TSA contact information;

b) the TSP 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 settlement of complaints and disputes;

n) assessment of whether the activities by the TSA comply with the TSP.

This information is 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 is updated immediately.

3.2 Key management life cycle

3.2.1 TSA 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 7.4.3 of [ETSI 1]) under, at least, dual control. The personnel authorized to carry out this function are limited to those requiring 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(s) which meets the requirements identified in the standard [FIPS 1] 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.

3.2.2 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 which meets the requirements identified in the standard [FIPS 1] 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 7.4.4 of [ETSI 1]). 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.

3.2.3 Distribution of the TSU public key

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) key is made available to relying parties in a public key certificate;

b) the TSU uses the signature verification (public) key certificate issued by a certification authority which provides a level of security equivalent to, or higher than, the TSP which is implemented following the present Time-stamping practice statement (TSPS).

3.2.4 Rekeying TSU's key

The life-time 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 2025.

The life-time of TSU's key pair is set equal to that of the TSU's certificate. 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 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 duty descriptions require to do so supervise and ensure that the keys which, according to the data of a journal, a certificate, or its revocation data, have become invalid, cannot be used. When the time of expiry comes, the personnel delete irreversibly the key from the cryptographic module as well as all its copies from the media specified in the journal. Having done this, they make sure once again that it is impossible to recover the deleted private key even using special software for recovery of deleted files. The personnel then destroy the media from which the data cannot be safely deleted. Then, they generate and install a new key pair as described in the section 3.2.1 TSA key generation;

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

c) the time stamp generation system rejects 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 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;

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 is 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;

f) the following events in the life cycle of the cryptographic module are registered and reviewed regularly:

- activation of the cryptographic module;
- any change in configuration;
- starting and shutting down;
- generation of the keys;
- deletion of the keys.

3.3 Time-stamping

3.3.1 Time stamp token

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

a) the time stamp token includes an identifier for the TSP;

b) each time stamp token has a unique identifier;

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

d) the value of time included in the time stamp token does not differ from UTC more than the accuracy defined in the TSP;

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 are not issued;

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

g) the time stamp token is signed using a key generated exclusively for this purpose and not used for anything else;

h) the time stamp token includes:

- 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 complies with the requirements of [ETSI 2].

The structure of a time stamp issued by the BalTstamp TSA, the names of the fields and their values are given in the *Table No. 3*:

Table No. 3. The structure of a TSA time stamp

Name	Value
version	1
policy	1.3.6.1.4.1.38424.1.3.1
messageImprint	Equals to the value of the corresponding field of request (*TimeStampReq*)
serialNumber	An integer (up to 160 bits long), unique for every TSA's time stamp
genTime	UTC time indicating the time when the time stamp was created
accuracy	200 ms

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: CN = BalTstamp QTSA TSU1 O = BalTstamp UAB C = LT SERIALNUMBER = 210 or C = LT L = Vilnius O = BalTstamp UAB CN = BalTstamp QTSA TSU2

3.3.2 Clock synchronization with UTC

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

- 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 the second;
- the TSU clocks are protected against threats which 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.;
- the TSA ensures 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 occurs during the last minute of the day when the leap second is scheduled to occur. A record is maintained of the exact time when this change occurred.

3.4 TSA operation and its management

3.4.1 Security management

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 Supervisory committee made up of the management of BalTstamp and FTMC. 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 TSA's management.

3.4.2 Asset classification and 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.

3.4.3 Security of the service with respect to personnel

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

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

c) 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;

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

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

e) 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;

f) all TSA personnel in trusted roles are 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 are formally appointed to trusted roles by the senior management responsible for security;

i) the TSA does 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 have no access to the trusted functions until any necessary checks are completed.

TSA management is responsible for employing the personnel complying with the requirements of the clause 3.4.3 of the TSP 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.

3.4.4 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 7.2.1 and 7.2.2 of [ETSI 1];

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

- the time-stamping management facilities are operated in an environment which 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.

3.4.5 Operations management

The TSA ensures 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 is protected against viruses, malicious and unauthorized software;

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

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

d) procedures are 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 are handled securely in accordance with the requirements of the information classification scheme (see clause 7.4.2 of [ETSI 1]). Media containing sensitive data are securely disposed of when no longer required;

System planning

f) capacity demands are 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 acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents are reported as soon as possible after the incident.

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

Operating procedures and responsibilities

h) TSA security operations are 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 are managed by TSA's trusted personnel, but, may actually be performed by, non-specialist, operational personnel, as defined within the appropriate security policy and job descriptions.

3.4.6 System access management

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

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 clause 7.4.10 of [ETSI 1]);

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 is 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 uses 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 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.

3.4.8 Compromise of the TSA services

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 stamp tokens 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.

3.4.9 TSA termination

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 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 are executed as a minimum:

- the TSA makes available to all subscribers and relying parties information concerning its termination at least 30 days in advance;
- 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 stamp tokens;
- the TSA transfers 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 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;

b) 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;

c) 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;

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

3.4.10 Compliance with legal requirements

The TSA ensures compliance with legal requirements. In particular:

a) the TSA ensures that the requirements of the European Data Protection Directive, as it is implemented through Lithuanian legislation, are met;

b) appropriate technical and organizational measures are 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 the users to the TSA is 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 ensures that all relevant information concerning the operation of time-stamping services is recorded at least for 10 years, 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 by the TSA;

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 7.1.2 of [ETSI 1]);

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 life-cycle of TSU keys are logged;

j) records concerning all events relating to the life-cycle 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.

3.5 Organizational issues

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

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

b) 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;

c) the TSA is a legal entity according to the law of the Republic of Lithuania;

d) the TSA has a system 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 activities;

f) it has the financial stability and resources required to operate in conformity with the TSP, including the requirements for TSA termination;

g) it employs a sufficient number of personnel having the education, training, technical knowledge and experience adequate to provision of the time-stamping services;

h) it has policies and procedures for the resolution of complaints and disputes 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 third parties.

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-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
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

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

[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".