APPROVED BY
Order No VE-282 (1.3 E) as of 23 April 2020 of
the Director General of
the State Enterprise Centre of Registers
(Recast by Order No VE-206 (1.3 E) as of 13
April 2021 of
the Director General of
the State Enterprise Centre of Registers)

TIME-STAMPING POLICY OF THE STATE ENTERPRISE CENTRE OF REGISTERS

Unique object ID (OID): **1.3.6.1.4.1.30903.1.3.2**
Version: 2.6
Valid from: **2021-04-13**

STATE ENTERPRISE CENTRE OF REGISTERS
Lvovo str. 25-101, LT-09320 Vilnius. Reg. No 124110246. VAT payer's code LT241102419
Tel.: +370 5 268 8202. E-mail: info@registrucentras.lt

TABLE OF CONTENTS

STATE ENTERPRISE CENTRE OF REGISTERS
Lvovo str. 25-101, LT-09320 Vilnius. Reg. No 124110246. VAT payer's code LT241102419
Tel.: +370 5 268 8202. E-mail: info@registrucentras.lt

History of amendments to the Time-Stamping Policy of the State Enterprise Centre of Registers:

Version	Date	Status
0.1	7 June 2008	Draft
1.0	28 October 2008	First version
2.0	28 April 2017	Second version
2.1	16 May 2017	Insignificant changes
2.2	8 November 2017	Changes
2.3	24 November 2017	Corrective changes
2.4	16 December 2019	Changes after comments from the Communications Regulatory Authority of the Republic of Lithuania
2.5	23 April 2020	Changes
2.6	23 March 2021	Functions of the TSA revised. List of legal acts updated.

Document approval:

Document preparation	Name, surname	Date	Signature
Document approved by	Saulius Urbanavičius, Director General	2021-04-13	

1. INTRODUCTION

The State Enterprise Centre of Registers (hereinafter referred to as the Centre of Registers, the Enterprise) was established in 1997. The founder of the Enterprise is the Government of the Republic of Lithuania. The institution exercising the rights and obligations of the Enterprise owner is the Ministry of Economy and Innovation of the Republic of Lithuania. The Enterprise processes data of the Real Property Cadastre and Register, Address Register, Register of Legal Entities, Population Register, Mortgage Register, Register of Property Seizure Acts, Register of Wills, Register of Marriage Contracts, Register of Powers of Attorney, Register of Legally Incapable Persons and Persons with Limited Legal Capacity, Register of Contracts; creates, implements, develops and manages information systems of the mentioned and other registers, keeps register archives. Information about the enterprise is available at http://www.registrucentras.lt.

In pursuance of efficient execution of the assigned functions, the Centre of Registers uses modern information technologies and provides qualified time-stamping service (hereinafter referred to as the qualified time-stamp token) in accordance with the legal acts of the Republic of Lithuania regulating provision of trust services.

1.1. Overview

The Time-Stamping Policy (hereinafter referred to as the TSP) shall mean a set of rules that indicates the applicability of time-stamp tokens created by the Time-Stamping Authority of the State Enterprise Centre of Registers (hereinafter referred to as the TSA) to a particular user groups and application areas with common security requirements. The present document shall be aimed at enhancing confidence in the TSA-created time-stamps meeting the requirements of this Policy.

The requirements identified in the TSP shall not be tailored to any particular technological solutions or the TSA organisational structure. Technical solutions, procedures and staff policy implementing the TSP requirements shall be specified in the Time-Stamping Practice Statement (hereinafter referred to as the TSPS) of the State Enterprise Centre of Registers.

This TSP shall define the requirements for the creation of time-stamp tokens with the accuracy of 1 (one) second, verified by the public key certificates.

The TSP is drawn up pursuant to the following legal acts:

a) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as the eIDAS);

b) The Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions;

c) Order No. 1V-594 of the Director of Communications Regulatory Authority of the Republic of Lithuania of 4 June 2019 "On the Approval of the Description of the Procedure for Reporting Security and/or Integrity Incidents in Trust Services";

d) ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;

e) ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and electronic time-stamp token profiles;

f) RFC 3628;

g) RFC 3161.

In provision of time-stamping services, the TSA fulfils the following functions:

- time-stamp creation
- time-stamp management

1.2. Identification

The object identifier (OID) of the TSP is as follows: **1.3.6.1.4.1.30903.1.3.2**

Digits separated by dots in this identifier shall have the following values as indicated below (see *Table 1*).

Table 1. Field values of the TSP unique identifier (OID)

Title	Value
ISO	1
ISO recognised organisation	3
US Defence Department	6
Internet	1
Private company	4
Private company registered with IANA	1
State Enterprise Centre of Registers	30903
Unit (RCSC)	1
Document type (Time-Stamping Policy)	3
Document version	2

The TSP shall be published in the repository on the Internet[1].

1.3. Users and Application Areas

The TSP shall be aimed at meeting the requirements of the time-stamp tokens, which are used to ensure validity of qualified electronic signatures (according to the European Union and national legal acts). Time-stamp tokens shall be created for the electronic data users seeking to prove that the

[1] https://www.elektroninis.lt/lt/n/teisininformacija-504

electronic data has been created prior to the time indicated in the time-stamp token. A time-stamping service provider may provide public services and it may also service the restricted user groups.

The Centre of Registers shall not set any limitations on the usage of time-stamp tokens. Time-stamp tokens meeting the TSP may be used in the process of electronic transactions, archiving of electronic documents, electronic signatures, etc.

1.4. Conformity

When recording the object identifier defined in Chapter 1.2 in the created time-stamp tokens, the TSA shall confirm that time-stamp tokens conform to the current TSP. Thus, the TSA must assume all obligations defined in Chapter 2.1 and meet the operational requirements laid down in Chapter 3.

1.5. Contact Details

The State Enterprise Centre of Registers shall be the organisation that approved this TSP and manages it (*Table 2*).

Table 2. Contact Details of the Centre of Registers

Person:	Head of e-Signature Certificates Division of the State Enterprise Centre of Registers
Address:	Vinco Kudirkos str. 18-3, 03105 Vilnius, Lithuania
Tel.:	+370 5 268 8262
URL:	http://www.registrucentras.lt
E-mail:	*info@elektroninis.lt*

2. GENERAL PROVISIONS

This Chapter shall specify the obligations of the TSA and the related parties and contain the statements on legal and general operational issues.

2.1. Obligations

2.1.1 General Obligations of the TSA

The TSA must ensure that all the requirements, to which it is subject as specified in Chapter 3, were met.

The TSA shall ensure conformity of the performed procedures and services with the requirements of the TSPS even if the procedures or services are undertaken by the TSA sub-contractors. Detailed distribution of the functions and responsibilities when a part of the services or procedures provided by the TSA are transferred to the sub-contractors shall be described in the concluded contracts.

The TSA must ensure implementation of all the supplementary obligations indicated in the time-stamp token either directly or incorporated by reference.

The TSA shall provide the time-stamping services in accordance with the TSPS and ensure the conformity of the TSPS with the TSP.

The TSA shall undertake to publish the latest TSPS and TSP versions (recasts) in the repository on the Internet.

2.1.2 Obligations of the TSA to the Subscribers

The TSA must follow the obligations pertaining to the provision of time-stamping services, including availability, appropriateness and accuracy of the provided services assumed according to the terms and conditions on the provision of time-stamp tokens and agreements with its subscribers.

2.1.3 Obligations of the Subscribers to the Time-Stamp Tokens

After obtaining a time-stamp token, the subscribers must verify if the service provider has correctly signed the time-stamp token, and if the certificate corresponding to the signature has been valid during signing process.

The subscribers must take into account any limitations on the usage of the time-stamp token and precautions specified in the Time-Stamping Policy or agreements with the service provider.

The obligations and liability of the subscriber shall be established in the agreement concluded between the subscriber and the service provider.

2.1.4 Obligations of the Relying Parties

The TSA terms and conditions on the provision of a time-stamp token, which must be made freely available to all related parties, must include the obligations for the relying parties that, when relying on a time-stamp token, shall:

a) make sure that the certificate verifying the time-stamp token signature has been valid during the signing process, and that the private cryptographic key (hereinafter referred to as the key) used to sign the time-stamp token has not been compromised until the time of the verification of correctness of the time-stamp token;

b) take into account any limitations on the applicability of the time-stamp token specified in the TSP, the TSPS, terms and conditions for the provision of time-stamp token or agreements with the service provider;

c) take into account any other precautions prescribed in the agreements or elsewhere.

If, during verification of a time-stamp token, validity of the TSA certificate has expired, a person must make sure whether:

a) the TSA private key has not been compromised prior to the issuance of a time-stamp token;

b) during verification period, hash algorithms used by the TSA to create a time-stamp token do not contain any collisions;

c) during verification period, the TSA signature algorithm and length of the signature key used to sign the time-stamp data are still technologically reliable and may not be subverted by cryptographic attacks.

2.2. Liability

General provisions concerning liability of the TSA shall be established by the eIDAS Regulation and legal acts of the Republic of Lithuania governing trust services as far as they do not contradict eIDAS and the agreements concluded.

2.3. Fees

The TSA shall not be entitled to request for compensation for publication of the TSP and the TSPS.

Fees for the time-stamping services are published in the repository.

2.4. Provision of Information and Repositories

The TSA must maintain a repository that is freely accessible through public telecommunications networks all the time without restrictions. The following information shall be published in the repository:

a) the latest versions of the TSP and the TSPS;

b) the certificate revocation lists (hereinafter referred to as the CRL) of the TSA;

c) other up-to-date information relevant to the provision of time-stamping services.

The TSA shall undertake to provide information on the TSA certificate status also in the OCSP protocol.

2.5. Intellectual Property Rights

Whenever the TSP and the TSPS are used, a reference to their source must be given.

3. OPERATIONAL REQUIREMENTS OF THE TSA

3.1. Practice Statement

The TSA operational procedures, control mechanism and technical requirements for infrastructure shall be detailed in the TSPS.

The TSA must ensure reliable provision of the time-stamping services:

a) the TSA shall carry out a risk analysis taking into account the managed property and threats to the property with a view to determining necessary security measures and operational procedures;

b) the TSA shall have detailed practice statements and procedures for implementation of the requirements indicated in this TSP;

c) the TSPS shall identify all external organisations contributing to the organisation of the TSA practice;

d) the TSA must furnish the subscribers and the relying parties with the TSPS and other related information with a view to assessing if the certification practices correspond to this Policy;

e) the TSA shall be obliged to communicate the terms and conditions of provision of time-stamping service to the subscribers and the relying parties;

f) the TSA must have a high level management body with the respective powers, which approves the TSPS;

g) the top management of the TSA must ensure that the TSPS was properly implemented;

3.2. Publication of Terms and Conditions on the Provision of Time-stamp Tokens

The TSA must publicly inform all its subscribers of the terms and conditions on the provision of time-stamping services, including the following:

a) the TSA contact details;

b) the object identifier (OID) of the TSP;

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

d) the expected life-time of the signature used to sign the time-stamp token;

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

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

g) obligations of the subscribers;

h) obligations of the parties relying on time-stamp tokens;

i) information on how to verify the time-stamp token in the manner that constitutes grounds for replying upon it;

j) the period of time, during which the TSA compiles and retains the event logs;

k) the applicable national law;

l) limitations on liability;

m) procedures for the settlement of complaints and disputes;

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

The above information must be available through the ordinary means of communications in such a form that remains stable over time, in a readily understandable language, and may be transmitted electronically.

3.3. Cryptographic Key Management Life Cycles

3.3.1 Generation of the TSA Cryptographic Keys

The TSA must ensure that any cryptographic keys were generated under controlled and secure environment:

a) the TSA private key must be generated under physically secured environment, under, at least, dual control of persons in trusted roles. The specific staff members holding exclusive trust roles that may fulfil the aforementioned function shall be indicated in the TSPS;

b) the cryptographic module whereby the private key is generated must meet the requirements of at least EAL 4 or higher standard in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security; or the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3;

c) the private key generation algorithm, the length of the key, signature algorithm must be generally or by the competent national authority recognised as fit for approval of time-stamp tokens.

3.3.2 TSA Private Cryptographic Key Protection

The TSA shall ensure the confidentiality and integrity (inviolability) of the TSA signature creation data (private key):

a) the TSA private key must be stored and used only in a cryptographic module meeting the requirements of the FIPS PUB 140-2 standard of level 3 or higher; or the requirements of EAL 4 or higher standard in accordance with ISO/IEC 15408, or equivalent national or internationally

recognized evaluation criteria for IT security; or the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3;

b) the TSA private keys may be recovered, and backup copies thereof may be stored by only using the system cards associated with the cryptographic technical device, each of such cards containing data fragment of the encryption key used for encrypting a copy of the STA private key. At least 2 out of minimum 4 of such cards are required to restore the private key. At least 2 (two) staff members holding exclusive trust role must be involved in the process of backing up, storing or recovering of the TSA private key, and this must be done in a physically secured environment;

c) the duration of the TSA certificate life cycle and use of the respective signature creation data (private key) shall be limited, taking into account the used data hash calculation and signature creation algorithms and the length of the electronic signature key used for approval of the time-stamp tokens.

3.3.3 TSA Public Cryptographic Key Distribution

When distributing its public key to the relying parties, the TSA shall ensure the authenticity and integrity (inviolability) of the TSA signature verification data (public key) and related parameters. The TSA public key shall be made available in the public key certificate. The certificate shall be issued by the certification service provider operating at similar or higher security level as established herein.

3.3.4 Rekeying of the TSA Cryptographic Keys

The TSA certificate validity period may not be longer than the validity period of the TSA key pair. Rekeying of the TSA private keys shall not be applicable while the same certificate is being kept.

3.3.5 End of Life Cycle of the TSA Cryptographic Key Pair

The TSA must ensure that the TSA signature creation data (private key) was not used beyond the end of its life cycle.

The established technical and management procedures must ensure that, upon expiry of the validity period of the TSA keys, a new pair of keys was created and used and the previously used private keys (or any part thereof) were destroyed. Time-stamp token creation system must prohibit issue of time-stamp tokens if the validity period of the TSA private key has expired.

3.3.6 Life Cycle of the Cryptographic Module Used for Signing Time-Stamp Tokens

The TSA must ensure security of the cryptographic technical equipment (cryptographic module) throughout its life cycle. The TSA must ensure that:

a) the cryptographic module used for signing time-stamp tokens has not been tampered with during delivery (shipment);

b) the cryptographic module used for signing time-stamp tokens has not been tampered with while stored;

c) that the TSA signature creation data (key pair) in the cryptographic module were installed and activated under physically secured circumstances, under the control of at least 2 (two) persons in trusted roles;

d) the cryptographic module used for signing time-stamp tokens was functioning properly;

e) the private keys stored in the cryptographic module used for signing time-stamp tokens were erased upon expiration of life cycle of the cryptographic module.

3.4. Creation of the Time-Stamp Token

3.4.1 Time-Stamp Tokens

The TSA must ensure that time-stamp tokens were safely issued and the correct time was included in them. The TSA must ensure that:

a) the time-stamping policy identifier was indicated in the time-stamp token;

b) each time-stamp token had a unique identifier;

c) the date and time values were indicated in the time-stamp token;

d) the time values in the time-stamp token were linked with at least one real time value provided by the UTC time laboratory;

e) the value of the time indicated in the time-stamp token was synchronised with the UTC time within the accuracy of no more than 1 (one) second;

f) if the TSA clock is detected as being out of the declared accuracy, the TSA ceased issuing time-stamp tokens;

g) the hash of the data being time-stamped provided by the subscriber of the time-stamp token was indicated in the time-stamp token;

h) the time-stamp token was signed using a key pair, which is created only for this purpose and shall not be used for any other purposes;

i) the time-stamp token indicated the identifiers of the TSA, the country of residence of the TSA and the TSA unit issuing time-stamp tokens.

3.4.2 Synchronisation with the UTC

The TSA shall ensure that the clock used by it was synchronised with the UTC (Coordinated Universal Time) with the declared accuracy. For this purpose, the TSA shall ensure that:

a) the TSA clocks are calibrated in such a manner as not to drift outside the stated accuracy;

b) the clocks are protected against threats, which could result in an undetected change to the clock that takes it outside its calibration;

c) if the time that would be indicated in a time-stamp token drifts or jumps out of synchronization with UTC, this will be detected;

d) the TSA shall ensure that the clock synchronization is maintained when a leap second occurs (a leap second is an adjustment to UTC by skipping or adding an extra 1 (one) second on the last second of a UTC month) 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 (within the declared accuracy) when this change occurred.

3.5.TSA Management and Operation

3.5.1 Security Management

The TSA shall ensure that administrative and management procedures are applied, which are adequate and correspond to recognised best practice.

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 third parties; nevertheless, responsibilities of third parties shall, in all cases, be clearly defined by appropriate agreements. Furthermore, the obligation performance securities must also be in place.

The TSA management or the security group under its supervision shall draw up a policy on information security and notify all employees who are impacted by this information security policy.

The TSA shall ensure that the information security infrastructure was properly maintained at all times. Any changes that will impact on the level of security provided shall be approved by the TSA management forum or the security group under its supervision.

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

TSA shall ensure that the security of information is maintained when the responsibility for TSA functions has been outsourced to third parties.

3.5.2 Asset Inventory and Management

The TSA must ensure that its information and other assets receive an appropriate level of protection.

The TSA must maintain an inventory of all assets and classify the asset protection requirements according to the risk analysis.

3.5.3 Staff Reliability Control

Persons shall be employed according to the requirements of the Labour Code of the Republic of Lithuania. Employment shall be recorded in an employment contract. Paragraph 26 of the Rules of

Procedure of the State Enterprise Centre of Registers (hereinafter referred to as the Rules of Procedure) sets forth the main qualification requirements as follows:

a) to have knowledge of the Lithuanian language;

b) to have necessary education or qualification;

c) to have competence in work with a computer or other office equipment;

d) to have knowledge of a foreign language (if necessary).

3.5.3.1 Staff Checking Procedure

The persons being employed shall be checked following the general procedure established by Paragraph 30 of the Rules of Procedure. In addition to the mentioned checking procedure, in accordance with which an employee's personal file shall be drawn up and retained, the employee must confirm that he/she has not been previously convicted by presenting a criminal record (certificate confirming the absence of any criminal record)[2]. This document shall also be retained in the employee's personal file.

The TSA shall be responsible that the hired personnel and hiring practices enhance and support the trustworthiness of the TSA's operations:

a) 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 precisely and clearly identified and documented;

b) the TSA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties, determining position sensitivity based on the duties and access levels. The job descriptions should include skills and experience requirements;

c) the 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 the time-stamping service management:

a) managerial personnel shall be employed who possess:

- knowledge of time-stamping technology; and
- knowledge of electronic signature technology; and

[2] According to Order No. VE-421 of the Director General of the State Enterprise Centre of Registers of 30 August 2019 "On the Approval of the Description of the Procedure for the Implementation of Corruption Prevention Measures and the List of Positions Checked by the State Enterprise Centre of Registers pursuant to Article 9 of the Law of the Republic of Lithuania on Prevention of Corruption" and the Law of the Republic of Lithuania on Prevention of Corruption

- knowledge of mechanisms for calibration or synchronization the TSA clocks with UTC; and
- familiarity with security procedures for personnel with security responsibilities; and
- experience with information security and risk assessment.

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

c) trusted roles include the roles that involve the following responsibilities:

- Security Officers: overall responsibility for administering the implementation of the security practices;
- System Administrators: authorised to install, configure and maintain the TSA trustworthy systems for time-stamping management. Authorized to perform system backup and recovery;
- System Auditors: authorized to view archives and audit logs of the TSA trustworthy systems.

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

e) The TSA shall not appoint to the trusted roles or management any person who is known to have a conviction for a crime or other offence, which affects his/her suitability for the position.

3.5.4 Physical Security Controls

The TSA shall ensure that physical access to critical services is controlled and physical risks to its assets is minimized.

Physical access to facilities concerned with time-stamping creation and management fucntions shall be limited to properly authorised individuals. Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities. Controls shall be implemented to avoid theft or compromise of information and information processing facilities.

Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in Chapters 3.3.1 and 3.3.2.

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

a) 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;

b) physical protection shall be achieved through the creation of clearly defined security perimeters. Any parts of the premises shared with other organizations shall be outside this perimeter;

c) 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 physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. telecommunications, power), structure collapse, plumbing leaks, floods, other accidents and thefts and disaster recovery;

d) controls shall be implemented to protect against equipment and software, information, data carriers and media being taken off-site without authorisation.

3.5.5 Procedural Security Controls

The time-stamping provider shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure, in particular:

a) the integrity of the time-stamping system and information shall be protected against viruses or other malicious software;

b) incident reporting and response procedures shall be precisely defined and employed in such a way that damage shall be minimized;

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

d) procedures shall be established for all positions in relation to creation and management of time-stamp tokens including trusted roles;

e) the media used in the TSA systems shall be classified and media containing sensitive data shall be securely disposed of when no longer required;

f) the system shall be constantly monitored by the TSA so that it could be timely projected when the system development should be carried out and the power and storage capacity should be increased;

g) the TSA shall act in a timely manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported in accordance with Article 19(2) of eIDAS and national legal acts;

h) in fulfilment of the time-stamp management functions, the TSA security operations shall be separated from other operations. The security procedures include: setting operational procedures and responsibilities; secure systems planning; 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 trusted personnel, but may actually be performed by specialists of lower qualification if this is defined within the appropriate security policy or other documents.

3.5.6 System Access Management

The TSA shall ensure that TSA system access is limited to properly authorised personnel.

The internal network of the TSA shall be protected from unauthorized access including access by subscribers and relying parties. Firewalls should also be configured to prevent all protocols and accesses not related to direct operation of the TSA.

The TSA shall ensure effective administration of user (including operators, administrators and auditors) access to maintain system security.

The TSA shall ensure that access to information and application system functions is restricted in accordance with the access control policy. The TSA system shall ensure separation of trusted roles including the separation of the system administrator and operation functions.

The TSA personnel shall be properly authenticated and identified before using critical components of the time-stamp creation and management system.

The TSA shall ensure accounting of the personnel activities with the TSA systems, for example, by recording and retaining logs of use of the systems.

All computer network components (routers, etc.) are kept in a physically secure environment, their configurations must be periodically audited for compliance with the requirements specified by the TSA.

Continuous monitoring and alarm facilities shall be provided to enable detection, registration and reaction in a timely manner upon any unauthorised and/or irregular attempts to access the TSA resources.

3.5.7 Trustworthy Systems Deployment and Maintenance

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 to ensure that security is built into IT systems.

Change control procedures shall be applied for emergency software fixes, releases and modifications of any operational software.

3.5.8 Compromise of the TSA Operations

The TSA shall ensure in the case of events, which affect the security of the time-stamping services, including compromise of the private key or detected loss of calibration, that relevant information is made available to subscribers and relying parties of the TSA. Information shall be reported in accordance with Article 19(2) of the eIDAS and national legal acts.

The TSA shall have a recovery plan to address the compromise or suspected compromise of the private key or loss of calibration of a TSA clock in place. In the aforementioned cases of compromise of the TSA operations, the general operation termination plan and the actions detailed in the CPS shall be observed.

In the case of a compromise or suspected compromise or loss of calibration the keys, the TSA shall make available to the subscribers and relying parties a description of compromise that occurred.

In the case of compromise to a TSA's operation (e.g. keys) or suspected compromise or loss of calibration, the time-stamp tokens shall not be issued until steps are taken to recover from the compromise.

In case of major beach of the operations (compromise of the private key or loss of calibration with the UTC), the time-stamp provider shall make available the information, which may be used to identify the time-stamp tokens, which may have been affected, to all subscribers of time-stamp tokens and relying parties as soon as possible by all possible means unless this breaches the privacy agreements with subscribers or reduce the security of services.

3.5.9 TSA Practice Termination

In case of termination of the provision of time-stamping services, the TSA shall obligate to operate according to the operation termination plan agreed with the supervisory body (hereinafter referred to as the agreed plan), including the following actions (in so far as they are not in contradiction with the agreed plan):

a) the TSA shall inform the supervisory body, all subscribers of the time-stamp tokens, the relying parties and the trust service supervisory body about the termination of time-stamping services at least 9 (nine) months prior to the date of termination of the operations;

b) the TSA shall terminate cooperation with all subcontractors providing time-stamping services;

c) taking into account the planned date of termination of services but not later than 6 (six) months prior to the said date, the TSA shall provide the supervisory body with: 1) the information about the organisation taking over the operation; 2) the takeover agreement; 3) a detailed plan agreed by the TSA;

d) the TSA shall transfer to a reliable party or perform its obligations to make available its public key or its certificates to relying parties within a reasonable period;

e) upon the decision not to transfer the activities of the Centre of Registers to the organisation taking over the operation (the third party), liquidation of the Enterprise or declaration of its bankruptcy, or upon decision of the supervisory body to revoke the qualified trust service status, the TSA must destroy all private keys in such a way that they cannot be restored.

The TSA shall have an arrangement to cover the costs of fulfilling the aforementioned requirements in case of bankruptcy or in other cases of insolvency. The TSA shall cover its practice by insurance, the amount of which is not lower than specified in Article 10 of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

The TSA shall state in the TSPS the provisions made for the termination of service, including notification of the affected entities and transfer of the TSA obligations.

The TSA shall take steps to have all certificates used for signature of the time-stamp token revoked.

Provision of time-stamping services shall be terminated in accordance with the procedure and under the terms and conditions provided for in the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

3.5.10 Compliance with Legal Requirements

The TSA shall ensure conformity of the procedures and operations with the legal requirements, in particular:

a) the requirements of the eIDAS;

b) the requirements of the Law of the Republic of Lithuania on Legal Protection of Personal Data;

c) the requirements of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

3.5.11 Recording and Management of Information Concerning Operation of Time-Stamping Services

The TSA shall ensure that all relevant information concerning the creation and management of time-stamp tokens is recorded and archived for a period of time defined in the TSPS, in particular, for the purpose of providing it as evidence in legal proceedings.

General requirements shall be as follows:

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

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

c) records shall be made available if required for the purposes of providing evidence of the correct operation for the purpose of legal proceedings;

d) the precise time of significant operations carried out by the TSA (key management, clock synchronization, etc.) shall be recorded;

e) after the expiration of the validity of the TSA keys, the records to be archived shall be held for a period of time specified in the terms and conditions for the provision of services;

f) the archived records shall be protected from deletion or other destruction for the entire storage period;

g) any information recorded about the subscribers of time-stamp tokens shall be kept confidential except as where agreement is obtained from the subscriber for its wider publication.

The TSA key management requirements:

a) all information concerning the life-cycle of the TSA key pair shall be logged and archived;

b) all information concerning the TSA certificates shall be logged and archived.

The TSA clock synchronisation requirements:

a) all information concerning operations of synchronization of the TSA's clock to UTC shall be logged and archived. Furthermore, information concerning calibration or synchronisation of clocks used for issue of the TSA time-stamp tokens shall be stored;

b) all records concerning failures of synchronisation of the TSA clocks shall be documented.

4. ORGANISATIONAL ISSUES

The TSA shall ensure reliability of its operations by employing the following measures:

a) the TSA shall make its time-stamping services accessible to all applicants whose activities fall within the scope of application of the time-stamp token defined by the TSA and that accept the terms and conditions of provision of services;

b) the TSA has systems for quality and information management appropriate for the provision of times-tamping services;

c) the TSA has adequate resources to cover its liabilities arising from the provision of time-stamping services;

d) the TSA has the financial stability and resources required to operate in conformity with this policy;

e) the TSA has a sufficient number of human resources having the necessary education, technical knowledge and experience necessary for provision of time-stamping services;

f) the TSA has properly legally executed sub-contracting, hire and other contracts.

5. ADMINISTRATION OF THE TSP

This chapter shall provide for the requirements on administration and supervision of the TSP.

A newly approved version of the TSP shall invalidate the previous version of the TSP. A new version shall be valid as of the date indicated on the cover page of the TSP. The latest version of the TSP shall be published in the repository on the Internet[3].

The users shall follow the latest version of the TSP, the OID of which is specified in the electronic time-stamp.

5.1. Procedures for Amending the TSP

The TSP may be amended in the event of inaccuracies observed, in case of a need to update the TSP, or upon receipt of proposals from the related parties.

Amendments to the TSP shall fall into the following two categories:

a) substantial amendments when users must be informed thereof and the TSP OID must be changed;

b) insignificant amendments when it is not mandatory for the TSA to inform other parties thereof, and the TSP OID is not changed.

After making substantial amendments, the first digit of a new TSP version and OID version element (the last digit) respectively shall be changed. After making insignificant amendments, the second and next digits of the new TSP version shall be changed.

Insignificant amendments in the TSP shall be possible only in cases when they are of recommendatory, explanatory or corrective nature, or when contact details of persons responsible for management of the TSP have changed.

In other cases, amendments shall be considered as substantial and their unique identifier shall be changed with every amendment to the TSP. In all cases, amendments shall be considered as substantial also in cases when they alter the level of security of time-stamping services.

The TSP shall be monitored, amended and approved under the following procedure:

a) the staff responsible for security policy shall revise the TSP every 1 (one) year as of the last TSP revision date and make sure if the TSP is relevant. In case of determining the need to amend the TSP in the course of review, amendment of the TSP shall be initiated;

b) amendments to the TSP shall be initiated by the TSA or users;

c) the staff responsible for the security policy shall draft a new version of the TSP;

[3] https://www.elektroninis.lt/lt/n/teisininformacija-504

d) the new version of the TSP shall be approved by the Director General of the Centre of Registers;

e) the approved new version of the TSP shall be placed in the repository where the TSP shall be fully accessible to all persons.

6. DEFINITIONS AND ABBREVIATIONS

Certificate/ Seal Revocation List (CRL) means a list of certificates that have been suspended or revoked, which is periodically (or urgently) issued and signed by the Centre of Registers. Such a list usually contains the name of the enterprise that made this list, date of making the list, the expected date of issuing the next version of the list, serial numbers of the revoked certificates, the time of, and reasons for, suspension or revocation of the certificates.

Compromise means loss, theft, modification, illegal use of the private key or any other violation of the private key security.

Cryptographic module – see Hardware security module.

Electronic signature (signature) means data, which are embedded, attached to, or logically bound with, other data for verification of authenticity thereof and identification of the signatory.

Hardware security module (cryptographic module) (HSM) means hardware and software used for generation of encryption key pairs – private and public keys – and/or for creation of electronic signatures.

Key pair means a mathematically associated pair of encryption (cryptographic) keys: private and public keys.

Private key means unique data that are used by a signatory to create the electronic signature (signature creation data).

Relying parties – see users of time-stamp tokens.

Repository means the repository of certificates and other information of the trust service provider accessed by users on-line at any time on the Internet site: www.rcsc.lt/repository/.

Subscriber means a person entering into agreement with the TSA and whom time-stamping services are provided.

Time-Stamping Authority (TSA) means certification service provider providing time-stamping services.

Time-Stamping Policy means a set of rules on creation and management of a time-stamp token, establishing rights and obligations of the service provider and users of time-stamp tokens. Time-Stamping Policy is chosen by the users of time-stamp tokens and implemented by the service provider.

Time-Stamping Practice Statement means rules on provision of time-stamping services approved by the service provider.

Time-stamp token means the data, which are logically bound with other data and verify that those other data existed prior to the time indicated in the time-stamp token.

Users of time-stamp tokens means recipients of a time-stamp token who rely upon this time-stamp token, including subscribers.

UTC means the Coordinated Universal Time, an internationally managed unified system of atomic clocks.

CP –	Qualified Certificate (Electronic Signature and Electronic Seal) Policy of the State Enterprise Centre of Registers
CPS –	Certification Practice Statement of the State Enterprise Centre of Registers
CRL –	Certificate/ Seal Revocation List
ETSI –	European Telecommunication Standardisation Institute
FIPS –	Federal Information Processing Standards
OCSP –	On-Line Certificate/ Seals Status Protocol
OID –	Object Identifier
RCSC –	Certification Centre of the Centre of Registers
TSA –	Time-Stamping Authority
TSP –	Time-Stamping Policy of the State Enterprise Centre of Registers
TSPS –	Time-Stamping Practice Statement of the State Enterprise Centre of Registers
UTC –	Coordinated Universal Time