STATE ENTERPRISE CENTRE OF REGISTERS

TIME-STAMPING PRACTICE STATEMENT OF THE CERTIFICATION CENTRE OF THE CENTRE OF REGISTERS

Unique object ID (OID): **1.3.6.1.4.1.30903.1.4.2**
Version: 2.7
Valid from: 29 May 2020

29 May 2020

TABLE OF CONTENTS

History of amendments to the Time-Stamping Practice Statement of the Certification Centre of the Centre of Registers:

Version	Date	Status
0.1	19 June 2008	Draft Statement
1.0	28 October 2008	First version
2.0	28 April 2017	Second version
2.1	11 July 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 after comments from the Communications Regulatory Authority of the Republic of Lithuania
2.6	11 May 2020	Changes after comments from the Communications Regulatory Authority of the Republic of Lithuania
2.7	29 May 2020	Changes after comments from the Communications Regulatory Authority of the Republic of Lithuania

Document approval:

Document preparation	Name, surname	Date	Signature
Document approved by	Saulius Urbanavičius, Director General	29 May 2020	

1. INTRODUCTION

The State Enterprise Centre of Registers (hereinafter referred to as the "Centre of Registers") 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 Justice of the Republic of Lithuania. The enterprise administers 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 Settlements, 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 afore-mentioned and other registers, keeps register archives. Information about the enterprise is available at http://www.registrucentras.lt.

To execute the assigned functions efficiently, the Centre of Registers applies modern information technologies. The Centre of Registers has established the Certification Centre of the Centre of Registers (hereinafter – RCSC) – a unit providing services pertaining to the creation of qualified certificates, and time-stamping services.

The current Time-Stamping Practice Statement (hereinafter – TSPS) defines technical, procedural and staff policy issues of the RCSC related to the provision of services on creation and management of time-stamp tokens.

1.1. Overview

The current TSPS defines in detail the RCSC practices pertaining to the provision of services on creation and management of qualified time-stamp tokens (hereinafter – time-stamp tokens) required to ensure a long-term validity of the qualified electronic signatures.

The TSPS contains description of the requirements for creation of time-stamp tokens with the accuracy of 1 (one) second, approved by the public key certificates.

The TSPS structure complies with recommendations contained in the following documents:

a) ETSI EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;

b) ETSI EN 319 422 v1.1.1 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and electronic time-stamp token profiles;

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

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

e) Order No 1V-1055 of Director of the Communications Regulatory Authority of the Republic of Lithuania of 26 October 2018 "On the Approval of the Description of the Procedure for Verifying the Identity and Additional Specific Attributes When Issuing Qualified Certificates for Electronic Signature, Electronic Seal, and Certificates for Website Authentication";

f) 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".

1.2. Identification

The current TSPS is approved by Order No v-115 of the Director General of the State Enterprise Centre of Registers as of 28 April 2017.

Certificates used to provide time-stamping services shall be issued under the Qualified Certificate/ Seal Policy of the Certification Centre of the Centre of Register, the OID of which is 1.3.6.1.4.1.30903.1.1.7.

The TSPS shall be placed in the repository on the Internet.

The unique identifier (OID) of the TSPS shall be as follows: **1.3.6.1.4.1.30903.1.4.2**.

Digits separated by dots in this identifier shall have the meanings indicated below (see *Table No 1*)

Table No 1. Field meanings of the TSPS unique identifier

Title	Meaning
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 (Certification Centre of the Centre of Registers – RCSC)	1
Document type (Time-Stamping Practice Statement)	4

Document version	2

The current TSPS has been prepared in compliance with the Time-stamp Policy (hereinafter – TSP), the unique OID thereof is **1.3.6.1.4.1.30903.1.3.2**.

1.3. Users and Applicability of Time-stamp Tokens

1.3.1 Users of time-stamp tokens

Time-stamp tokens shall be designed for the electronic signature users seeking to prove that the electronic signature has been created prior to the time indicated in the time-stamp token. A time-stamping service provider may provide public services and he may also service the restricted user groups.

1.3.2 Applicability of time-stamp tokens

The principal field of application of the time-stamp tokens provided by the RCSC shall be provision of time-stamping service for secure electronic signatures created with the secure signature creation device and verified with qualified certificates in accordance with the Certification Practice Statement (hereinafter referred to as the "CPS"), the Qualified Certificate Policy (hereinafter referred to as the "CP") and the TSP. However, the RCSC shall not set any limitations on usage of time-stamp tokens. Time-stamp tokens provided by the RCSC may be used in the process of electronic transactions, electronic documents' archiving, etc.

1.4. RCSC Organisational Structure

The RCSC shall consist of the Certification Authority (hereinafter – CA) established in the premises of the State Enterprise Centre of Registers, the Time-Stamping Authority (hereinafter – TSA), the Authority supporting certification operations (hereinafter – Support Service) and the Registration Authority (hereinafter – RA), both acting according to the agreement signed with the CA and subordinate to the CA.

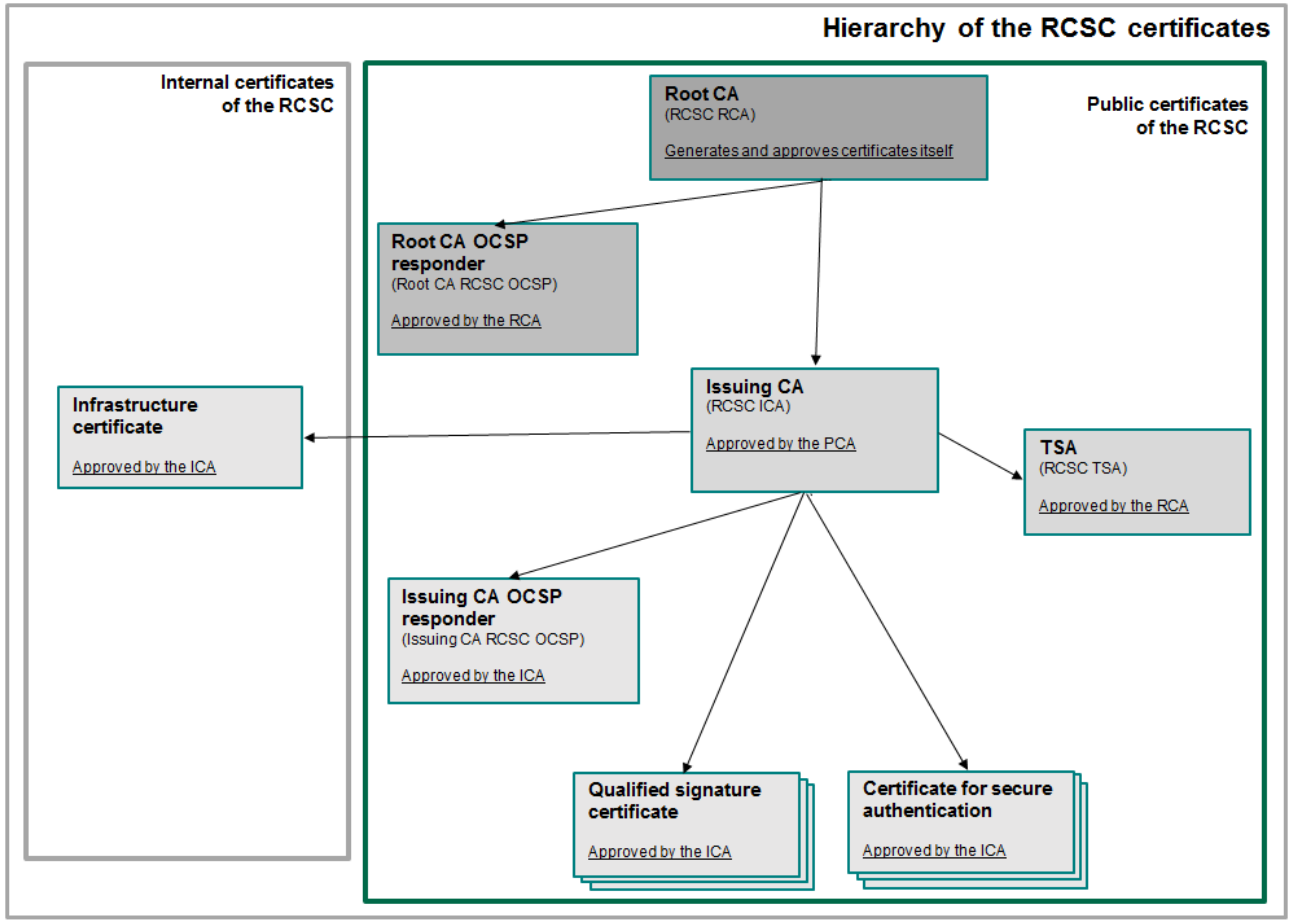
1.5. Sequence of the CA and TSA Certificates

The sequence of the CA certificates shall be based upon two-level CA hierarchy. Root CA at the top level shall use a self-signed certificate, issue Issuing CA and Root CA OCSP responder certificates, sign Root CA CRLs, be off-line and stored in an isolated environment. Issuing CA shall issue Time-Stamping Authority (hereinafter – TSA), personal, Issuing CA OCSP responder and infrastructure certificates, and sign Issuing CA CRLs.

The scheme of sequence of the CA certificates is provided below (see *Scheme **1***).

1.6. Legal Effect of Electronic Time-Stamps

An electronic time-stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time-stamp. A qualified electronic time-stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound. A qualified electronic time-stamp issued in one Member State shall be recognised as a qualified electronic time-stamp in all Member States.



Scheme 1. Hierarchy of the RCSC certificates

1.7. Contact Details

1.7.1 Organisation that issued and manages the TSPS

Organisation	State Enterprise Centre of Registers
Address:	Lvovo str. 25-101, 09320 Vilnius, Lithuania
Telephone:	+370 5 268 8202
URL:	http://www.registrucentras.lt
E-mail:	info@registrucentras.lt

1.7.2 Contact person

Person responsible for the conformance of the TSPS to the TSP, and for the TSPS administration shall be:

Head of e-Signature Certificates Division of the State Enterprise Centre of Registers,

Lvovo g. 25-101, 09320 Vilnius, Lithuania,

Tel.: +370 5 2688 388,

E-mail: *info@elektroninis.lt*.

1.7.3 Information about the services provided by the CA

The CA website www.elektroninis.lt provides information about ordering of time-stamps, the current CRL list and other services provided by the CA. This website also contains the up-to-date versions of CP, CPS, TSP, and TSPS.

2. GENERAL PROVISIONS

This chapter presents obligations, provisions regarding legal and general practices of the TSA and parties related thereto.

2.1. Obligations

2.1.1 TSA obligations

The TSA must provide all the time-stamping services consistent with the current TSPS, and ensure conformance of the TSPS to the TSP under implementation.

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

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 must ensure that its clocks used for creation of time-stamp tokens are synchronized with the UTC within the accuracy of no more than 1 (one) second. The TSA shall undertake to publish the latest TSPS and TSP versions in the repository on the Internet.

The TSA shall respond to all incoming time-stamp requests; however, they shall be formed in accordance with RFC3161. Users shall be identified according to concluded/signed agreements and this verification shall be performed by a part of the infrastructure – Firewall.

2.1.2 Obligations of subscribers to the time-stamp tokens

After obtaining a time-stamp token, the subscribers must verify that the service provider has correctly signed the time-stamp token, and that 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 TSP, TSPS, terms and conditions on the provision of time-stamp token or agreements with the service provider.

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

2.1.3 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 the related parties, must include obligations on the relying parties that, when relying on a time-stamp token, they shall:

a) assure that the time-stamp token has been correctly signed, that the certificate corresponding to the signature has been valid during signing process, and that the private cryptographic key (hereinafter – 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, TSPS, terms and conditions on the provision of time-stamp token or agreements with the service provider.

c) take into account any other precautions prescribed in the agreements or the rules concerning the use.

If, during verification of a time-stamp token, validity of the TSA certificate has expired, a person must assure 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

The TSA shall be liable for its illegal actions, and indemnify the subscribers for any caused damages in accordance with the procedure established by laws of the Republic of Lithuania.

Liability restrictions shall be specified in the agreements on the provision of time-stamp tokens concluded with the subscribers.

2.3. Legal Provisions and Interpretations

2.3.1 Governing legal acts

Creation and provision of time-stamp tokens, requirements for and liability of the providers of time-stamp tokens shall be collectively established by:

a) the latest version of the European Data Protection Directive;

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

c) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

d) the latest version of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions;

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

2.3.2 Dispute resolution procedures

Any disputes between the TSA and the end users shall be resolved by the goodwill negotiation. If the dispute has not been resolved, one shall address to the courts of the Republic of Lithuania.

2.4. Fees

Fee for provision of the TSP and TSPS

The TSP and TSPS shall be provided free of charge. They shall be made freely available at:

http://www.rcsc.lt/repository.

2.5. Information Provision and Repositories

2.5.1 Information provided by the TSA

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) up-to-date versions of the TSP and TSPS;

b) certificate/ seal revocation lists (hereinafter – CRL) of the TSA;

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

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

2.5.2 Frequency of information updating

Information provided by the TSA shall be updated with the following frequency:

a) amendments to the TSP and TSPS shall be made as provided for under the TSP and TSPS;

b) once amended, data of the certificates owned by the TSA shall be published immediately;

c) other information to be published and having been updated shall be published after its receipt.

2.6. Compliance Audit

Compliance of the TSA practices with the TSP and TSPS shall be audited in accordance with the internal procedures established by the TSA as detailed by the TSA in Chapter 8.

2.6.1 Frequency of audit of the TSA practices

Compliance of the TSA practices with the TSP and TSPS must be audited at least once every 1 (one) year or after significant amendments.

2.6.2 Verifying compliance

a) Following Article 20(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter – eIDAS), the CA shall be audited every 24 (twenty-four) months by a conformity assessment body.

b) Following Article 20(2) of eIDAS, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the CA (at the expense of the CA), to confirm that the services provided by the CA fulfil the requirements laid down in eIDAS.

c) Following Article 20(3) of eIDAS, where the supervisory body requires the CA to remedy any failure to fulfil requirements under eIDAS and where the CA does not act accordingly within a time limit set by the trust service supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of the CA or of the affected service it provides and inform the body referred to in Article 22(3) of eIDAS for the purposes of updating the trusted lists. The supervisory body shall inform the

qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

d) Provision of certification services shall be supervised by the trust service supervisory body authorized by the Government of the Republic of Lithuania.

2.6.3 Topics covered under the audit

To assess the TSA practices, the following topics shall be covered under the audit:

a) physical security;

b) time-stamping services and procedures for provision of these services to the end users;

c) security of software and computer network access system;

d) reliability of the TSA staff;

e) logs on registration of the TSA system operations and practices;

f) creation and usage of information back-ups;

g) archive keeping procedures;

h) log file on changes to the TSA structure;

i) log file on checking and maintenance of hardware and software.

2.6.4 Actions after finding deficiencies

Internal and external audit protocols shall be delivered to the TSA security officer. The security officer must within 30 (thirty) calendar days formulate in writing his opinion regarding deficiencies specified in the protocol, anticipate actions and a period for elimination of deficiencies. Information regarding elimination of deficiencies shall be presented to the organisation that performed the audit.

If the deficiencies found poses a threat to the security of procedures for provision of time-stamping services, the security officer may adopt the decision on temporary suspension of the TSA service provision. In this case, all the subscribers to time-stamp tokens shall be informed accordingly and notified of the scheduled time when the practices are to be resumed.

2.6.5 Publication of the audit results

Conclusions of the audit regarding conformity of the TSA practices shall be placed in the TSA repository and made publicly available.

2.7. Intellectual Property Rights

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

3. OPERATIONAL REQUIREMENTS

This chapter defines the requirements for the TSA practices when providing the services on creation and management of time-stamp tokens.

3.1. 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:

a) the TSA contact details;

b) the unique 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 parties relying on time-stamp tokens;

i) information on how to verify the time-stamp token;

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.

This 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.

3.2. Life Cycle of the TSA Cryptographic Keys

3.2.1 Generation of the TSA cryptographic keys

The TSA key pair shall be generated using a workstation, designed exclusively for this purpose and connected to hardware security module (cryptographic module). Hardware security module shall meet the requirements identified in the FIPS PUB 140-2 standard of level 3. The TSA private key must be generated under physically secured circumstances, under, at least, dual control of persons in trusted roles.

Key pair generation operations shall be logged, by indicating the date of performance thereof, and signed by all the persons involved in the generation process. The log files made shall be retained, since later they may be required to perform the checks (audit) and general system revision.

3.2.2 TSA private key protection

Hardware security module (cryptographic module) used to create the TSA electronic signature/seal for signing time-stamp tokens shall meet 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.

3.2.3 TSA public key distribution

The TSA public key shall be made available in the TSA certificate, OCSP responder notifications and the official website of the RCSC.

3.2.4 Recovery of the TSA private key

The TSA private key shall be restored using the system cards associated with the cryptographic equipment, each of such cards containing data fragment of the cryptographic key used for encrypting a copy of the TSA private key. The procedure for recovering the TSA private keys shall be analogous to the TSA key generation procedure (see Chapter 3.2.1).

3.2.5 Transferring of the private key into the cryptographic module

Procedures for transferring of the TSA private key into and from the cryptographic module shall be applied only in cases of the private key restoring and backing up.

3.2.6 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.

3.2.7 End of life cycle of the TSA cryptographic key pair

Upon expiration of life cycle of the TSA key pair, the TSA must ensure that the private key is destroyed and cannot be duplicated.

3.2.8 Life cycle of the TSA cryptographic module

The TSA must ensure security of the cryptographic 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) the cryptographic module used for signing time-stamp tokens is functioning properly;

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

3.3. Time-Stamping

3.3.1 Time-stamp token

The TSA shall sign a time-stamp token being issued with its own electronic signature. The TSA private key shall be used for signing only time-stamp tokens being issued, and shall not be used for any other purposes.

No more signatures shall be used in the time-stamp token. The identifier of the RCSC TSA certificate shall be included as an attribute in the self-signed certificate. If the TSA system clock is detected as being out of the declared accuracy, HSM automatically ceases creating and issuing time-stamp tokens.

The TSA shall use:

- "ncipher DSE200 Document SealingEngine" TS, which meets HSM (FIPS 140-2 Level 3 Certified) requirements. Certificate No 1197.
- "Utimaco TimestampServer Se500 LAN V4" TS, which meets HSM (FIPS 140-2 Level 3 Certified) requirements. Certificate No 2814
- "Utimaco TimestampServer Se1500 LAN V4" TS, which meets HSM (FIPS 140-2 Level 3 Certified) requirements. Certificate No 2814.

The time-stamp token shall include:

a) hash of the data being time-stamped that were provided by the subscriber;

b) a unique serial number used to order and identify time-stamp tokens;

c) the TSP unique identifier;

d) the TSA identifier, which meaning is the same as one of those from the *subject* field of the RCSC TSA certificate used to verify a time-stamp token;

e) from the fields being chosen, only the *nonce* field shall be maintained;

f) values of the TSA system clock are traceable to the time value distributed by at least one of the UTC laboratory.

Field	**Meaning and constraints of meanings**
Version	2
PolicyID	**0.4.0.2023.1.1**
messageImprint	Field meaning is the same as in the Time-stamp request (*TimeStampReq)*, if the size of data hash corresponds to the expected size of hashing algorithm indicated in the *hashAlgorithm* field.
serialNumber	Users of time-stamp tokens must maintain integer numbers up to the length of 160 bits.
genTime	UTC time
Accuracy	1s
ordering	FALSE
nonce	Obligatory, if such a field was in the Time-stamp request (*TimeStampReq).* The field meaning is the same as in the *TimeStampReq*.
TSA	CN = RCSC TSA O = VI Registru Centras - I.k. 124110246 OU = RCSC C = LT

3.3.2 Synchronization with the UTC

The TSA shall ensure that its time is synchronized with the UTC (Coordinated Universal Time) within the accuracy of 1 (one) second. For this purpose, the TSA shall ensure that:

a) the TSA system 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 outside its calibration;

c) the difference between the TSA clocks and the UTC is recorded. Time shall be computed following the BIPM and NTP recommendations; and

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.

3.4. Collection of Log Files on the TSA Operations

3.4.1 Logged events

The main operations of the TSA system shall be recorded in the secure Operation Log. The operations being logged shall cover:

a) events related to the life cycle of the TSA-owned cryptographic keys and certificates;

b) events related to the calibration and synchronization of the TSA system clocks;

c) requests to create a time-stamp token;

d) facts on creation of a time-stamp token;

e) suspension and dissolution of the Time-Stamping Authority.

Each log must contain the following information:

a) event type;

b) event identifier;

c) event date and time;

d) identifier or other data enabling to identify a person responsible for such event;

e) decision on whether the event is traceable to the operation, which has been performed either successfully or erroneously.

The Operation Log shall be protected by the access management system and signed with the infrastructure signature of the RCSC.

In addition to the Operation Log, Logs on Registration of the TSA System Practices shall be kept, enabling to monitor the system operation, receive information on shutdowns and errors of the system operations.

The Diagnostics Log shall record detailed system operations that are used for analysis of the system functioning, diagnostics and elimination of shutdowns. The main users of the Diagnostics Log shall be the system developers and administrators. Details of records in the Diagnostics Log shall be manageable by receiving more detailed or less detailed information on certain operations of the system.

The Error Log shall record information on system shutdowns and errors, by indicating the time when the shutdown occurred, source and description of the shutdown.

System monitoring may be also performed using the standard software.

When forming log files on the system operation, the following information shall be included:

a) alerts of system firewalls and intrusion detection system (IDS);

b) data on each change to hardware and software;

c) data on changes to the computer network and its connections;

d) data on physical access of the staff into the secure zones and breaches;

e) data on changes to passwords, PIN codes and the staff positions;

f) successful and unsuccessful prompts into the TSA databases and server application programs;

g) history on creation of back-up copies, archival logs, and databases.

3.4.2 Frequency of reviewing of log files on events

Logs on Registration of the TSA System Operations and Practices shall be reviewed at least once every 1 (one) month. Each event of major importance or event occurred due to system malfunctioning must be described.

3.4.3 Retention period of log files

Logs on Registration of the TSA System Operations and Practices shall be retained by the TSA for 10 (ten) years, the subsequent retention being regulated by the Law on Documents and Archives of the Republic of Lithuania.

3.4.4 Protection of log files

Back-up copies of Logs on Registration of the TSA System Operations and Practices shall be made once per week. If the number of log files exceeds the number anticipated for a particular Log, the content of Log shall be transferred to the archive. Data recorded into the archive shall be encrypted using the AES algorithm. The encryption key shall be managed by the TSA security officer.

Logs on Registration of the TSA System Operations and Practices may be reviewed solely by the TSA security officer, TSA administrator or auditor. Parameters of the access into the Log shall be such that:

a) the security officer might solely enter into or remove from the archive the Log files;

b) it would be possible to detect any breach pertaining to data corruption;

c) nobody would be entitled to change the Log content.

3.4.5 Log file collection system

The TSA shall use the internal system for registration of the log files on events. Wherever possible, logs shall be made automatically.

3.5. Data Archiving

3.5.1 Data transferred into the archive

The following data shall be transferred into the archive:

a) logs on Registration of the TSA System Operations and Practices;

b) database on subscribers to a time-stamp token;

c) history of keys and certificates owned by the TSA from their generation until destruction.

3.5.2 Period for data retention in the archive

Data shall be retained in the archive for 10 (ten) years, the subsequent retention being regulated by the Law on Documents and Archives of the Republic of Lithuania.

3.5.3 Archive protection

The TSA archive shall be protected in line with the internal procedures established by the Centre of Registers and Law on Documents and Archives of the Republic of Lithuania.

3.5.4 Archive backing-up

Back-up copies shall enable to retrieve the system operation after shutdowns. For this purpose, copies of the following software and data files shall be made:

a) installation disk with the TSA system software;

b) installation disk with the TSA application programs;

c) installation disks of the WWW server and repository;

d) copy of the repository data.

Back-up copies of databases shall be made every day, of other information – once per week. Operation of the TSA system after shutdowns shall be restored not later than within 48 (forty eight) hours.

3.6. 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 Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 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 afore-mentioned 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 to all subscribers of

time-stamp tokens and relying parties information which may be used to identify the time-stamp tokens which may have been affected, unless this breaches the privacy agreements with subscribers or reduces the security of services as soon as possible by all possible means.

3.6.1. Incident registration, identification and analysis procedure

The CA shall follow the procedure below:

a) in case of shutdowns/incidents in operation of the information system that designate unusual or non-conforming operation of the information system components, such failures/incidents shall in all cases be registered in the event log that must be archived and protected from damage, loss, unauthorized or accidental change or destruction to ensure that the evidence of offences committed during electronic information (cyber) security incidents is appropriate and sufficient for law enforcement bodies to establish the fact of offences, and to prevent the perpetrators of offences from denial of the fact;
b) in case of registering failures/incidents, such failures/incidents shall be prioritized and identified in accordance with the Description of the Security Information and Event Management Procedure. During identification, an event record shall be identified and assigned a category or priority depending on settings of the specialised event log analyser tools;
c) during analysis, it shall be determined whether an event or a universe of events at a given moment of time meets certain alert generation rules established by specialised event log analyser tools. Where, during analysis, the specialised event log analyser tools determine that a certain event or a universe of events at a given moment of time meets certain established alert generation rules, the specialised event log analyser tools shall automatically generate the alert;
d) administrators of information system components shall revise the generated alert and, where appropriate, notify responsible persons of the alert, its content and circumstances;
e) the appointed security officer shall revise the generated alert and assess whether it can be related to any breach of security or loss of integrity provided for in Article 19(2) of eIDAS, the security officer shall immediately, but not later than within 4 (four) hours, convene a working group. The supervisory body and natural or legal persons shall be informed about the above-mentioned incidents in accordance with the procedure set forth in point e) of Part 2 of Chapter 4.4.2 of the CPS no later than within 24 (twenty four) hours;
f) pursuant to the procedure for management of information technology incidents and electronic information security (cyber) incidents laid down by order of the Director General of the Centre of Registers, incidents shall be registered with an appropriate marking designating that it is related to a breach of security or loss of integrity provided for in Article 19(2) of eIDAS;
g) with a view to ensuring the compliance with legal requirements and possessing collected data for potential future investigations of electronic information (cyber) security incidents, the events shall be retained.

3.7. Termination of the TSA Operations

In case of termination of provision of time-stamping services, the TSA shall ensure that potential disruptions to subscribers and relying parties are minimised. In the event of cessation of the time-stamping services, the TSA shall ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

Before the TSA terminates its operations, the following procedures shall be executed as a minimum:

a) the TSA shall inform the supervisory body on any intended termination of the activity at least 3 (three) months prior to the date of termination of the activity and make available to all subscribers of the time-stamp tokens, relying parties and electronic signature supervisory body information concerning termination of time-stamping services not later than 1 (one) month in advance;

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

c) the TSA shall transfer all obligations in relation to maintaining of event logs and audit archives to a reliable transferee or a supervisory body to demonstrate the proper operation according to the rules and procedures for a reasonable period within 1 (one) month;

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 for a reasonable period;

e) all private keys shall be destroyed by the TSA in a manner such that the private keys cannot be retrieved.

The TSA shall have an arrangement to cover the costs to fulfil the afore-mentioned requirements in case of bankruptcy or in other cases of insolvency. The TSA shall insure its third party liability for the amount not lower than the amount determined by the trust service supervisory body.

The TSA shall state in the TSPS the provisions made for termination of service including: notification of affected entities and transferring 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 latest version of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions. Detailed procedures, time limits and actions of the TSA shall be specified in the plan for termination of operations in provision of trust services.

4. PHYSICAL, PROCEDURAL AND STAFF SECURITY CONTROLS

4.1. Physical Security Controls

The TSA computer system, workplaces of operators, and information resources shall be equipped and stored in the appropriate site, which is physically safeguarded against any unauthorised access thereto, any destruction of the equipment and operation. Access to the key components of the system shall be monitored. Each access of persons to the system shall be registered; stability of electric power supply, temperature and humidity shall be under surveillance.

4.1.1 Head office location

The address of the TSA head office shall be as follows:

Vinco Kudirkos str. 18, LT-03105 Vilnius, Lithuania.

TSA hardware hosting addresses are as follows:

Vinco Kudirkos street 18-3, LT-03105 Vilnius, Lithuania

Tilto street 17, LT-01101 Vilnius, Lithuania

4.1.2 Physical access

With the aim to control physical access to the TSA premises and staff activities inside the premises, a respective video surveillance system operating 24 hours per day has been installed. Fire prevention and protection system, water-exposure protection system, intrusion prevention system and back-up power supply system are all in operation.

Persons visiting the TSA shall be received during working days at the working hours approved by the Order of the Director General of the Centre of Registers. During the remaining time (including days-off), only the persons authorised by the TSA management whose names and surnames are known to the security service shall have the right to enter the TSA head office.

Visitors may enter the TSA premises only if accompanied by the TSA authorised persons.

Three security zones of the TSA premises shall be distinguished:

a) computer system zone;

b) zone of operators and administrators;

c) zone of developers and programmers.

Computer system zone shall be established in the common repositories of the service stations of the Centre of Registers. Equipment associated with the time-stamping services shall be stored in separate consoles of the service stations. Access to the repositories of service stations shall be regulated by the electronic system cards, the appropriate access control card reader being installed at the entrance door. Each entrance to and exit from this zone shall be automatically registered in the Log on Registration of System Practices.

Access to the zone of operators and administrators shall be controlled by the electronic cards and the respective card readers. Safe-deposit boxes shall be used for storage of confidential information. Prior to using the operator and administrator terminals, authorisation of a staff member shall be verified. Only authorised persons may be present in this zone. At least 2 (two) persons must be simultaneously present in the zone.

Zone of developers and programmers shall be protected in the same manner as that of operators and administrators. There shall be no such requirement that at least 2 (two) persons must be simultaneously present in this zone. Developers and programmers shall not have access to the confidential information. If necessary, the security officer must be present in the zone at the same time. Projects under implementation and software thereof shall be tested using a pilot version of the TSA system created or its model.

4.1.3 Electric power supply and air conditioning

Modern air conditioning systems maintaining the appropriate temperature and protecting the equipment from dust have been installed in the repositories of service stations of the Centre of Registers. In the event of interruptions of the electric power supply from the network, back-up power resources (4 UPSs and 3 diesel electric power generators) shall ensure regular system operation for 96 (ninety six) hours.

4.1.4 Water-exposure protection

Humidity and water sensors have been installed in the computer system zone. They shall be connected to the security system of all premises of the Centre of Registers. Workers on watch shall be informed of possible threats and in the event of disaster obliged to address to the public city authorities, notify accordingly the TSA security officer and the TSA administrator.

4.1.5 Fire prevention and protection

Fire prevention and protection system, meeting the requirements established by the fire prevention and protection service, has been installed in the RCSC premises. Gas automatic fire-extinguishing system has been installed.

4.1.6 Media storage

Depending on the importance of information, storages with archival data and back-up copies of data shall be kept in the fire-proof safe-deposit boxes located in the zones of operators and administrators.

4.1.7 Waste disposal

Paper and electronic storages containing information affecting security of the TSA operations shall be destroyed using shredders upon expiration of the information retention period. Storages of encryption keys and PIN codes shall be destroyed using devices of DIN3 class (thereby, only storages containing information, which cannot be fully erased, shall be destroyed, e.g., cryptographic cards).

4.1.8 Backup storage

Copies of the current information produced by the system as well as installation copies of all the TSA application programs shall be stored in the archive. In the event of failure, this shall allow recovering any of the TSA functions within 48 (forty eight) hours.

5. PROCEDURAL SECURITY CONTROLS

5.1.1 Staff roles

The TSA staff roles that may be assumed by one or several persons shall be as follows:

a) **security officer**. He shall initiate installation and management of the TSA hardware (including computer network) and software; initiate and terminate the TSA services; guide other administrators by initiating generation of keys and other confidential data; entitle the TSA staff in terms of security and assign to them privileges of access to the system; provide the initial passwords to users; preview the Event Logs; supervise the service provision; supervise the procedures for internal and external audit; accept audit protocols and prepare answers thereto; supervise elimination of deficiencies found during audit;

b) **TSA administrator.** He shall supervise work of the TSA operators; install the equipment in use; establish the system and network parameters; undertake the network security measures and set the security parameters; create the TSA user accounts; preview the system logs; make back-up copies to eliminate failure; change the server names and addresses; create and update the repository catalogues; create WWW page of the repository and administer interfaces;

c) **TSA operator.** He shall be responsible for day-to-day procedures for creation and management of time-stamp tokens; prepare, on a regular basis, back-up copies of data and keep archive of databases and logged events; manage databases; but he shall not have physical access to other system resources;

d) **TSA auditor.** He shall be responsible for preview of the Event Logs, performance of internal audit, and compliance with the TSPS.

Appointment of the above-mentioned roles shall preclude from any abusive usage of the TSA system. Each system user shall be authorised to perform actions that are appropriate only for his role (see *Scheme 2*).

	Security officer	CA administrator	CA operator	CA auditor
Security officer		X	X	X
CA administrator	X		X	X
CA operator	X	X		X
CA auditor	X	X	X	

Scheme 2. Role exclusion matrix (X – role is not possible).

5.1.2 Role identification and authentication

Roles of the TSA staff shall be identified and authenticated in the following cases:

a) when making a list of persons who are authorised to access the TSA premises;

b) when making a list of persons who are authorised to physically access the TSA system and network resources;

c) when allocating user accounts and passwords in the TSA information system.

Each verification or appointment:

a) shall be unique and exclusively bound with a particular person;

b) may not be shared with any other persons;

c) shall include limited functions (arising from roles of a particular person) related only to the TSA system software, operation system and control measures.

The TSA operations that may be performed with shared network resources shall be protected by strict measures of authenticity verification and encryption of information being sent.

6. STAFF RELIABILITY CONTROL

Persons shall be employed in accordance with the requirements of the Labour Code of the Republic of Lithuania. Employment shall be recorded in an employment contract. The Rules of Procedure (Chapter III, p. 26) shall set out the general requirements for the qualification of employees:

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).

In addition to the afore-mentioned general requirements, it shall be ensured that the persons fulfilling the duties assigned by the CA:

e) and involved in the creation and management of certificates have higher education;

f) have signed an agreement on performance of duties and responsibilities;

g) have received internal training in relation to fulfilment of the duties assigned to them;

h) have received training in relation to protection of personal data and confidential information, have familiarised themselves with the security documents and have signed a pledge of non-disclosure of confidential information, that they have familiarised themselves with the security documents.

6.1.1 Background checking procedure

Following the common procedure prescribed in clause 30 of Chapter III of the Rules of Procedure, the persons being employed must provide the following documents:

a) a personal identity document;

b) a state social insurance certificate;

c) a certificate regarding (the absence of) a criminal record[1];

d) documents confirming education, professional training;

[1] 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

e) a curriculum vitae;

f) a medical certificate issued after the mandatory health check-up;

g) a disability certificate (if any);

h) a birth certificate(s) of a child (children);

i) a marriage or divorce certificate.

In additional to the afore-mentioned general documents on the basis of which the employee's personal file is kept and stored, the employee must confirm that he/she has not been convicted. The afore-mentioned document shall also be stored in the employee's personal file.

6.1.2 Training requirements

The TSA executive staff shall have completed trainings and been familiarized with:

a) the TSP and TSPS requirements;

b) the TSA security requirements and procedures for checking compliance to these procedures;

c) liability for shutdowns of operations performed by the system;

d) possible shutdowns of the system operations and breaches of the TSA practices.

Participants who completed the training shall sign the documents that they have been familiarized with the TSP and TSPS, and also agree with the requirements raised for them and the established roles.

6.1.3 Requirements for the contracted persons

Contracted persons performing tasks on the contractual basis (providers of external services, software developers, etc.) shall be checked following the same procedures as applied for the TSA staff. In addition, the contracted persons performing tasks in the TSA premises must be accompanied by the TSA staff member.

6.1.4 Documentations supplied to staff

The TSA shall ensure that its staff have access to the following documents:

a) the TSP and TSPS.

7. PROFILES ON THE TSA CERTIFICATE AND CRL

The certificates created by the RCSC shall comply with the requirements of ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles" standard.

7.1. Profile of the Root CA Certificate

X.509 V1 main fields	Critical	Attribute	Description
Version			*V3*
Serial number			*Automatically created by the root CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras- i.k. 124110246* *C = LT*
Valid from			*Issue date*
Valid to			*Issue date + 27 years*
Subject			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras- i.k. 124110246* *C = LT*
Public key			*RSA (4096 Bits)*
X.509 V3 Extensions			
Subject Key Identifier	No		*the 160 bit hash value of RCSC RootCA public key*
CA Version	No		*V0.0*
Key Usage	Yes		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*
Basic Constraints	Yes		*Subject Type=CA* *Path Length Constraint=None*

7.2. Profile of the Issuing CA Certificate

X.509 V1 main fields	Critical	Attribute	Description
Version			*V3*
Serial number			*Automatically created by policy CA*
Signature algorithm			*sha256RSA*
Issuer			*CN = RCSC RootCA* *OU = RCSC* *O = VI Registru centras- i.k. 124110246* *C = LT*
Valid from			*Issue date*
Valid to			*Issue date +9 years*
Subject			*CN = RCSC IssuingCA* *OU = RCSC* *O = VI Registru centras- i.k. 124110246* *C = LT*

Public key			*RSA (2048 Bits)*
X.509 V3 extensions			
Subject Key Identifier	No	Key Identifier	*the 160 bit hash value of RCSC IssuingCA public key*
CA Version	No		*V0.0*
Certificate Policies	No	Policy Identifier	*2.5.29.32.0*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Certificate Template Name	No		*System template identifier*
Authority Key Identifier	No	Key Identifier	*the 160 bit hash value of RCSC RootCA public key*
CRL Distribution Points	No	Distribution Point Name	*http://csp2.rcsc.lt/cdp/RCSC_RootCA.crl*
Authority Information Access	No	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*https://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_RootCA.crt*
Basic Constraints	Yes		*Subject Type=CA* *Path Length Constraint=None*
Key Usage	Yes		*Certificate Signing, Off-line CRL Signing, CRL Signing (06)*

7.3. Profile of the TSA Certificate

X.509 V1 main fields	**Critical**	**Attribute**	**Description**
Version			*V3*
Serial number			*Automatically created by the policy CA*
Signature algorithm			*Sha256RSA*
Issuer			*CN = VI Registru Centras RCSC (PolicyCA)* *OU = Registru Centro Sertifikavimo Centras* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Valid from			*Issue date*
Valid to			*Issue date +7 years*
Subject			*CN = VI Registru Centras RCSC (TSA)* *OU = Registru Centro Sertifikavimo Centras (may be supplemented by serial number of the TSU device)* *O = VI Registru Centras - I.k. 124110246* *C = LT*
Public key			*RSA (2048 Bits) or RSA (3072 Bits)*
X.509 V3 extensions			
Subject Key Identifier	No	Key Identifier	*Hash of the TSA public key (SHA1)*
Certificate Policies	No	Policy Identifier	*1.3.6.1.4.1.30903.1.1.7. or* *1.3.6.1.4.1.30903.1.4.2.*

		Policy Qualifier Id=User Notice	*No value.*
		Policy Qualifier Id=CPS	*http://www.rcsc.lt/repository*
Authority Key Identifier	No	Key Identifier	*Hash of the policy CA public key (SHA1)*
CRL Distribution Points	No	Distribution Point Name	*URL= http://csp2.rcsc.lt/cdp/RCSC_IssuingCA.crl*
Authority Information Access	No	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	*http://ocsp2.rcsc.lt/ocspresponder.rcsc*
		Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	*http://csp2.rcsc.lt/aia/RCSC_IssuingCA.crt*
Extended Key Usage	No		*Time Stamping (1.3.6.1.5.5.7.3.8)*
Key Usage	Yes		*Digital Signature, Non-Repudiation (c0)*
Properties			
Thumbprint algorithm			*sha1*
Thumbprint			*Summary of the TSA certificate*

8. ADMINISTRATION OF THE TSPS

This chapter provides for the requirements on the TSPS administration.

A new version of the TSPS shall invalidate the previous version of the TSPS. A new version shall be valid as of the date indicated on the cover page of the TSPS. The latest version of the TSPS shall be published in the repository on the Internet.

Users of time-stamp tokens shall follow the latest version of the TSPS, the OID of which is specified in the electronic time-stamp.

8.1. Procedures for Amending the TSPS

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

Amendments to the TSPS shall fall into two categories:

a) substantial changes when users must be informed thereof and the TSPS OID must be amended;
b) insignificant changes when it is not mandatory for the RCSC to inform other parties thereof, and the TSPS OID is not changed.

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

Insignificant changes in the TSPS 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 TSPS have changed.

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

The TSPS shall be monitored, amended and approved under the procedure as follows:

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

b) the TSA or users of time-stamp tokens shall initiate the TSPS changes;

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

d) in case of substantial changes, a draft version of new TSPS shall be published in the repository on the Internet 30 (thirty) days prior to the approval of the TSPS, in order to receive comments of the related parties. Having considered the comments received within 30 (thirty) days, or not having received any comments within 30 (thirty) days, a new version shall be approved. In case of insignificant comments, a new version shall be submitted for approval immediately after being drafted;

e) the RCSC work group on security policy shall adopt the decision regarding submission of a new TSPS version for approval; in case of substantial changes, a new OID shall be assigned;

f) the Director General of the Centre of Registers shall approve a new version of the TSPS;

g) the approved new version of the TSPS shall be placed in the repository.

8.2. Publication and Notification Procedures

The TSA shall not publish information that might affect security of the system in use. Information shall be accessible solely to the security officer, TSA administrator and controlling institutions. Documents of this type may be familiarized with only in special premises. Each access to the confidential documents shall be recorded.

The TSA shall keep all its versions of the TSPS and, upon request, provide them to the interested parties.

A valid version of the TSPS and TSP implemented by the TSA shall be made publicly available in the repository on the Internet.

Following point (a) of Article 24(2) of eIDAS, the TSA shall in all cases inform the trust service supervisory body of any change in its operations.

9. DEFINITIONS AND ABBREVIATIONS

Activation data means the data (e.g., PIN code, password, etc.) that must be entered in order to use cryptographic module and private key. Activation data, like private key, must be stored and not disclosed.

Authentication means the process of determining authenticity of whether a person is who he claims to be, or whether an object is the original one.

Certificate means an electronic certificate, which associates public key (signature verification data) with the signatory and verifies or enables to determine identity of the signatory.

Certificate/ Seal Revocation List (**CRL**) means a list of certificates/ seals that have been suspended or revoked, which is periodically (or immediately) issued and signed by the certification centre. Such a list usually contains the name of the certification centre 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/ seals, time and reasons of revocation or suspension.

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).

Public key means unique data, which are used for verification of electronic signature (signature verification data).

Public Key Infrastructure (**PKI**) means structure, organisation, methods and procedures of the cryptographic system of public keys based on certificates.

Qualified certificate means a certificate created by the certification centre complying with the requirements established by the Government of the Republic of Lithuania or its authorised institution.

Relying parties – *see* users of time-stamp tokens.

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

RSA means the cryptographic system of public keys conceived by scientists Rivest, Shamir and Adleman.

Security policy means a document of the highest importance defining secure operation policy of the certification centre.

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

Time-Stamping Authority (TSA) means a 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. The time-stamp token of electronic signature is a proof that the signature has been created 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.

BIPM – Bureau International des Poids et Mesures (*International Bureau of Weights and Measures*)

CA – Certification Authority

CP – Qualified Certificate/ Seal Policy

CPS – Certification Practice Statement

CRL – Certificate/ Seal Revocation List

CWA – CEN Workgroup Agreement

ETSI – European Telecommunication Standardisation Institute

FIPS – Federal Information Processing Standards

IDS – Intrusion Detection System

LAN – Local Area Network

LST – Lithuanian Standards Board

NTP – Network Time Protocol

OCSP – Online Certificate/ Seal Status Protocol

OID – Object Identifier

PIN – Personal Identification Number

PKI – Public Key Infrastructure

RA – Registration Authority

RCSC – Certification Centre of the Centre of Registers

RSA – Rivest-Shamir-Adleman algorithm

TSA – Time-Stamping Authority

TSP – Time-Stamping Policy

TSPS – Time-Stamping Practice Statement

UPS – Uninterrupted Power Supply

UTC – Coordinated Universal Time

10. SOURCES

[1]	ETSI EN 319 421 v1.1.1	Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
[2]	ETSI EN 319 422 v1.1.1	Time-stamping protocol and electronic time-stamp profiles http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
[3]	ETSI TR 119 300 v1.2.1	Business guidance on cryptographic suites http://www.etsi.org/deliver/etsi_tr/119300_119399/119300/01.02.01_60/tr_119300v010201p.pdf
[4]	ETSI TS 119 312 v1.1.1	Cryptographic Suites http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf
[5]	CWA 14168	Secure Signature-Creation Devices, version 'EAL 4'. http://www.uninfo.polito.it/WS_Esign/docs.htm#published
[6]	ISO/IEC 19790:2006	Information Technology – Security Techniques – Security Requirements for Cryptographic Modules.
[7]	FIPS PUB 140-2	Security Requirements for Cryptographic Modules. http://www.nist.gov/cmvp
[8]	FIPS 112	Password Usage. http://csrs.nist.gov/fips/
[9]	ITU-T	Recommendation X.509 – Information Technology – Open System Interconnection – The Directory: Authentication Framework, June 1997 (equivalent ISO/IEC9594-8).
[10]	VeriSign CPS	VeriSign Certification Practice Statement. http://www.verisign.com
[11]	Unizeto CERTUM	General Certification Authority – Certification Practice Statement. http://www.certum.eu/certum/cert,docs_certification practise_statement.xml
[12]	LST ISO/IEC 15408:1999(E) Information technology	Security techniques – Evaluation criteria for IT security.