STATE ENTERPRISE CENTRE OF REGISTERS

QUALIFIED CERTIFICATE/ SEAL POLICY OF THE CERTIFICATION CENTRE OF THE CENTRE OF REGISTERS

Unique Object ID (OID): **1.3.6.1.4.1.30903.1.1.5**
Version: 5.0
Valid from: 28 April 2017

28 April 2017

TABLE OF CONTENTS

History of amendments to the Certificate Policy:

Version	Date	Status
0.1	17 April 2008	Project
1.0	15 July 2008	First version
2.0	5 March 2009	Second version
3.0	24 November 2010	Third version
4.0	25 January 2017	Fourth version
5.0	28 April 2017	Fifth version

Document approval:

Document preparation	Name	Date	Signature
Document approved by	Arvydas Bagdonavičius, Acting Director General	28 April 2017	

1. INTRODUCTION

The State Enterprise Centre of Registers (hereinafter – Centre of Registers) was established in 1997. The founder of the enterprise is the Government of the Republic of Lithuania. The institution exercising 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 mentioned and other registers, keeps register archives.

To execute the assigned functions efficiently, the Centre of Registers applies modern information technologies and provides certificate/seal creation and management services, pursuant to the Requirements for Certification Service Providers Creating Qualified Certificates approved by the up-to-date version of Resolution No 2108 of the Government of the Republic of Lithuania as of 31 December 2002 "On the Approval of the Requirements for Certification Service Providers Creating Qualified Certificates, Requirements for Electronic Signature Equipment, Procedure for Registration of Certification Service Providers Creating Qualified Certificates, and Regulations on Electronic Signature Supervision".

1.1. Overview

Qualified Certificate/Seal Policy (hereinafter – CP) means a set of rules determining whether certificates/seals issued by the Certification Authority (hereinafter – CA) are suitable for particular user groups and application areas with common security requirements. The present document aims at enhancing confidence in the CA-created certificates/seals meeting the requirements of this policy. The CP shall establish rights and obligations of the certification service provider and certificate/seal users.

The CP requirements may be applied to all certificates created and managed under the current policy, regardless of whether these certificates are qualified or not.

Requirements identified in the CP shall not be tailored to any particular technological decisions or the CA organisational structure. Technical decisions, procedures and staff policy implementing the CP requirements shall be specified in the Certification Practice Statement (hereinafter – CPS) of the Certification Centre of the Centre of Registers (hereinafter – RCSC).

The CP is defined on the basis of the following documents:

a) The up-to-date version of Resolution No 2108 of the Government of the Republic of Lithuania as of 31 December 2002 "On the Approval of the Requirements for Certification Service Providers Creating Qualified Certificates, Requirements for Electronic Signature Equipment, Procedure for Registration of Certification Service Providers Creating Qualified Certificates, and Regulations on Electronic Signature Supervision";

b) The up-to-date version of the Law on Electronic Signature of the Republic of Lithuania;

c) The up-to-date 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;

d) The up-to-date version of the Law on Legal Protection of Personal Data of the Republic of Lithuania;

e) ETSI EN 319 403 v2.2.2: Requirements for conformity assessment bodies assessing Trust Service Providers;

f) ETSI EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;

g) ETSI EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates;

h) ETSI EN 319 412 Certificate Profiles;

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

j) ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles;

k) ETSI TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation;

l) ETSI TS 119 101 v1.1.1 on Policy and security requirements for applications for signature creation and signature validation;

m) ETSI TR 119 300 v1.2.1 Business guidance on cryptographic suites;

n) ETSI TS 119 312 v1.1.1 Cryptographic Suites;

o) ETSI TR 119 600 v1.2.1 Business guidance for trust service status lists providers;

p) ETSI TS 119 612 v2.1.1 Trusted Lists;

q) ETSI EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles.

With reference to the certificate creation and management practices, the CA shall execute the following functions:

a) Registration;

b) Certificate/seal creation;

c) Issuance of certificates/seals and provision of information on the certificate/seal use, restrictions, terms and conditions;

d) Certificate/seal life-cycle management;

e) Provision of information on the certificate/seal status;

f) Preparation and provision of the SSCD.

1.2. Identification

The CP unique identifier (OID – Object Identifier) shall be as follows:

1.3.6.1.4.1.30903.1.1.5

The OID field meanings are indicated below (see *Table No 1*).

Table No 1. Field meanings of the CP unique identifier

Title	Meaning
ISO	1
ISO recognised organisation	3
US Defense 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 (Certificate Policy)	1
Document version	5

The latest CP version shall be published in the RCSC repository.

1.3. Certificate/Seal Users and Application Areas

In line with the current CP, the following certificates shall be created and managed:

a) Qualified certificates for generation of a qualified electronic signature (a secure electronic signature created with the secure signature creation device and verified by the valid qualified certificate) pursuant to the up-to-date version of the Law on Electronic Signature of the Republic of Lithuania, and other legal acts and standards specified in Chapter 1.1 of the CP;

b) Qualified seals serving the purpose of verification that electronic documents were issued by a legal person, ensuring certainty of the document's origin and integrity;

c) Other certificates, created and managed in line with the current CP as well as containing the OID of the current CP.

Certificate/seal users shall be as follows:

a) Subscribers;

b) Certificate/seal owners;

c) Parties relying on certificates/seals.

In line with the current CP, certificates shall not be issued to legal persons, i.e. only a natural person may be the owner of a certificate; however, a legal person may be the owner of a seal.

1.4. Organisational Structure

Functions of the Certification Service Provider (hereinafter – CSP) shall be executed by the Centre of Registers. The CSP shall provide certificate/seal creation and management services, time-stamping and other certification services. The certificate/seal creation and management services shall be provided by the CA.

According to the current CPS, the CA shall delegate a certain part of its functions pertaining to certificate/seal creation and management to the Authority supporting certification operations (hereinafter – Support Service) and Registration authorities (hereinafter – RA). The RA functions shall be executed by the branch offices of the Centre of Registers, or other third parties with whom the agreements on provision of the RA services have been concluded.

The CA shall remain responsible for all the certification services being provided and certification practices being implemented; however, the rights, obligations and liability of third parties shall in all cases be detailed in concluded agreements and in the CPS, CP.

1.5. Conformance

When recording the unique identifier, defined in Chapter 1.2, into the created certificates/seals, the CA shall attest that certificates/seals conform to the current CP. Thereby, the CA must assume all obligations, defined in Chapter 2.1, and meet the operational requirements laid down in Chapters 3-5.

1.6. Contact Details

The CP shall be administered by:

Person	Head of the Certification Centre of the State Enterprise Centre of Registers
Address	Vinco Kudirkos str. 18, LT-03105 Vilnius, Lithuania
Tel.	+370 5 2688 388
Fax	+370 5 2688 311
URL	http://www.registrucentras.lt
E-mail	*info@elektroninis.lt*

2. GENERAL PROVISIONS

This chapter specifies obligations of the CA and parties related to certificate/seal use, and contains the statements on legal and general operational issues.

2.1. Obligations

2.1.1 CA obligations

The CA must ensure that all requirements, which it is subject to, as specified in Chapters 3-5, are met.

The CA must ensure that operational procedures being followed comply with the CP requirements, even when execution of certain procedures or provision of certain services is transferred to the third parties.

The CA must provide certificate/seal creation and management services in line with its CPS.

When executing its functions, the CA shall undertake to:

a) Ensure that the CA private cryptographic keys (hereinafter – keys) are secure;

b) Ensure that information contained in the issued certificate/seal is true;

c) Ensure that a person whom a certificate/seal is being issued has been properly identified;

d) Ensure that applications to issue certificates/seals are properly collected and processed:

   - Ensure that applications to issue certificates/seals are collected and processed, as specified in the CP and CPS;
   - Ensure that the SSCD is prepared and presented to persons in a secure manner;

e) Provide the certificate/seal users with accurate and true information, which enables to:

   - Check the certificate/seal validity;
   - Draw attention upon the procedure and restrictions on the certificate/seal use;

f) Collect applications to revoke or suspend a certificate/seal:

   - Collect and process applications to revoke or suspend a certificate/seal, as specified in the CP and CPS;
   - Revoke a certificate/seal upon expiration of the certificate/seal suspension period;

g) Collect applications to withdraw the certificate/seal suspension:

- Collect and process applications to withdraw the certificate/seal suspension, as specified in the CP and CPS;

- Remove the certificates/seals, suspension thereof has been withdrawn, from the Certificate/Seal Revocation List (hereinafter – CRL).

h) Ensure personal data protection regulated by the up-to-date version of the Law on Legal Protection of Personal Data of the Republic of Lithuania implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

i) Use only the SSCD for generation and storage of cryptographic keys and storage of certificates/seals created for persons relating to these keys.

2.1.2 RA obligations

The Registration Authority shall undertake to:

a) Authenticate the identity of a person;

b) Collect applications to create certificates;

c) Collect applications to revoke certificates;

d) Collect applications to suspend certificates;

e) Collect applications to withdraw the certificate suspension;

f) Adhere to the agreement signed with the CA; in case the activity has been delegated, the RA shall assume overall responsibility for the operations performed by the third party.

The CA shall periodically, (every 1 (one) year or after significant amendments to the CP and the CPS), carry out inspections of the obligations and functions of the RA.

2.1.3 Obligations of the support service

The support service shall undertake to:

a) Collect, 7 (seven) days per week, 24 (twenty-four) hours per day, by telephone, applications to suspend a certificate/seal, and provide information related to the certification practices.

2.1.4 Obligations of the subscribers and certificate/seal owners

When applying procedures for persons' registration, the CA must ensure that persons are obligated to:

a) Submit accurate and complete information to the RA according to the CP and CPS requirements;

b) Authorise usage and storage of personal data, as specified in the CP and CPS;

Obligations of certificate/seal owners:

c) Use the pair of public and private keys only in accordance with the purpose of use indicated in the certificate/seal, following the restrictions detailed therein;

d) Exercise reasonable care to avoid any unauthorised use of their private key or disclosure of activation data to other persons;

e) Notify the CA immediately, but not later than within 12 (twelve) hours, if any of the following events occur prior to expiration of the certificate/seal validity period:

- Private key of a person has been lost, stolen or otherwise compromised;
- Control over the use of private key has been lost in the event of disclosure of activation data;
- Inaccuracies in the certificate/seal have been detected, or changes need to be made thereto;

f) If the private key has been compromised, urgently and completely cease its use.

2.1.5 Obligations of the relying parties

Persons relying on a certificate/seal must:

a) Assure that the CA is reliable;

b) Assure that the certificate/seal has been used in accordance with its purpose of use;

c) Assure that the certificate/seal is valid;

d) Undertake the procedure for checking the certificate/seal sequence;

e) Assure that the software used is capable to process all the certificate/seal information, including additional fields. Prior to making decision regarding the certificate/seal reliability level, the parties relying on a certificate/seal must get familiar with the CP and CPS. Relying

parties must use certificates/seals only in accordance with the purpose of use and be aware of the restricted areas of certificate/seal use.

2.2. Liability

The CA shall be liable for:

a) Accuracy of data in the created certificate/seal;

b) Corresponding of the signature creation data to the signature verification data;

c) The fact that a person indicated in the created certificate/seal is the holder of the signature creation data corresponding to the signature verification data indicated in the certificate/seal;

d) Timely revocation or suspension of the certificate/seal.

The CA shall assume liability for any loss incurred by the certificate/seal users and caused by the third parties (the RA), whom the CA delegated part of its functions. The CA shall also be liable for the quality and availability of the services being provided, but only within its operational limits, which shall include:

a) the infrastructure for creation and management of qualified certificates/seals that ends at the firewall of the Centre of Registers adjoining to the public Internet;

b) provision of the time-stamping service – the infrastructure required for provision of the TSA that ends at the TSA infrastructure external network interface.

The CA shall not be liable for any system faults or disturbances on the part of third parties (registered beyond the operational limits of the CA) that could possibly result in failures in the provision, quality and availability of the services being provided.

All terms and conditions, restrictions as well as rules relating to the use of certificates/seals shall be specified in a concluded agreement and in the publicly available CPS and CP. In that regard, the CA shall not be held liable for any illegal actions of the certificate/seal users and other parties that are not associated with the CA, as well as for any losses incurred by certificate/seal users when they have been duly informed in advance about the terms and conditions as well as restrictions on the use of certificates/seals and when the losses were caused as a result of their failure to comply with the above-mentioned terms and conditions as well as rules. Also, the CA shall not assume liability if the loss was incurred due to:

e) Natural forces, e.g., fire, flood, storm, or other circumstances, such as war, terrorist attack, epidemics or *force majeure* circumstances, which could not be controlled, foreseen or prevented in advance;

f) Unauthorised use of certificates/seals (e.g., when the certificate/seal is not valid or when the restrictions on the certificate/seal use, the rules provided for in the CPS, CP and the agreements signed have been breached).

2.3. Legal Provisions and Interpretation

Creation, verification, validity of electronic signature, rights and obligations of the signature users, certification services, including creation and management of qualified certificates/seals and requirements for service providers, and liability shall be collectively established by the up-to-date version of the Law on Electronic Signature of the Republic of Lithuania, the up-to-date 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, and other national legal acts as well as EU legislation. The CPS implementing the current CP shall specify the terms and conditions on certification service provision as well as liability cases.

2.4. Fees

The CA may charge fees for the certificate/seal creation and management services.

The CA shall not require any remuneration for:

a) Issue of the CRL;

b) Publication of the CP and CPS;

c) Certificate/seal revocation or suspension.

2.5. Information Provision and Repositories

The CA must maintain a repository, which shall be made available through public telecommunications networks, at all times without restrictions. The following information shall be published in the repository:

a) The latest versions of the CP and CPS;

b) The CRL;

c) Other up-to-date information related to certification practices.

The CA shall undertake to provide information about the certificate/seal status in the CRL. Beyond the CRL, the CA may provide the OCSP responder service.

Prior to entering into agreement, the CA must inform a person applying for certificate/seal creation about the terms and conditions on certificate/seal creation and management. The terms and conditions must contain the following information to be provided by the CA:

a) Authorised use of certificate/seal (use area, restrictions on use area, maximum permitted value of transaction and other);

b) Components and procedures for verifying electronic signature and validity period thereof;

c) Obligations of the certificate/seal owner;

d) CA obligations and liability.

The terms and conditions must contain the following information to be provided to the parties relying on certificates/seals:

a) Authorised use of certificate/seal (use area, restrictions on use area, maximum permitted value of transaction and other);

b) Components and procedures for verifying electronic signature and validity period thereof;

c) Obligations of the relying parties.

2.6. Confidentiality Provisions

a) The CA must protect the data of persons requesting certificate/seal creation in conformance with the Law on Legal Protection of Personal Data of the Republic of Lithuania implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Personal data shall be retained for an appropriate and necessary period (Chapter 4.3.2 of the CPS) (including when the CA ceases its operations), but for no longer than it is necessary for the purposes for which the data were processed, of which a person applying for certificate/seal creation shall be informed in order that the data can be used in court proceedings as well as to ensure the continuity of operations;

b) Personal data must be destroyed when they are no more needed for their processing purposes, with the exception of data which must be transferred to State archives in the cases laid down in laws;

c) In order to protect the aforementioned data against forgery or theft, the CA shall take preventive measures with regard to adequate and effective physical, technical, procedural security and staff reliability controls.

2.7. Intellectual Property Rights

The CP and its implementing CPS shall be made available for certificate/seal users. Whenever the current CP and CPS are used, a reference to their source must be given.

The CA shall not apply ownership rights to the created certificates/seals.

3. OPERATIONAL REQUIREMENTS

3.1. Practice Statement

The CA operational procedures, control mechanism and technical requirements for infrastructure are detailed in the CPS. The CA must show in the CPS that undertaken certification practices are reliable, i.e.:

a) The CA shall have detailed practice statements and procedures for implementation of the requirements indicated in the current CP;

b) Obligations of all external organisations, related to the certification practice, shall be described in detail;

c) The CPS and other related information shall be made publicly available, in such a way as to assess conformance of the certification practices to the CP;

d) The certificate/seals users shall be provided with all the information regarding restrictions as well as terms and conditions on certificate/seals use;

e) The CA shall define a review process for certification practices and shall establish responsibilities for supervision of the CPS;

f) The CA shall give notice (in due time and form) of changes it intends to make in its CPS and shall, following approval thereof as required under point e) above, make the revised CPS immediately available to the certificate/seals users and relying parties as required under point c) above.

The CA manager shall assume responsibility for conformance of the CA practices to the CPS.

3.2. Life Cycle of Cryptographic Keys

3.2.1 Generation of the CA cryptographic keys

The CA must ensure that the CA cryptographic keys are generated under controlled and secure conditions, the private key being kept secret. The CA must ensure that:

The CA key pairs shall be generated by special workstation connected with hardware security module (cryptographic module). Hardware security module shall meet the requirements of FIPS PUB 140-2 standard Security Level 3. Actions related to key pair generation shall be recorded, including the date of key pair generation, and shall be signed by all persons who participated in the generation process. The log files shall be kept because they might be used later for inspections.

All private keys of personal certificates/seals shall be generated using hardware; therefore keys are protected against copying or any other unauthorised use. Certificates/seals shall be created only for persons, using the SSCD Type 3 provided by the CA, security of which was rated 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.

3.2.2 Storage of the CA cryptographic keys

To ensure security of the CA private keys, due technical measures and procedures must be undertaken, which offer reliable protection against disclosure or unauthorised use of the private key and enable to maintain confidentiality and integrity of the private key.

Due technical measures and procedures must ensure that the private key is kept and used only within a device meeting the requirements.

Whenever the CA private keys are stored or kept outside the secure cryptographic device (hardware security module, hereinafter – HSM), they must be encrypted. The key length and algorithm used for encrypting must ensure that the CA private keys are secure and resistant to cryptographic attacks throughout the key life cycle.

Whenever the CA private keys are stored in the HSM, access controls must ensure that the keys are not accessible outside the HSM.

3.2.3 Backup and recovery of the CA private cryptographic keys

The CA 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 CA private key. At least 2 (two) out of minimum 4 (four) 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 CA private key, and this must be done in a physically secured environment.

3.2.4 Dissemination of the CA public cryptographic keys

The CA must make its public keys available to the relying parties. When disseminating its public keys, the CA must ensure integrity and authenticity of the public key and other related data.

3.2.5 CA key escrow to the third parties

The CA shall not have any possibilities to escrow private keys owned by the CA and certificate/seal owners to the third parties.

3.2.6 Usage of the CA private cryptographic keys

The CA must ensure that private keys belonging to the CA are properly used. The CA must ensure that:

a) The CA private keys, used for verifying the certificates/seals and CRLs of persons, are not used for any other purposes;

b) Private keys, used for verifying the CA certificates/seals, must be used under physically secured conditions.

3.2.7 End of life cycle of the CA cryptographic keys

The CA must ensure that the CA private keys are not used beyond the end of their life cycle. The established technical and management procedures must ensure that upon expiration of validity period of the CA keys, a new pair of keys is used, the previously used private keys being destroyed.

3.2.8 Life cycle of cryptographic device used for signing certificates/seals

The CA must ensure security of HSM throughout its life cycle.

The CA must ensure that:

a) HSM has not been tampered with prior to its delivery;

b) HSM is tamper-proof when used for implementation of the certification practices;

c) Cryptographic device, used for signing the certificates/seals, CRLs, OCSP messages and other important information, is functioning correctly;

d) Keys stored in HSM are destroyed upon retirement of this device.

3.2.9 Management of the CA cryptographic keys issued to persons

The CA must ensure that:

a) Pairs of keys are generated using algorithms meeting the requirements of qualified electronic signature;

b) Generated key length is fit for the purposes of qualified electronic signature;

c) Pairs of keys are generated using the SSCD type 3, security thereof being assessed to 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;

d) Any copies of the private key are not made.

3.2.10 Preparation and provision of the SSCD

The CA must ensure that the SSCD is prepared and passed to certificate/seal owners in a secure manner. The CA must ensure that:

a) SSCD preparation is securely controlled and performed;

b) SSCD is securely stored and passed;

c) SSCD activation and deactivation is securely controlled and performed.

The CA shall apply the following measures to ensure the security of the processes of preparation and transfer of the SSCD to the user:

a) issue only the SSCD which complies with the FIPS 140-2 standard of SSCD type 3, or the SSCD the security of which meets the requirements of either CWA 14167-3 or CWA 14167-4 standard or its Evaluation Assurance Level is 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;

b) before the SSCD is assigned to a person or the certificate/seal generation is initiated, the SSCD shall be safely stored in accordance with all the instructions of the SSCD manufacturer;

c) after SSCD is assigned to a person or the SSCD public key certificate/seal is generated, the private key activation data (PIN) shall be protected (either by placing it in a protective envelope or covering it with a protective layer of paint), thus ensuring that the cases of unauthorised viewing of the activation data are found before or during the transfer of the SSCD to a person;

d) at the time of issuing the SSCD, shall carry out the procedure for identification of the person, record the exact date and time (to the nearest minute) of the transfer of the SSCD;

e) the SSCD shall be issued only to a person physically present in the RA; the SSCD shall not be sent or transferred to the user through any other channels.

3.3. Certificate/Seal Management Cycle

3.3.1 Persons' registration

The CA must ensure that persons applying for certificate/seal issuance are properly identified, and the submitted applications are lawful, complete and valid.

The RA must:

a) Prior to concluding an agreement on the provision of certification services, inform a person applying for certificate/seal creation about the terms and conditions, restrictions on certificate/seal creation and management, obligations and liability of the CA, the subscriber and the certificate/seal owner;

b) Communicate this information in a form that is durable, i.e. with integrity over time;

c) Require that, in order to prove their identity, **natural** persons applying for creation of certificates submit:

- a passport;
- an ID card;
- a residence permit.

Require that representatives of **legal** persons applying for creation of electronic seals submit:

- the head of a legal entity – a personal identity document;
- another representative of a legal entity – a personal identity document and the original of the power of attorney to represent the legal entity.

d) According to the national legal acts, make sure of the identity of persons applying for certificate/seal creation;

e) Require that persons applying for certificate/seal creation provide the contact details, which can be relied upon when contacting them;

f) Document and store all the information used to identify a person, including the document type, number and restrictions on the document validity;

g) Document and retain the concluded agreement covering:

- Obligations of the certificate/seal owner;
- Terms and conditions on publication of personal data, the certificate/seal and separate data of the certificate/seal;
- Consent to store information on the registration of the certificate/seal owner, SSCD delivery and other information, and consent to transfer this information to the third parties following the procedures specified in the CP and CPS, in the event of termination of the CA practices;

- Confirmation that information provided by the certificate/seal owner is true;

h) Store the collected data specified under points c)-g) for the period indicated in the agreement; prior to signing the agreement, the certificate/seal owner shall be informed about this period, which is necessary for presentation of evidentiary material of the certification practices for judicial proceedings;

i) Undertake to protect personal data following the Law on Legal Protection of Personal Data of the Republic of Lithuania.

3.3.2 Certificate/seal updating

Any updating of certificates/seals, rekey without changing the certificate/seal, and change of the certificate/seal information shall not be applicable under the current CP. A new certificate/seal shall be issued whenever the personal data contained in the certificate/seal have changed, or under other circumstances, which are precisely defined in the CPS.

3.3.3 Certificate/seal creation

The CA must ensure that certificates/seals are created in a secure manner, so that authentic certificates/seals could be maintained.

The certificate/seal creation process and created certificates/seals must meet the following requirements:

a) The procedure for certificate/seal creation must be securely linked to other related procedures of certificate life cycle;

b) The procedure for generation of the personal key pair must be as follows:

- Securely linked to the procedure for certificate/seal creation;
- The private key must be generated within the SSCD;
- The SSCD must be securely passed to the certificate/seal owner.

c) The identification data specified in the created certificate/seal must be unique within the domain of all certificates/seals created by the CA and not assigned to any other person;

d) Confidentiality and integrity of the certificate/seal creation data must be ensured throughout the certificate/seal life cycle;

e) The CA must ensure that data exchange with external registration authorities is secure, and registration authorities are reliable.

The qualified certificates/seals created must meet the requirements for qualified certificates used for the purposes of electronic signature, as stipulated in the latest version of the Law on Electronic Signature of the Republic of Lithuania.

3.3.4 Provision of information regarding the terms and conditions on certificate/seal creation and management

The CA must ensure that certificate/seal users are informed of the terms and conditions on certificate/seal creation and management. The CA must:

a) Clearly indicate the applicable CP;

b) Inform of the restrictions on certificate/seal use;

c) Inform of the obligations of certificate/seal users;

d) Provide information on how to check the certificate/seal validity;

e) Inform of the CA liability and restrictions thereof;

f) Inform of the period of time, during which registration information is stored;

g) Inform of the period of time, during which data on the CA operations are stored;

h) Inform of the procedures for dispute settlement;

i) Inform of the applicable laws related to the practices.

All the above-mentioned information must be provided in a form acceptable for everyone, in a clear and understandable manner.

3.3.5 Certificate/seal issuance

The CA must ensure that:

a) Upon creation, the complete and accurate certificate/seal is passed to the certificate/seal owner;

b) The terms and conditions on certificate/seal creation and management are made available to the certificate/seal users and can be readily identifiable for a given certificate/seal;

c) Information identified in point b) above is available 24 (twenty four) hours per day, 7 (seven) days per week. In cases of operational shutdowns, the CA shall make best endeavours to recover the operation.

Dissemination of lists of certificates/seals issued by the CA as well as search for certificates/seals shall not be applicable in the certification practices.

3.3.6 Certificate/seal revocation and suspension

The CA shall ensure that a certificate/seal is revoked not later than within 8 (eight) working hours following the receipt of an application. The received application shall, in all cases, be registered in the database on certificates/seals and the revocation status of the certificate/seal shall be published no later than within 24 (twenty-four) hours after the receipt of the request. A certificate/seal shall lose its validity from the moment of its revocation and the revocation shall become effective immediately upon its publication. The validity status of the revoked certificate/seal shall not in any circumstances be reverted.

When issuing a certificate/seal, the CA must inform the certificate/seal owner of the methods and communication means that enable to revoke or suspend a certificate/seal.

The CA shall revoke a certificate/seal in the following cases:

a) Upon request of the certificate/seal owner;

b) When the certificate/seal data are known to be no longer true;

c) When the certificate/seal is known to have been created on the basis of inaccurate data;

d) When the CA issuing a certificate/seal ceases its operations and any other CA does not take over the certification practices;

e) When the certificate/seal owner does not follow the terms and conditions on the certificate/seal use;

f) When the control over the signature creation or activation data corresponding to the certificate/seal has been lost;

g) On the basis of the restrictions on certificate/seal validity, as specified in the certificate/seal during creation;

h) Upon receipt of notification that the certificate/seal owner has become legally incapable;

i) Upon receipt of notification that the certificate/seal owner died;

Pursuant to the national legislation, a certificate/seal shall be suspended within 4 (four) working hours following the receipt of an application. Suspension of a certificate/seal shall, in all cases, be indicated in the database on certificates/seals and information on the suspension status shall be available in the course of providing information on the status of the certificate/seal. A certificate/seal, which has been suspended, shall lose its validity for the period of suspension.

The CA shall suspend a certificate/seal in the following cases:

a) Upon request of the certificate/seal owner;

b) Upon requirement of law enforcement institutions, with the aim of preventing offences;

c) Upon receipt of information that the certificate/seal data are not true or the certificate/seal owner has lost control over the signature creation or activation data corresponding to the certificate/seal.

The CA, seeking to ensure timely revocation and suspension of a certificate/seal, on the basis of verified and lawful application, must ensure that:

a) The CPS specifies the procedures for certificate/seal revocation and suspension, and contains the following information:

   - In what cases and under what circumstances a certificate/seal must be revoked and suspended;
   - Who may submit an application to revoke or suspend a certificate/seal;
   - How an application may be submitted;
   - Any requirements for confirmation of an application to revoke or suspend a certificate/seal;
   - What mechanism is used for distributing of information on certificates/seals that have been suspended or revoked;

b) The maximum period of time between receipt of an application to revoke and suspend a certificate/seal and distribution of information on the change to the certificate/seal status is at most 1 (one) working day;

c) Applications to revoke and suspend a certificate/seal are processed immediately upon receipt;

d) Applications to revoke and suspend a certificate/seal are checked to be true and lawful, and this is confirmed as required under the CPS implementing the current CP;

e) The support service is available at any time. Upon failures in the support service availability, which are independent of the CA operation, the CA must make best endeavours to ensure that the service unavailability period is no longer than specified in the CPS implementing the current CP;

f) Prior to confirming the certificate/seal revocation, the suspension status may be set to the certificate/seal; however, duration of such a status should not exceed the period required for confirmation of the certificate/seal status;

g) Where a certificate/seal has been suspended or revoked without request of the certificate/seal owner, the certificate/seal owner must be informed accordingly.

Any certificate/seal shall not be revoked and suspended by the retroactive date or time. The certificate/seal revocation shall not be withdrawn.

3.3.7 Checking of the certificate/seal validity

The CA must ensure that its created certificates/seals are available:

a) Upon certificate/seal creation, the complete and accurate certificate must be made available for the certificate/seal users. The CA shall provide information on the certificate/seal status in the following manner:

   - In CRL, which shall be updated at least once every 24 (twenty four) hours. The CRL must be signed by the CA electronic signature, and each CRL must state a time for next CRL issue; or (and)

   - By the OCSP responder indicating the certificate/seal status in real time;

b) The above-mentioned information must be available 24 (twenty four) hours per day, 7 (seven) days per week. Upon failures in the availability, which are independent of the CA operation, the CA must make best endeavours to ensure that the unavailability period is no longer than specified in the CPS implementing the current CP;

c) The CA must ensure integrity and authenticity of information on the certificate/seal status;

d) The above-mentioned information must be publicly and internationally available.

3.4. CA Management and Operation

3.4.1 Security management

The CA must ensure that during certification practices, security management and administration procedures are applied, which are recognised and correspond to the standards.

The CA must:

a) Assume overall responsibility for undertaken certification practices, even if some functions are transferred to the third parties. The CA must clearly define the liability and obligations of the third parties and ensure compliance to the required operational and security procedures;

b) Have the security management group that would define the security policy and disseminate it to the CA employees;

c) Maintain permanent protection of information managed by the CA; any change to the information security policy must be agreed with the CA security management group;

d) Ensure that security controls and procedures, pertaining to the CA devices, systems and information, are defined, followed and documented.

3.4.2 Asset inventory and management

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

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

3.4.3 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. The Rules of Procedure of the State Enterprise Centre of Registers (paragraph 26 of Section III) set 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 working with computers and using other office equipment;

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

In addition to the above-mentioned general requirements, it shall be ensured that persons filling roles assigned to them by the CA:

a) Those who perform creation and management of the certificates must have higher education;

b) Have signed the agreement regarding implementation of responsibilities and liability;

c) Have completed internal training related to implementation of responsibilities assigned to them;

d) Have completed training related to protection of personal data and confidential information, have familiarised themselves with security documents and have signed a pledge to protect the confidentiality of information certifying that they have familiarised themselves with the security documents.

3.4.4 Background checking procedure

Pursuant to the general procedure established in paragraph 26 of Section III of the Rules of Procedure of the State Enterprise Centre of Registers, a person being employed must present the following:

a) a personal identity document;

b) a state social insurance certificate;

c) documents confirming education, professional training;

d) a curriculum vitae (CV);

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

f) a disability certificate, if any;

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

h) a marriage or divorce certificate.

In addition to the above-mentioned general documents, 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. This document shall also be retained in the employee's personal file.

3.4.5 Training requirements

The CA staff must have completed trainings and been familiarized with:

a) CP and CPS;

b) RA procedures;

c) CA and RA security requirements and procedures for checking compliance to these procedures;

d) Software of the CA and RA systems;

e) Liability for shutdowns of operations performed by the system;

f) Possible shutdowns of the system operations.

3.4.6 Physical security control

The CA must ensure physical security of vulnerable elements of the CA system and minimise the risk of physical destruction of the assets used for certification services.

The CA must ensure that:

General requirements

a) Physical access to the premises, wherein certificates/seals are created, the SSCD is provided, certificates are revoked or suspended, is restricted and allowed only to the authorised persons;

b) The implemented measures enable to avoid asset loss, damage or compromise and interruption of operations;

c) The implemented measures enable to avoid compromise or theft of information or information processing devices;

Management of physical security of procedures related to the certificate/seal generation, provision of the SSCD, revocation and suspension of certificates:

a) Operational devices related to the creation of certificates/seals, provision of the SSCD as well as revocation and suspension of certificates/seals are used in a physically secured environment and are protected against compromise and illegal access to the system or data;

b) Physical security has been attained by establishing secure zones for the creation of certificates/seals, provision of the SSCD as well as revocation and suspension of certificates/seals. Any premises used for general operations of the CA and other units should be outside these zones;

c) Physical and other security measures have been implemented, which safeguard the premises, certification service provision system and other service provision resources against natural disasters, fire, power supply interruptions, shutdowns of communications networks.

3.4.7 Procedural security control

The CA must ensure secure and proper operation of the system providing certification services as well as the minimum risk of shutdowns.

The CA must ensure that:

a) Integrity of the CA hardware, software and information possessed is protected against computer viruses and other software vulnerability;

b) Procedures of notifications of violations and response to the arising threats have been clearly defined; they should be implemented in such a way as to minimise the damage;

c) Information drives and carriers used in the CA systems are protected against breakdowns, thefts, unauthorised access or wear; also the information is protected with regard to the established security level (Chapter 3.4.2);

d) Procedures for all roles related to the certificate/seal creation and management have been established;

e) Regular monitoring of the system status is performed in order to forecast the development of the system or increase of capacities in due time;

f) The CA security procedures have been separated from other procedures. The security procedures shall include: the establishment of operational procedures and responsibilities, secure planning of the system development, protection against damaging applications, supervision of premises, administration of network, active monitoring of audit journal, analysis of events, management and security of information carriers, exchange of data and software. These operations must be managed by the staff holding exclusive trust roles; however they may be also performed by the lower-qualification staff, if this was described in the security policy or other documents.

3.4.8 Management of access to the systems

The CA must ensure access to the CA systems only for the properly authorised staff.

The CA must ensure:

General requirements:

a) Inaccessibility of the CA Intranet through the Internet;

b) Protection of the important data when they are transferred through unsafe networks;

c) Administration of user access to the system, maintenance of security through the management of user registration data;

d) Restriction of access to the system data and functions in conformity with the Access Control Rules. Exclusive trust roles must be distinguished by separating system administration and operational functions;

e) Identification and authentication of the staff prior to the performance of critical procedures related to the management of certificates/seals;

f) Recording of the staff actions with the CA systems, for example recording and storing logs to the system;

Requirements for the certificate/seal generation:

a) Physical protection of local computer network components and regular audit of their configuration;

b) Implementation of regular observation and signalisation system enabling to detect, register and respond timely to the attempts to access the system resources;

Requirements for the certificate/seal issuance:

a) Control of the certificate/seal issuance system in case of attempt to add, remove or change certificates/seals and other related information;

Requirements for revocation and suspension:

a) Implementation of regular observation and signalisation system enabling to detect, register and respond timely to the attempts to change the certificate/seal status;

Requirements for provision of information on the certificate/seal status:

a) Control of the system for provision of information on the certificate/seal status in case of attempt to add, remove or change the certificate/seal status and other related information and timely response to such event.

3.4.9 Development and maintenance of reliable systems

When implementing any system development project, the analysis of security requirements shall be done in the designing and needs specification phase. The CA must ensure the implementation of security management measures in every IT system related with the certification practice.

The procedures for managing changes related to software modification or improvement must be established.

3.4.10 Management of shutdowns and continuity

The CA must ensure that in case of shutdowns, including compromise of the CA private key used for signing certificates/seals, all possible measures shall be undertaken to restore operations of the CA as soon as possible.

The CA must draw up an operation continuity plan specifying the actions related to recovery and continuity of operations, if the private key has been, or is suspected to be, compromised.

The following urgent actions shall be completed as a minimum:

a) Notification of all certificate/seal users, the relying parties and other persons whom agreements were entered with, or who in any other way are related to the operations of the CA;

b) Information on possible declaration as invalid of the created certificates/seals and the CRLs signed with a compromised private key.

3.4.11 Termination/transfer of certification services

In case the CA ceases its operations, any inconveniences for the certificate/seal users must be minimised, and continuity of the collected certification practice data, as evidentiary materials for judicial proceedings, must be ensured.

The CA, prior to ceasing operations on the certification service provision, shall undertake to:

c) Inform accordingly all the persons, whom it created certificates/seals and whose certificates/seals are valid, and other certification service providers with whom surety agreements have been concluded, as well as the Electronic Signature Supervision Institution not later than 1 (one) month in advance;

d) Revoke all of its created certificates/seals, if any other certification service provider does not take over its practices, not later than 1 (one) month from the date of announcement of the intended termination of the certification service provision;

e) Draft an agreement with another certification service provider, and if the latter has not been found – with the Electronic Signature Supervision Institution regarding taking over, storage and provision of the collected data to the relying parties;

f) Revoke the authorisations of third parties to act on behalf of the CA in providing the certification services.

3.4.12 Storage of records and archiving

The CA must store records on all operations related to the certificates/seals issued with the aim of having evidentiary materials of proper certification practice for judicial proceedings. Facts and circumstances of incidents and specific operational events must be documented and archived.

The documentation form must enable checking of the data, authenticity of the data and recording date at any time.

The data must be stored for the period of time provided for in the CPS; they must be available and protected against loss and damage. The CA must:

General requirements:

a) Ensure confidentiality and integrity of current and archival records on certificates/seals;

b) Ensure that records related to certificates/seals are archived and stored pursuant to the latest version of the Law on Documents and Archives of the Republic of Lithuania;

c) Present current and archival records about certificates/seals as evidentiary materials of proper certification practice for judicial proceedings;

d) Ensure recording of the exact time of important events related to the operations of the CA, life cycle of certificates or keys;

e) Records related to the certificates/seals must be stored for the period when the CA has to present legal evidentiary materials of certification practice to ensure validity of the qualified electronic signatures;

f) The recorded events must be stored in such a way that there is no possibility to change, delete or destroy them during the storage period;

g) Important and exceptional events and data must be documented;

Registration:

h) Ensure that all the events related to the registration procedure have been recorded;

i) Ensure that all the information received during the registration has been recorded and documented. Such information must include the following:

- Types of documents presented along the applications to create a certificate/seal;
- Unique identification data of the submitted documents, such as number and date of issue;
- Place where applications, documents submitted for identification and copies of agreements are stored;
- Specific options of the signatory in the agreement;
- Identification data of the employee who received the application;
- Methods applied for verification of identity documents;

Generation of certificates/seals:

a) Record all the events in the life cycles of keys managed by the CA;

b) Record all the events in the life cycles of the issued certificates/seals;

Preparation and issue of the SSCD:

c) Record all the events related to preparation and issue of the SSCD;

Management of changes to the certificate/seal status:

d) Record all the events related to the changes to the certificate/seal status, including applications, reports and events resulting thereof.

4. ORGANISATIONAL ISSUES

The CA shall ensure reliability of its operations with the following measures:

General measures:

a) Show that certification practice follows the CP and the CPS provisions;

b) Show that the CA is practicing legally and in conformity to the laws of the Republic of Lithuania;

c) Have appropriate quality and information management systems;

d) Have due means for fulfilling obligations arising from the liabilities undertaken;

e) Ensure financial stability and have enough resources for proper implementation of the CP and operation under the CPS;

f) Employ the staff with relevant education, experience and knowledge necessary for the performance of certification practice;

g) Have defined procedures for the settlement of disputes and claims related to the certification practice;

h) Have properly legally documented sub-contracting, hire and other contracts.

Generation of certificates/seals and management of the status

i) Operations of the CA related to the generation of certificates/seals, suspension and revocation of certificates/seals must be independent. The staff holding exclusive trust roles must be protected against possible external financial or commercial influence, which may affect reliability of the CA activities;

j) Operations of the CA related to generation of certificates/seals, suspension and revocation of certificates/seals must be strictly documented in order to ensure equity, objectivity and transparency of the operations.

5. THE CP ADMINISTRATION

This chapter provides for the requirements on the CP administration.

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

5.1. Procedures for Amending the CP

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

Amendments to the CP shall fall into two categories:

a) Substantial changes when users should be informed thereof and the CP OID should be amended;
b) Insignificant changes when the CA is not obligated to inform other parties thereof and the CP OID is not changed.

When substantial changes are made, the first digit of a new CP version and OID version element (the last digit) shall be changed. When insignificant changes are made, the second and later digits of the new CP version shall be changed.

Insignificant changes 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 CP have changed.

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

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

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

b) The CA or certificate/seal users shall initiate the CP changes;

c) The staff at the CA responsible for security policy shall draft a new version of the CP;

d) The Electronic Signature Supervision Institution shall be notified of a new CP version.

6. DEFINITIONS AND ABBREVIATIONS

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

Authentication means the process of determining authenticity or personal identity if a user is who he claims to be, or if an object is the original one.

Authentication certificate means a certificate for identifying a person in the electronic environment, which verifies or enables to determine identity of a person in the electronic environment.

Authenticator means a competent natural person who holds signature creation device and uses signature creation data for self-authentication in the electronic environment.

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 owner means a natural person whom (on behalf of whom) a certificate is created. In case of qualified certificates, the certificate owner shall be the signatory, while in case of authentication certificate – authenticator.

Certificate/Seal Policy means certificate/seal creation and use policy establishing the rights and obligations of the certification centre, the certificate/seal owner and the relying parties. Qualified certificate/seal policy is selected by the signature users, while approved and implemented by the certification centres. Qualified certificate/seal policy shall be developed on the initiative of the signature user group, the certification centre or selected from the Lithuanian Standard LST ETSI TS 101 456 "Strategic Requirements for Certification Services Providers Who Issue Qualified Certificates".

Certificate/Seal Revocation List (**CRL**) means a list of certificates/seals that have been suspended or revoked, which is periodically (or urgently) issued and signed by the certification centre. Such a list usually contains the name of certification centre that made this list, date of making the list, the expected date of issuing next version of the list, serial numbers of the revoked certificate/seal, time when the certificate/seal was suspended or revoked.

Certificate sequence means a set of certificates verifying signature of the signatory, which consists of a signatory's certificate, certificate of the service provider who created and signed the signatory's certificate and other in such a way related certificates of service providers (or none of them), ending with the certificate of the service provider who creates and signs the certificate for himself.

Certification Authority (**CA**) means the certification service provider who creates and manages persons' certificates/seals.

Certification Practice Statement (**CPS**) means the approved basic rules of operations of the certification centre that creates qualified certificates/seals.

Certification Service Provider (**CSP**) means the enterprise having no rights of legal entity or legal entity creating certificates or providing other services related to electronic signature.

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

Cryptographic module – see Hardware security module.

Electronic seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

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

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

Key pair means mathematically associated pair of cryptographic keys: private and public keys.

Private key means unique data that are used by a person 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 the authorised institution.

Qualified Certificate/Seal Policy (**CP**) means the certificate/seal policy containing the requirements 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.

Qualified electronic signature means the secure electronic signature created with the secure signature creation devise (SSCD) and verified with a valid qualified certificate.

Registration Authority (**RA**) means a unit of the certification authority or a separate legal entity that has entered into agreement with the certification authority, and is collecting and processing applications of persons to create and revoke certificates and to withdraw suspension of the certificates.

Relying parties means persons who receive data and certificates/seals signed by the certificate/seal owners and aim at assuring identity of the certificate/seal owner and other information provided in the certificates/seals.

Repository means the database of certificates/seals and other information of the RCSC accessed by users on-line at any time on the Internet site: http://www.elektroninis.lt/.

Secure electronic signature means the electronic signature complying with the following requirements: (1) electronic signature is bound only with the signatory; (2) it enables identification of the signatory; (3) it is created using the means that may be managed by the signatory only at his will; (4) it is associated with the signed data in such a way that any change of these data is detectable.

Secure Signature Creation Device (**SSCD**) means hardware or software where private and public keys as well as certificates are generated (or recorded into) and stored, and which is used for the creation of electronic signatures or determination of personal identity. It should comply with the following requirements: (1) signature formation data used for the creation of electronic signature could be practically obtained only once, and their secrecy must be secured; (2) signature formation data used for the creation of electronic signature could not be practically restored, thus the existing technologies safeguard against forgery of electronic signature; (3) signature formation data used for the creation of electronic signature could be reliably secured by the signatory against other persons; (4) when creating electronic signature, the signature creation device does not change the signed data and does not prevent the signatory from following the data before signing.

Security policy means a document of the highest importance defining secure operation policy of the centre issuing certificates/seals.

Signatory means a competent natural person who holds a signature creation device (private key) and creates an electronic signature.

Signature users mean persons who use electronic signature in their activities or receive the signed data from other persons.

Subscriber means a person entering into agreement with the CA on behalf of one or more persons (certificate/seal owners) whom a certificate/seal is created. At the same time the subscriber may be a certificate/seal owner.

Time stamp means the data, which are logically bound with other data and verify that those other data existed prior to the time indicated in time stamp. Time stamp of electronic signature is a proof that signature has been created prior to the time indicated in the time stamp.

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

Users means certificate/seal owners and parties relying on certificates/seals.

CA – Certification Authority

CP – Qualified Certificate/Seal Policy

CPS – Certification Practice Statement

CSP - Certification Service Provider

CRL – Certificate/Seal Revocation List

CWA – CEN Workgroup Agreement

ETSI – European Telecommunication Standardisation Institute

FIPS – Federal Information Processing Standards

LST – Lithuanian Standards Board

OID – Object Identifier

OCSP – Online Certificate/Seal Status Protocol

PIN – Personal Identification Number

PKI - Public Key Infrastructure

RA - Registration Authority

RCSC - Certification Centre of the Centre of Registers

RFC - Request For Comments Authority

RSA – Rivest-Shamir-Adelman algorithm

SHA-1 – Secure Hash Algorithm 1

SSCD – Secure Signature Creation Device