STATE ENTERPRISE CENTRE OF REGISTERS

QUALIFIED CERTIFICATE (ELECTRONIC SIGNATURE AND ELECTRONIC SEAL) POLICY OF THE CERTIFICATION CENTRE OF THE CENTRE OF REGISTERS

Unique Object ID (OID): **1.3.6.1.4.1.30903.1.1.7**
Version: 7.2
Valid from: 23 April 2020

23 April 2020

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
6.0	11 July 2017	Sixth version
6.1	24 November 2017	Insignificant changes
7.0	31 May 2019	Changes after comments from the Communications Regulatory Authority of the Republic of Lithuania
7.1	16 December 2019	Changes after comments from the Communications Regulatory Authority of the Republic of Lithuania
7.2	23 April 2020	Changes

Document approval:

Document preparation	Name	Date	Signature
Document approved by	Saulius Urbanavičius, Director General	23 April 2020	

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.

1.1. Overview

Qualified Certificate (Electronic Signature and Electronic Seal) Policy (hereinafter – CP) means a set of rules determining whether qualified electronic signature and qualified electronic seal certificates issued by the trust service provider – Certification Authority (hereinafter – CA) of the Centre of Registers 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 meeting the requirements of this policy. The CP shall establish rights and obligations of the trust service provider and certificate owners, users and persons relying on them.

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

b) The up-to-date version of 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 (hereinafter – General Data Protection Regulation);

c) Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(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;

d) Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services;

e) The up-to-date version of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions;

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

g) Resolution No 144 of the Government of the Republic of Lithuania of 18 February 2016 "On the Designation of the Supervisory Body for Trust Services and the Body Responsible for the Establishment, Maintenance and Publication of the National Trusted List";

h) Order No 1V-588 of Director of the Communications Regulatory Authority of the Republic of Lithuania of 21 June 2018 "On the Approval of the Specification of the Procedure for Granting Status of Qualified Trust Service Providers and Qualified Trust Services and Incorporation Thereof in the National Trusted List and Provision of Activity Reports of Qualified Trust Service Providers";

i) 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";

j) 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";

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

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

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

n) ETSI EN 319 412 Certificate Profiles;

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

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

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

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

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

t) ETSI TS 119 312 v1.3.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;

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

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

w) 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 creation;

c) issuance of certificates and provision of information on the certificate use, restrictions, terms and conditions;

d) certificate life-cycle management;

e) provision of information on the certificate status;

f) preparation and provision of the SSCD/QSCD.

1.2. Identification

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

1.3.6.1.4.1.30903.1.1.7

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	7.0

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

1.3. Certificate Users and Application Areas

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

a) qualified certificates for electronic signature, i.e. electronic signature certificates (electronic attestations which link electronic signature validation data to a natural person and confirm at least the name or the pseudonym of that person), created in compliance with eIDAS and other legal acts and standards specified in Chapter 1.1 of the CP;

b) qualified certificates for electronic seal, i.e. electronic seal certificates (electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person), created in compliance with eIDAS and other legal acts and standards specified in Chapter 1.1 of the CP;

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

Qualified and authentication certificates for electronic signature issued by the CA are associated with natural persons, while qualified certificates for electronic seals – with legal persons. The CA does not issue certificates associated with a person's job duties.

Certificate users shall be as follows:

a) subscribers;

b) certificate owners;

c) parties relying on certificates.

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

1.4. Organisational Structure

Functions of the Trust Service Provider (hereinafter – **TSP**) shall be executed by the Centre of Registers. The CSP shall provide certificate creation and management services, time-stamping and other trust services. The qualified certificate creation and management services shall be provided by the CA.

The CA shall delegate a certain part of its functions pertaining to qualified certificate creation and management to authorities supporting trust service operations (hereinafter – **Support Service**) and registration (person identification) 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.

Pursuant to eIDAS, the CA shall remain responsible for all the trust services being provided and trust service 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, the CA shall attest that certificates 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 e-Signature Certificates Division of the State Enterprise Centre of Registers
Address	Lvovo str. 25-101, LT-09320 Vilnius, Lithuania
Tel.	+370 5 268 8202
URL	http://www.registrucentras.lt
E-mail	*info@elektroninis.lt*

2. GENERAL PROVISIONS

This chapter specifies obligations of the CA and parties related to the use of certificates 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 creation and management services in line with its CPS.

When executing its functions, the CA shall undertake to:

a) ensure security of the CA private cryptographic keys (hereinafter – keys);

b) ensure that information contained in the issued certificate is true;

c) ensure proper identification of a person to whom a certificate is being issued;

d) ensure acceptance and handling of applications to issue certificates:

- ensure that applications to issue certificates are being accepted and handled consistent with the CP and CPS;
- ensure secure preparation and delivery of SSCDs/QSCDs to persons;

e) provide the certificate users with accurate and true information enabling to:

- check the certificate validity;
- draw attention upon the procedure for, and restrictions on, the certificate use;

f) accept applications to revoke or suspend a certificate:

- accept and handle applications to revoke or suspend a certificate, as provided for in the CP and CPS;

- revoke a certificate upon expiration of the certificate suspension period;

g) accept applications to withdraw the certificate suspension:

- accept and handle applications to withdraw the certificate suspension, as provided for specified in the CP and CPS;
- remove the certificates, suspension thereof has been withdrawn, from the Certificate Revocation List (hereinafter – CRL).

h) ensure personal data protection regulated by the General Data Protection Regulation, the Law of the Republic of Lithuania on Legal Protection of Personal Data, and other legal acts of the Republic of Lithuania to the extent they do not contradict the General Data Protection Regulation;

i) use only the SSCD/QSCD compliant with eIDAS for generation and storage of cryptographic keys and storage of certificates created for persons relating to these keys: certificates for electronic signature – Articles 29 and 30 of eIDAS; certificates for electronic seal – Article 39(1) and 39(2) of eIDAS.

2.1.2 RA obligations

The Registration Authority shall undertake to:

a) verify the identity of a person;

b) accept applications to create certificates;

c) prepare SSCS/QSCD, certificates and present them to persons;

d) accept and handle applications to revoke certificates;

e) accept and handle applications to suspend certificates;

f) accept and handle applications to withdraw the certificate suspension;

g) revoke, suspend or withdraw the suspension of certificates issued by the RA;

h) 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. Assessment of the functions and obligations of the RA shall include the following:

a) information on the conditions of certificate creation published by the RA;

b) the procedure for identification of the person, who wants to buy a certificate;

c) security of the RA staff;

d) the procedure for revocation or suspension of certificates issued by the RA;

e) the procedure for archiving and storage of documentation received in the course of provision of certificate issuing services;

f) physical and procedural security of the premises and equipment used by the RA.

2.1.3 Obligations of the Support Service

The Support Service shall undertake to:

a) accept, 7 (seven) days per week, 24 (twenty-four) hours per day, via the telephone, applications to suspend a certificate, technically suspend the certificate, and provide information related to the trust service practices.

2.1.4 Obligations of the subscribers and certificate 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 owners:

c) use the pair of public and private keys only in accordance with the purpose of use indicated in the certificate, 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 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 have been detected, or changes need to be made thereto;

f) if a private key has been compromised, urgently and completely cease its use.

2.1.5 Obligations of the relying parties

Persons relying on certificates must:

a) assure that the CA is reliable;

b) assure that the certificates have been used in accordance with their purpose of use;

c) assure that the certificates are valid;

d) undertake the procedure for checking the certificate sequence;

e) assure that the software used is capable to process all the certificate information, including additional fields. Prior to making decision regarding the certificate reliability level, the parties relying on certificates must get familiar with the CP and CPS. Relying parties must use certificates only in accordance with the purpose of use and be aware of the restricted areas of certificate use.

2.2. Liability

General provisions concerning liability of the CA shall be governed by the eIDAS Regulation and the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

The CA shall be liable for the following:

a) the accuracy of the data of the created certificates;

b) consistency between the signature creation data and the signature verification data;

c) the fact that a person specified in the created certificates is the holder of the signature creation data corresponding to the signature verification data indicated in the certificates;

d) timely revocation or suspension of the certificates;

e) appropriate publication of information about the revocation of the issued qualified electronic signature certificates.

The CA shall assume liability for any loss incurred by the certificate 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 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 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 certificate users and other parties that are not associated with the CA, as well as for any losses incurred by certificate users when they have been duly informed in advance about the terms and conditions as well as restrictions on the use of certificates 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:

f) 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;

g) unauthorised use of certificates (e.g., when the certificate is not valid or when the restrictions on the certificate 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, trust services, including creation and management of qualified certificates and requirements for service providers, and liability shall be collectively established by eIDAS, and other national legal acts as well as EU legislation. The CPS implementing the current CP shall specify the terms and conditions on trust service provision as well as liability cases.

2.4. Fees

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

The CA shall not require any remuneration for:

a) provision of the CRL;

b) publication of the CP and CPS;

c) revocation or suspension of certificates.

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 trust service practices.

The CA shall undertake to provide information about the certificate 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 creation about the terms and conditions on certificate creation and management. The terms and conditions must contain the following information to be provided by the CA:

a) authorised use of the certificates (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 owner;

d) obligations and liability of the CA.

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

a) authorised use of the certificate (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 creation in conformance with the General Data Protection Regulation and other legal acts of the Republic of Lithuania and other legal acts of the Republic of Lithuania to the extent they do not contradict the General Data Protection Regulation. 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 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 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.

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 trust service 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 trust service practices, 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 trust service practices to the CP;

d) the certificate users shall be provided with all the information regarding restrictions as well as terms and conditions on certificate 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 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 shall be generated using hardware; therefore keys are protected against copying or any other unauthorised use. Certificates for electronic signature shall be created only for persons, using the SSCD/QSCD compliant with the requirements of Article 29 and Article 30 of eIDAS provided by the CA. Certificates for electronic seal shall be created using the qualified electronic seal creation devices compliant with the requirements of Article 39(1) and Article 39(2) of eIDAS.

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 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 and CRLs of persons, are not used for any other purposes;

b) private keys, used for verifying the CA certificates, 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, and the previously used private keys are destroyed.

3.2.8 Life cycle of cryptographic device used for signing certificates

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 trust service practices;

c) cryptographic device, used for signing the certificates, CRLs, OCSP notifications and other important information, is functioning correctly;

d) keys stored in HSM are destroyed upon expiry of the HSM usage period.

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 electronic signature keys are generated using the SSCD/QSCD compliant with the requirements of Article 29 and Article 30 of eIDAS. Pairs of electronic seal keys

are generated using the seal creation devices compliant with the requirements of Article 39(1) and Article 39(2) of eIDAS;

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

3.2.10 Preparation and provision of the SSCD/QSCD

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

a) SSCD/QSCD preparation is securely controlled and performed;

b) SSCD/QSCD is securely stored and passed;

c) SSCD/QSCD 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/QSCD to the user:

a) issue only the SSCD/QSCD compliant with the provisions of Article 39(1) and Article 39(2) of eIDAS or Article 29 and Article 30 of eIDAS;

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

c) after SSCD/QSCD is assigned to a person or the SSCD/QSCD public key certificate 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/QSCD to a person;

d) at the time of issuing the SSCD/QSCD, 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/QSCD;

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

3.3. Certificate Management Cycle

3.3.1 Agreement conclusion

The CA must ensure that persons applying for certificate issuance are properly identified, i.e. the identity and additional specific attributes (if applicable) of those persons is verified as laid down in 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, approved by Order No 1V-1055 of Director of the Communications Regulatory Authority of the Republic of Lithuania of 26 October 2018. Also, the CA must ensure that the submitted applications are lawful, complete and valid.

The RA must:

a) prior to concluding an agreement on the provision of trust services, inform a person applying for certificate creation about the terms and conditions, restrictions on certificate creation and management, obligations and liability of the CA, the subscriber and the certificate 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 personally:

- a passport or
- an ID card;
- a residence permit in Lithuania issued by the Migration Department of the Republic of Lithuania (only for non-citizens of the Republic of Lithuania).

require that representatives of **legal** persons applying for creation of electronic seal certificates submit personally:

- 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) A qualified provider or its authorised third party shall also verify the identity of a legal person to whom qualified certificate is issued, when the identity is verified with an authorized representative of the legal entity being physically present, on the basis of the following documents provided by the authorized representative of the legal person:

- an extract from the register, in which data on the legal person is accumulated and stored, or if, in accordance with the legal acts of a foreign state, such an extract is not issued, another document confirming the fact of registering a legal person, which contains the following data:

  - name of the legal person;
  - legal form of the legal person;
  - registered office (address) of the legal person;
  - code of the legal person (if, in accordance with the legal acts of a state, in which the legal person is registered, such a code is assigned);

d) according to the national legal acts, verify the identity and specific attributes (if applicable) of persons applying for certificate creation;

e) assess whether a valid personal identity document has been submitted;

f) determine whether the submitted personal identity document contains a photograph of that person;

g) assess the status of the submitted personal identity document (by paying special attention to whether the photo, pages or records have not been altered, corrected or similar);

h) require that persons applying for certificate creation provide the contact details, which can be relied upon when contacting them;

i) document and store all the information (by making photocopies or digital copies) used to identify a person, including the document type, number and restrictions on the document validity and, if applicable, documents proving specific attributes;

j) document and retain the concluded agreement covering:

- obligations of the certificate owner;
- terms and conditions on publication of personal data, the certificate and separate data of the certificate;
- consent to store information on the registration of the certificate owner, SSCD/QSCD 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 owner is true;

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

l) undertake to protect personal data following the General Data Protection Regulation.

The data received by the CA from the RA shall be transmitted via the SSL channel. TSP can be accessed only by known endpoints (PCs) (controlled by Firewall) and only by authorized persons (authorization is done by a person's certificate). All valid/invalid and successful/unsuccessful requests shall be written in the log database.

If the CA receives incorrect, inaccurate or incomplete data, certificates shall not be issued.

3.3.2 Certificate updating

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

3.3.3 Certificate creation

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

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

a) the procedure for certificate 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 creation;
- the private key must be generated within the SSCD/QSCD;
- the SSCD/QSCD must be securely passed to the certificate owner.

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

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

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

The qualified certificates created must meet the requirements of the eIDAS Regulation and legal acts of the Republic of Lithuania governing trust services (to the extent they they do not contradict eIDAS).

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

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

a) clearly indicate the applicable CP;

b) inform of the restrictions on certificate use;

c) inform of the obligations of certificate users;

d) provide information on how to check the validity of certificates;

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 issuance

The CA must ensure that:

a) upon creation, the complete and accurate certificates are passed to their owner;

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

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 issued by the CA as well as search for certificates shall not be applicable in the trust service practices.

3.3.6 Certificate revocation and suspension

The CA shall ensure the revocation of certificates. A received application shall, in all cases, be registered in the database on certificates. Certificates shall be revoked and information on the revocation status of the certificates shall be published no later than within 24 (twenty-four) hours after the date of receipt of the application. Certificates shall lose their validity from the moment of their revocation and the revocation shall become effective immediately upon its publication. The validity status of the revoked certificates shall not in any circumstances be reverted.

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

The CA shall revoke certificates in the following cases:

a) upon request of the subscriber or the certificate owner;

b) when the data specified in certificates is found to be no longer true;

c) when the certificates are found to have been created on the basis of inaccurate data;

d) when the CA issuing certificates ceases its operations, and any other CA does not take over the trust service practices;

e) when the certificate owner does not follow the terms and conditions on the certificate use;

f) when the control over the signature creation or activation data corresponding to the certificates has been lost;

g) on the basis of the restrictions on certificate validity, as specified in the certificates during their creation;

h) upon receipt of notification that the certificate owner has become legally incapable;

i) upon receipt of notification that the certificate owner died;

Pursuant to the national legislation, certificates shall be suspended within 4 (four) working hours following the receipt of an application. Suspension of certificates shall, in all cases, be indicated in the database on certificates and information on the suspension status of certificates shall be available in the course of providing information on their status. Certificates, which have been suspended, shall lose validity for the period of their suspension.

The CA shall suspend certificates in the following cases:

a) upon request of the certificate owner;

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

c) upon receipt of information that the certificate data is not true or the certificate owner has lost control over the signature creation or activation data corresponding to the certificates.

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

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

    - in what cases and under what circumstances certificates must be revoked and suspended;
    - who may submit an application to revoke or suspend certificates;
    - how an application may be submitted;
    - any requirements for confirmation of an application to revoke or suspend certificates;
    - what mechanism is used for distributing of information on certificates that have been suspended or revoked;

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

c) applications to revoke and suspend certificates are processed immediately upon receipt;

d) applications to revoke and suspend certificates 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 revocation of certificates, the suspension status may be set to the certificates; however, duration of such a status should not exceed the period required for confirmation of the certificate status;

g) where certificates have been suspended or revoked without request of the certificate owner, the certificate owner must be informed thereof accordingly.

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

3.3.7 Checking of certificate validity

The CA must ensure that its created certificates are available:

a) upon certificate creation, the complete and accurate certificate must be made available for the certificate users. The CA shall provide information on the certificate 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 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 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 trust service 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 trust service practices, even if some functions thereof 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 regarding 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 30 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) a certificate regarding (the absence of) a criminal record[1];

d) documents confirming education, professional training;

e) a curriculum vitae (CV);

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);

[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

i) 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 trust services.

The CA must ensure that:

General requirements

a) physical access to the premises, wherein certificates are created, the SSCD/QSCD 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 generation, provision of the SSCD/QSCD, revocation and suspension of certificates:

a) operational devices related to the creation of certificates, provision of the SSCD/QSCD as well as revocation and suspension of certificates 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, provision of the SSCD/QSCD as well as revocation and suspension of certificates. 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, trust service provision system and other service provision resources against natural disasters, fire, theft, 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 trust 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 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

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

Requirements for the certificate 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 issuance:

a) control of the certificate issuance system in case of attempt to add, remove or change certificates 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 status;

Requirements for provision of information on the certificate status:

a) control of the system for provision of information on the certificate status in case of attempt to add, remove or change the certificate 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 trust service 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, 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 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 and the CRLs signed with a compromised private key.

3.4.11 Termination/transfer of trust services

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

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

a) inform accordingly all the persons, whom it created certificates and whose certificates are valid, and other trust service providers with whom surety agreements have been concluded, partners to whom the functions of the CSP, as the trust service provider, have been transferred on a contractual basis, third parties to whom trust services are provided on a contractual basis, as well as the supervisory body not later than 9 (nine) months in advance;

b) taking into account the scheduled date of termination of the service provision, but not later than 6 (six) months in advance, submit to the supervisory body the following: 1) information on the transferee of the operations; 2) an agreement on the takeover of the operations; 3) a Detailed Plan for Termination of Qualified Trust Service Practices;

c) if, after deciding to terminate the provision of qualified trust services, the operations are not transferred to any third party, the CSP must ensure that the certificates issued to persons remain valid during their life cycle and that all information collected (in the course of provision of trust services) is retained for use as evidentiary materials for judicial proceedings. In order to fulfil this commitment, the CSP shall ensure OCSP and CRL generation functions until the expiry of all issued qualified certificates, i.e. both timely expiry and after revocation, as well acceptance and execution of requests for suspension/revocation of certificates;

d) if it is impossible to ensure the validity of certificates issued to persons during the period of their life cycle, such certificates shall be revoked and private cryptographic keys of trust service providers used to create certificates for persons, as well as private cryptographic keys for signing OCSP requests shall be destroyed immediately after the revocation of certificates issued to persons. Detailed destruction procedures are set out in the Detailed Plan for Termination of Qualified Trust Service Practices;

e) revoke the authorisations of third parties to act on behalf of the CA in providing the trust services.

3.4.12 Storage of records and archiving

The CA must store records on all operations related to the certificates issued with the aim of having evidentiary materials of proper trust service 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;

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

c) present current and archival records about certificates as evidentiary materials of proper trust service 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 must be stored for the period when the CA has to present legal evidentiary materials of trust service 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;
- 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:

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;

Preparation and issue of the SSCD/QSCD:

c) record all the events related to preparation and issue of the SSCD/QSCD;

Management of changes to the certificate status:

d) record all the events related to the changes to the certificate 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 trust service 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 trust service practice;

g) have defined procedures for the settlement of disputes and claims related to the trust service practice;

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

Generation of certificates and management of the status

i) Operations of the CA related to the generation of certificates, suspension and revocation of certificates 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, suspension and revocation of certificates 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.

Users shall follow the latest version of the CP, the OID of which is specified in the electronic signature certificate.

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 trust 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 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 supervisory body 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.

Advanced electronic signature means an electronic signature that meets the following requirements: (1) it is uniquely linked to the signatory; (2) it is capable of identifying the signatory; (3) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (4) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

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

Certificate (electronic seal) owner means a legal person whom (on behalf of whom) an electronic seal certificate is created.

Certificate Revocation List (**CRL**) means a list of certificates 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 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, the time of, and reasons for, suspension or revocation of the certificates.

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 a trust service provider who creates and manages persons' certificates.

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

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

Creator of a seal means a legal person who creates an electronic seal.

Cryptographic module – see Hardware security module.

Electronic identification means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

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 means data in electronic form, which is attached to or logically associated with other data in electronic form and which are used by the signatory to sign.

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 a 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 for electronic seal means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in eIDAS.

Qualified certificate for electronic signature means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in eIDAS.

Qualified Certificate (Electronic Signature and Electronic Seal) Policy (**CP**) means certificate creation and use policy, prepared in accordance with the requirements laid down in eIDAS, defining the rights and obligations of the certification centre, the certificate owner and the parties relying on certificates. The Qualified Certificate Policy is selected by the signature users, while approved and implemented by the certification centre. The Qualified Certificate Policy shall be developed on the initiative of the signature user group by the certification centre or selected from the Lithuanian Standard LST ETSI TS 101 456 "Strategic Requirements for Certification Services Providers Who Issue Qualified Certificates".

Qualified electronic seal means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.

Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Qualified Signature (Seal) Creation Device (QSCD) means an electronic signature or electronic seal creation device (configured software or hardware used to create an electronic signature or electronic seal) that meets the requirements laid down in eIDAS and is included in the list published by the European Commission.

Qualified trust service provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

Registration Authority (**RA**) means a unit of the trust service provider or a separate legal entity that has entered into agreement with the trust service provider, and is accepting and handling applications of persons to create and revoke certificates and to withdraw suspension of the certificates.

Relying parties means natural or legal persons that rely upon an electronic identification (signature, seal) or another trust service.

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

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 shall 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 certification centre.

Signatory means a natural person having legal capacity who 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 (natural/legal) person entering into agreement with the CA on behalf of one or more persons (certificate owners) whom a certificate for electronic signature or electronic seal is created. At the same time the subscriber may be a certificate owner.

Time stamp means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

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

Trust service means an electronic service provided for remuneration which includes: (1) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps; (2) the creation, verification and validation of certificates for website authentication; and (3) the preservation of electronic signatures, seals or certificates related to those services.

Trust Service Provider (TSP) (Certification Service Provider (CSP)) means a natural or a legal person who provides one or more trust services.

Users means certificate owners and parties relying on certificates.

CA – Certification Authority

CP – Qualified Certificate (Electronic Signature and Electronic Seal) Policy

CPS – Certification Practice Statement

CSP – Trust Service Provider

CRL – Certificate/ Revocation List

ETSI – European Telecommunication Standardisation Institute

FIPS – Federal Information Processing Standards

LST – Lithuanian Standards Board

OID – Object Identifier

OCSP – Online Certificate Status Protocol

PIN – Personal Identification Number

PKI – Public Key Infrastructure

QSCD – Qualified Signature (Seal) Creation Device

RA – Registration Authority

RCSC – Certification Centre of the Centre of Registers

RSA – Rivest-Shamir-Adleman algorithm

SHA-1 – Secure Hash Algorithm 1

SSCD – Secure Signature Creation Device