AS Sertifitseerimiskeskus
Certification Practice Statement CPS

Version 2.4
OID: 1.3.6.1.4.1.10015.1.2.4
01.07.2009

Version and Changes		
Date	**Version**	**Changes**
30.04.2009	2.4	References to standards updated RFC 2459 → RFC 3280, Lingual corrections. Additions and changes: - Introduction - names of founding members updated; - 1.1 - Certificate Policies are now submitted to RCS; - 1.2.3.2 – update with requirements of digital stamp; - 2.1.4 – certificate validity confirmation against CRL is now replaced with validity information provided by the SK; - 2.1.5 – directory service does not indicate the status of the certificates issued; - 2.1.5 – deleted: security measures have to be applied to prevent spoofing of directory service and for ensuring data integrity; - 2.4.1 – addresses of public informational services are updated, LDAP address is added; - 2.5 - internal audit is carried out by internal auditor twice a year. Audit results shall be published on the SK's website; - 4.3.1 – public network is discarded from the list of channels for suspension and revocation of certificates; - 4.4.1.4 – the certificate holder shall be notified immediately after processing the certificate suspension operation; - 4.5.4 - the certificate holder shall be notified immediately after processing the certificate suspension operation; - 4.8 – The SK will establish internal regulations, instructions and recovery plans for acting in emergency situation in order to ensure quality and security of the service provisioning; - 6.2.1 – The SK uses the access control system.
07.10.2002	2.1	Section “Secure Log System” (4.7.3) is added.
01.02.2002	2.0	Redesigned into universal source document for various Certificate Policies: - The CA structure of the SK has been omitted; - The CPS no longer has OID; - Provides for a possibility to delegate certain procedures (e.g. identification) under a contract; - Generalizes the clauses on the certificate and CRL profiles;

		- Omits many inessential and/or ID-card specific provisions; Language usage and layout have been elaborated, inessential provisions have been omitted.
31.08.2001	1.1	First public version.

Table of Contents

1. Introduction 5
1.1. Overview 5
1.2. Organization and Area of Application 6
1.2.1. Sertifitseerimiskeskus (SK) 6
1.2.2. Registration Centre 6
1.2.3. User 6
1.2.4. Area of Application of Certificates 7
1.3. Contact Details 7
2. General Provisions 8
2.1. Obligations 8
2.1.1. SK Obligations 8
2.1.2. Registration Authority Obligations 8
2.1.3. Obligations of Clients 9
2.1.4. Obligations of Relying Party 9
2.1.5. Obligations of Directory Service 9
2.2. Liability 10
2.2.1. SK Liability 10
2.2.2. RA Liability 10
2.2.3. Limits of Liability 10
2.3. Dispute Resolution Procedure 10
2.4. Publication of Information and Directory Service 11
2.4.1. Publication of Information by the SK 11
2.4.2. Frequency of Publication 11
2.4.3. Rules of Access 11
2.4.4. Directory Service 11
2.5. Compliance Audit 11
2.6. Confidentiality Provisions 12
2.6.1. Confidential Information 12
2.6.2. Public Information 12
2.6.3. Protection of Personal Data 12
3. Client Identification 13
3.1. Identification of Client 13
3.2. Procedure of Certifying Correspondence of Applicant's Private Key to Public Key 13
3.3. Distinguished Name 13
4. Provision of Certification Service. Procedure and Terms of Certification Process 14
4.1. Submission of Applications for Certificates 14
4.2. Processing of Applications for Certificates 14
4.2.1. Decision Making 14
4.2.2. Issuing Certificates 15
4.2.3. Procedure for Registration of Certificates 15
4.2.4. Certificate Validity Check and Verification 15
4.2.5. Certificate Renewal 15
4.3. Applications for Suspension and Revocation of Certificates 15
4.3.1. Establishment of Authority to Apply for Suspension or Revocation of Certificates 15
4.3.2. Exclusion of Misuse of Revoked, Suspended or Expired Certificate 16
4.3.3. Consequences of Illegal Revocation 16
4.4. Suspension of Certificates 16

4.4.1. Conditions and Procedure of Suspension ... 16
4.5. Termination of Suspension ... 18
4.5.1. Conditions of Termination of Suspension ... 18
4.5.2. Authority to Terminate Suspension ... 18
4.5.3. Application for Termination of Suspension ... 18
4.5.4. Procedure of Termination of Suspension ... 18
4.5.5. Effect of Termination of Suspension ... 19
4.6. Certificate Revocation ... 19
4.6.1. Authority to Revoke Certificates ... 19
4.6.2. Submission of Application for Revocation ... 19
4.6.3. Procedure of Revocation ... 19
4.6.4. Effect of Revocation ... 20
4.7. Procedures Ensuring Tracking ... 20
4.7.1. Preservation of Documents ... 20
4.7.2. Activities Leaving Audit Trail ... 20
4.7.3. Secure Log System ... 21
4.8. Action in an Emergency Situation ... 21
4.9. Termination of Certification Service Provider Operations ... 22
5. Physical and Organizational Security Measures ... 23
5.1. Security Management ... 23
5.2. Physical Security Measures ... 23
5.2.1. SK Physical Entrance Control ... 23
5.3. Requirements for Work Procedures ... 23
5.3.1. Performance of Essential Operations ... 23
5.4. Personnel Security Measures ... 24
6. Technical Security Measures ... 25
6.1. Key Management ... 25
6.1.1. Certification Keys of SK ... 25
6.1.2. Client Keys ... 25
6.2. Logical Security ... 26
6.2.1. Access Control ... 26
6.2.2. Software Security ... 27
6.2.3. Network Connection Security ... 27
6.2.4. Time Synchronization ... 27
6.3. Description of Technical Means Used for Certification ... 27
6.4. Storage and Protection of Information Created in Course of Certification ... 27
7. Technical Profiles of Certificates and Revocation Lists ... 29
7.1. Profiles of Certificates ... 29
7.2. Revocation Lists (CRL) ... 29
8. Management of Certification Practice ... 30
9. References ... 31
10. Glossary ... 32
11. Abbreviations ... 34

1. Introduction

AS Sertifitseerimiskeskus was founded on February 16th 2001. The owners of the limited liability company by equal shares of 25 percent are AS Swedbank, AS SEB Pank, AS Elion Ettevõtted and AS EMT. The principal activities of AS Sertifitseerimiskeskus are offering services associated with necessary certification and other related services required for implementation of digital signature. These services guarantee secure and verified electronic communication with public institutions as well as businesses in everyday life.

The mission of AS Sertifitseerimiskeskus is to provide its clients with completely trustworthy certification services in accordance with the legal acts of the Republic of Estonia and international standards, to be one of the most secure establishments in Estonia as regards data protection and to use state of the art technologies on the basis of specific needs and economic aspects.

1.1. Overview

This document (hereafter CPS) describes the certification practices and procedures used by AS Sertifitseerimiskeskus while providing certification services.

This CPS extends only to the digital certificates issued by root certificate of AS Sertifitseerimiskeskus (Juur-SK) and to the certificates issued by its lower-level certification authorities.

This CPS serves as a basis for framing different Certificate Policies and corresponding certification services provided by AS Sertifitseerimiskeskus.

This CPS has been registered in the Registry of Certification Services (RCS). All the Certificate Policies issued under this CPS, which facilitate issue of certificates for digital signing within the meaning of the Digital Signatures Act [2], are also registered with the RCS.

Internet Engineering Task Force recommended document RFC 2527 [7] has been used in drafting this CPS.

The “Policy Qualifier” field in the root certificate of AS Sertifitseerimiskeskus refers to the version 2.4 of the CPS (OID: 1.3.6.1.4.1.10015.1.2.4).

This CPS helps to achieve the security level approved by the management board and documented in the security policy of AS Sertifitseerimiskeskus. According to the security policy of AS Sertifitseerimiskeskus data protection and reliance on secure and high-quality service founded thereon is the highest priority of AS Sertifitseerimiskeskus.

In the case of conflict between the CP and the CPS the provisions of this CP shall prevail. In case of conflict between the Estonian original document and the English translation the Estonian original shall prevail.

1.2. Organization and Area of Application

1.2.1. Sertifitseerimiskeskus (SK)

SK provides certification services in accordance with the Certificate Policy devised on the basis of this CPS along with related additional services.

The certification service provided by the SK includes by default all the procedures related to the life cycle of the pairs of keys and certificates, which have been described in this document. The SK is entitled to conclude contracts, by which the obligations and assignments are delegated to third parties. Delegated obligations and assignments as well as division of responsibility have been described in the respective Certificate Policy.

This CPS serves as a source document for all Certificate Policies of CA-s administered by the SK. The Certificate Policy of the relevant certification service further specifies the principles set out herein. In the case of conflict between this CPS and a specific Certificate Policy the provisions, the Certificate Policy shall prevail.

The OID of the Certificate Policy is indicated in the “Certificate Policies” extension of the relevant service certificate.

1.2.2. Registration Centre

1.2.2.1. SK Client Service Point

The SK’s Client Service Point acts as the representative of the SK in the relations between the SK and the Client. The SK Client Service Point within the meaning of this CPS accepts applications for certificates, as well as applications for renewal, revocation, suspension and termination of suspension thereof.

The employees of the SK’s Client Service Point have been trained to offer high quality services to the clients of the SK.

The SK Client Service Points may vary with different Certificate Policies. The relationship between the SK Client Service Point and the SK is regulated by a bilateral agreement(s).

For information on the SK Client Service Points and their contact visit the SK’s website for corresponding documentation of the public service.

1.2.2.2. Help Line

The Help Line shall act as the representative of the SK in the field of client telephone servicing and accepts applications for suspension of certificates from clients and other parties after it has identified the person in accordance with the established procedure of identification 24 hours a day;

For further information on the Help Line and its contact details visit the SK’s website (http://www.sk.ee). Instructions for use of the Help Line have also been set out on the website.

1.2.3. User

1.2.3.1. Client

A Client is a holder of a certificate issued on the basis of the Certificate Policy devised on the basis of this CPS.

Distinguished name of a client in the certificate is designed in accordance with the certificate profile of the Certificate Policy designed in accordance with the requirements set out in clause 7.1. The SK shall ensure the uniqueness of the combination of the client's distinguished name and issuer name.

1.2.3.2. Relying Party

A Relying Party is a person or institution who takes a decision relying on the certificate issued by the SK.

A relying party:

- Takes account of the principles set out in the specific Certificate Policy, this CPS and documents referred to;
- Verifies the validity of the certificate via the appropriate certificate status information service provided by the SK;
- Verifies the certificate's correspondence to its area of application;
- In case of certificates facilitating digital signing or digital stamp, verifies the completeness of the digitally signed or stamped data collection and identifies the signer;
- In case of verification a digital signature or a digital stamp, relies on the status of the certificate affixed at the time of signing or stamping.

1.2.4. Area of Application of Certificates

Use of the certificates shall conform to the certificate requirements defined in the Certificate Policies and to the legislation applicable in the Republic of Estonia.

The area of application of the certificates issued may be limited according to the certificate profile. Conforming limitation mechanisms are described in the Certificate Policy, which serves as a basis for issuing certificates.

The conformance of a certificate with the Digital Signatures Act is defined by the Certificate Policy and by the confirming certificate profile description. This CPS does not impose any restrictions or limitations on the designing of such Certificate Policies and its principles are fully founded on the Digital Signatures Act.

This CPS does not limit the use of the certificates issued by the SK in different software applications.

1.3. Contact Details

For further information on the certification services, including the issues related to the work of the certification centre, registration centre and the Help Line please contact:

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 12, 10148 Tallinn
Tel +372 610 1880
Fax +372 610 1881
E-post: pki@sk.ee

http://www.sk.ee/

The change of contact details is immediately announced on the website of the SK.

2. General Provisions

2.1. Obligations

2.1.1. SK Obligations

The SK shall ensure that:

- The supply of the certification service is in accordance with the Digital Signatures Act and related statutory acts;
- The supply of the certification service is in accordance with this CPS.

The SK hereby undertakes to:

- Publish its CPS and Certificate Policies and guarantee their availability in a public data communications network;
- Maintain confidentiality of the information which has become to its knowledge in the course of supply of the service and is not subject to publication;
- Keep account of the certificates issued by it and of their validity;
- In the case of certificates enabling digital signature accept applications for suspension of certificates 24 hours a day;
- In the case of certificates enabling digital signature verify upon request of the Relying Party the validity of the digital signature with the digital signature of its representative with the help of the private key corresponding to the public key incorporated in the certificate issued;
- Ensure round-the-clock possibility to check the validity of certificates in a public data communications network;
- Preserve all the documentation related to certification until termination of its activity;
- Ensure an annual audit of the information system and present the auditor's report to the authorized employee of the national registry to ensure continual registration at Registry of Certification Services;
- Publish the terms of the compulsory insurance policy in a public data communications network.

An employee of the SK may not have been punished for an intentional crime.

2.1.2. Registration Authority Obligations

2.1.2.1. Obligations of Client Service Points

A Client Service Point shall accept applications for creation of certificates, for suspension, termination of suspension and revocation of certificates as well as check the correctness and completeness of these applications. In the performance of all the aforementioned procedures the Client Service Point shall identify and verify the powers and authority of the person submitting any of the named applications.

A Client Service Point shall forward the true and complete data to the SK.

A Client Service Point shall immediately notify the SK about any technical failure hindering the supply of the service and use all reasonable endeavors to repair the failure as soon as possible.

A Client Service Point shall provide its employees with necessary training for supply of high-quality service.

An employee of a Client Service Point may not have been punished for an intentional crime.

2.1.2.2. Obligations of Help Line

The Help Line shall take Client calls 24 hours a day 7 days a week.

The Help Line shall immediately notify the SK about any technical failure hindering the supply of the service and use all reasonable endeavors to repair the failure as soon as possible.

An employee of the Help Line may not have been punished for an intentional crime.

2.1.3. Obligations of Clients

A Client shall observe the requirements provided by the SK in this CPS.

A Client shall supply true and adequate information in the application for the certificate and in the case of a change in the data entered on the certificate notify the correct data in accordance with the rules established in the Certificate Policy. A client shall be aware of the fact that the SK may refuse to issue a certificate if the Client has intentionally presented false, incorrect or incomplete information in the application for the certificate.

A Client shall use his/her private keys and corresponding certificates pursuant to the procedure and in the manner prescribed by the SK.

A Client shall immediately inform the SK of a possibility of unauthorized use of his/her private key and suspend or revoke his/or her certificate.

A Client shall be solely responsible for the maintenance of his/her private key. A Client shall use his/her private key in accordance with the provisions of clause 6.1.2.3 of this CPS.

A Client shall be aware that digital signatures given on the basis of expired, revoked or suspended certificates are invalid.

2.1.4. Obligations of Relying Party

A Relying Party shall study the risks and liabilities related to acceptance of the certificate. The risks and liabilities have been set out in this CPS and appropriate Certificate Policy.

If not enough evidence is enclosed to the certificate or digital signature with regard to the validity of the certificate, a Relying Party shall verify the validity of the certificate on the basis of certificate validation services offered by SK at the time of using the certificate or affixing a digital signature.

A Relying Party shall follow the limitations stated within the certificate and make sure that the transaction to be accepted corresponds to the Certificate Policy.

2.1.5. Obligations of Directory Service

The purpose of the directory service is to provide the clients, relying parties and other persons access to the certificates register to make inquiries about certificates and their validity.

The exact requirements to the directory service shall be specified in the Certificate Policy.

The directory service shall meet the following requirements:

- The directory shall contain valid certificates and their status;
- The directory may not contain delicate personal details within the meaning of the Personal Data Protection Act [5];
- The directory shall be accessible in a public data communications network 24 hours a day.

2.2. Liability

2.2.1. SK Liability

The SK shall be liable for the performance of all its obligations specified in clauses 2.1.1 and 2.1.5 to the extent prescribed by the legislation of the Republic of Estonia.

2.2.2. RA Liability

2.2.2.1. Liability of Client Service Point

The Client Service Point is responsible for the performance of all its obligations specified in clause 2.1.2.1.

2.2.2.2. Liability of Help Line

The Help Line is responsible for the performance of all its obligations specified in clause 2.1.2.2.

2.2.3. Limits of Liability

The SK is not liable for the secrecy of the private keys of the Clients, possible misuse of the certificates or inadequate checks of the certificates by a Relying Party.

The SK is not liable for the non-performance of its obligations, if such non-performance is due to faults or security problems of the Registry of Certification Services, data protection supervision authority or any other public authority.

Non-fulfillment of the obligations arising from the CPS is not considered a violation if such non-fulfillment is occasioned by *Force Majeure*.

2.3. Dispute Resolution Procedure

All disputes between the parties shall be settled by way of negotiations. If the parties fail to reach an amicable agreement, the dispute shall be resolved at the court of the seat of the SK.

The other parties shall be informed of any claim or complaint not later than within 30 calendar days after occurrence of the causes of the claim, unless otherwise provided by law.

2.4. Publication of Information and Directory Service

2.4.1. Publication of Information by the SK

Valid root certificate and archive of root certificates of the SK is published at http://www.sk.ee/certs.

All the SK documents directly related to provisioning of certification services are available in the public data network at https://www.sk.ee/repository.

Certificate Revocation Lists are published at http://www.sk.ee/crls.

Issued certificates are published at ldap://ldap.sk.ee, subject to the relevant Certificate Policy.

The SK guarantees the integrity and availability of the above-mentioned information 24 hours a day and 7 days a week.

2.4.2. Frequency of Publication

The maximum allowed delay in the change of status of the certificate is from registration of the change of certificate status until a new revocation list is issued. The validity time of the revocation list shall be laid down in the Certificate Policy.

The SK shall ensure publication of adequate and up-to-date information about the certificates on its website.

2.4.3. Rules of Access

Access to the information described in clause 2.4.1 in public data communications network is free of charge and access is unrestricted. In the case of other manners of publication the SK may fix a fee in a pricelist and/or require the existence of a service contract.

2.4.4. Directory Service

The revocation lists and valid certificates issued by the SK are published in the directory on the address ldap://ldap.sk.ee, subject to relevant Certificate Policy.

Copies of the revocation lists are available on the website http://www.sk.ee/crls/.

The structures of the directory and the instructions for the use thereof have been listed on the website of the SK.

2.5. Compliance Audit

The operations and activity of the SK shall be audited as follows:

- The operations and activity of the SK are audited once a year according to Regulation No. 83 “Procedure of Auditing Information Systems Servicing Institutions” of the Minister of Transport and Communication dated 3 October 2000;
- Twice a year, an internal audit shall be carried out by the SK’s internal auditor;
- In the case of essential services and modifications in the information system an external auditor shall audit the information systems.

The areas of activity subject to audit are the following:

a) Quality of service;
b) Security of service;
c) Security of the SK's operations and procedures;
d) Protection of the data of the SK's clients and the SK's security policy, performance of work procedures and contractual obligations, as well as compliance with the CPS and Certificate Policies.

Audit reports shall be published on the SK's website.

2.6. Confidentiality Provisions

2.6.1. Confidential Information

All information that has become known while providing the certification service and that is not intended for publication (e.g. information about the activities and information containing technical details of the SK) is confidential.

Disclosure or forwarding of confidential information to a third party is allowed only with the written consent of the legal possessor of the information, on the basis of a court order or in other cases provided by law.

2.6.2. Public Information

The following materials are regarded as public information:

- Certification Practice Statement with the documents referred to herein;
- Certificate Policies with referred to documents;
- Terms and conditions of the compulsory insurance policy;
- Principles of personal data protection;
- Public keys and relevant service certificates of the SK;
- Audit results;
- Information on the validity of the certificates issued.

Access to the public information is ensured in accordance with clause 2.4.3.

2.6.3. Protection of Personal Data

The SK's principles of personal data protection have been stipulated in the document tiled "Personal Data Protection Principles" [4]. By ensuring the personal data protection principles, confidentiality of non-public information, adequacy of client information storage as well as compliance to the Personal Data Protection Act [5] and Public Information Act [1] are guaranteed.

3. Client Identification

3.1. Identification of Client

The identity of the Client shall be verified in accordance with the identity verification procedures stated in the Certificate Policy.

3.2. Procedure of Certifying Correspondence of Applicant's Private Key to Public Key

The procedure of certifying the correspondence of the applicant's private key to the public key can be found in the Certificate Policy.

3.3. Distinguished Name

The client's distinguished name is created in accordance with the profile of the certificate and revocation list defined in the Certificate Policy.

The SK shall guarantee the uniqueness of the combination of the client's distinguished name and the certificate connected to the private key of the SK as used during the certificate approval.

The SK shall record a unique certificate serial number on every issued certificate for every certification service.

4. Provision of Certification Service. Procedure and Terms of Certification Process

4.1. Submission of Applications for Certificates

Certificates can be applied for only in the Client Service Point of the SK if not specified otherwise in the Certificate Policy.

A more detailed procedure for application for the certificates is established by the Certificate Policy.

The procedure of submission of application for certificates facilitating digital signature must at least conform with the Digital Signature Act and with the following statements:

- An application for the certificate shall at least include the following:
  - A reference to the Certificate Policy of the certificate applied for;
  - A note about how a pair of keys is generated;
  - A note about the client authorizing the SK to generate a certificate corresponding to the client's pair of keys;
  - A reference to the media via which the information obtained in the course of supplying the certification service (e.g. information on suspension of certificate) shall be forwarded to the client;
  - A statement to the effect that the client accepts the certification principles, the Certificate Policy and other areas of application of the certificate as well as the documents describing the liability arising from the foregoing.
- The Client fills in and signs the application for the certificate;
- An employee of the Client Service point shall identify the signatory in accordance with the provisions of clause 3.1.

4.2. Processing of Applications for Certificates

The exact procedure and terms for processing applications for certificates are stipulated in a relevant Certificate Policy. In processing the applications for certificates the truth and completeness of the information supplied by the client shall be verified.

4.2.1. Decision Making

The acceptance or rejection of the applications for certificates is the decision of the SK or its contractual partner specified in the Certificate Policy. The decision shall be made within 5 workdays as maximum.

Upon decision making the SK or the contractual partner of the SK specified in the Certificate Policy shall consider whether or not the Client:

- Has a right to receive a certificate under Estonian law;
- Has supplied true and complete information about his/her person in the application for the certificate;
- Holds not the certificates of the same area of application or with the same distinguished name.

The Client shall be informed of the decision via the media described in the Certificate Policy or agreed in the application.

4.2.2. Issuing Certificates

The SK shall, after the establishment of the authenticity and completeness of the application for certificate presented by the Client Service Point of the SK, issue the certificates corresponding to the application. An issued certificate shall be delivered to the Client according to the Certificate Policy.

4.2.3. Procedure for Registration of Certificates

All issued certificates are recorded in the certificate database maintained in a closed information system of the SK.

At the time of certificate issuing, the certificate's copy is saved in a public directory accessible through a public data communications network to all service users 24 hours a day, subject to the Certificate Policy. The directory guarantees access to all valid certificates and revocation lists. In case of need accessibility may be limited if so required in the Certificate Policy and system availability requirements.

4.2.4. Certificate Validity Check and Verification

Upon request of a Relying Party, the representative of the SK shall verify the validity of a digital signature with his/her digital signature containing the private key that corresponds to the public key in the certificate issued by the SK.

The data formats, service charges and time limits of the certificate verification service are established by the SK. The exact terms and conditions are published on the SK's website.

4.2.5. Certificate Renewal

Certificate renewal terms and conditions as well as related procedures and deadlines shall be defined in the Certificate Policy.

The Certificate Policy shall provide for the following renewal possibilities:

a) Certificate renewal after expiry of the certificate;
b) Certificate renewal after revocation of the certificate.

These renewal possibilities shall contain information on whether the new certificate is issued with the same pair of keys or not.

4.3. Applications for Suspension and Revocation of Certificates

4.3.1. Establishment of Authority to Apply for Suspension or Revocation of Certificates

The authority to suspend and revoke certificates shall be established in accordance with the following Table 1 if not specified otherwise in the Certificate Policy.

Table 1. The Authority to Suspend and Revoke Certificates.

Method of Submission of Application	Application for Suspension	Application for Termination of Suspension	Application for Revocation
By phone calling the SK Help Line. Upon suspension of the certificates the personal details of the applicant are asked and they are compared to the data contained in the information system of the SK.	Certificate is suspended if the check-up questions about personal details were answered correctly.	Not accepted. The Client shall be informed of appropriate method of termination of suspension of the certificate.	Certificate is suspended if the check-up questions about personal details were answered correctly and a convenient medium is offered to the client for submitting the request for revocation.
Upon presentation of a personal identification document in a Client Service Point of the SK.	Suspended.	Suspension is terminated.	Revoked.

4.3.2. Exclusion of Misuse of Revoked, Suspended or Expired Certificate

Exclusion of misuse of revoked, suspended or expired certificates is guaranteed after revocation or expiry of the certificate by deletion thereof from the directory and archiving the same in the information system of the SK.

Revoked or suspended certificates shall be published in the revocation list after revocation or suspension of relevant certificates.

4.3.3. Consequences of Illegal Revocation

A person or an institution, due to whose intent or gross negligence a certificate has been revoked without valid legal grounds, shall compensate for any direct loss or damage caused by such revocation.

4.4. Suspension of Certificates

4.4.1. Conditions and Procedure of Suspension

4.4.1.1. Conditions of Suspension

The exact conditions for suspension of certificates have been stipulated in a relevant Certificate Policy. The possibility to suspend certificates shall be set out in the Certificate Policies facilitating digital signing.

According to the Digital Signatures Act [2] a certificate is suspended if:

- The SK or its contractual partner named in the Certificate Policy has reasonable doubts that the certificate contains incorrect data or the private key corresponding to the public key contained in the certificate can be used without the holder's consent;
- Suspension of the certificate is requested by the certificate holder or his or her duly authorized representative;

- Suspension of the certificate is requested by the data protection supervision authority or a senior processor of the Registry of Certification Services in the case of reasonable doubt that the certificate contains incorrect data or the private key corresponding to the public key contained in the certificate can be used without the holder's consent;
- Suspension of the certificate is requested by a court, prosecutor's office or institutions carrying out pre-court criminal investigation to prevent further crimes.

4.4.1.2. Authority to Suspend Certificates

A certificate may be suspended by:

- The Client (certificate holder);
- A senior executive of the SK or its contractual partner named in the Certificate Policy;
- Senior processor of the Registry of Certification Services;
- An authorized public servant named in the Digital Signature Act for carrying out pre-court criminal investigation and preventing further crimes.

4.4.1.3. Submission of Applications for Suspension

The person filing an application for suspension shall file a written application for suspension of the certificate to the nearest Client Service Point of the SK.

Applications for suspension may be also filed round the clock by telephone via the Help Line.

Information about the Client Service Points and their opening hours is published on the website of the SK.

4.4.1.4. Processing of Applications for Suspension

The authority to suspend applications shall be verified pursuant to the procedure described in Table 1 depending on the manner of submission. If the client submits an application for suspension of the certificate in a Client Service Point of the SK, he/she shall first fill in and sign an application form. After that, the applications shall be processed as follows:

- The authority of the applicant to suspend the certificate is verified;
- Legality of the application for suspension of the certificate is established;
- The suspension request is registered by the Help Line operator or suspension is registered by an employee of the Client Service Point of the SK;
- The data related to the person filing an application for suspension are verified;
- The compliance of the application for suspension of the certificate with the Certificate Policy is verified in an information system of the SK;
- The application for suspension is registered in the information system of the SK;
- The certificate is marked as suspended in the certificate database (root code 6 (hold) is used in the CRL);
- The certificate is deleted from the public directory;
- A new CRL is published in accordance with the provisions of clause 2.4.2;
- The documentation on which the applications for suspension were based is archived.

In case the application for certificate suspension was submitted via the Help Line, the certificate holder shall be immediately notified of the successful certificate suspension after the completion of the suspension procedure. The client has a possibility to ascertain on the basis of a public directory or CRL that the certificate has been suspended.

4.4.1.5. Effect of Suspension

The suspension of the certificate is immediately recorded in the certificate database of the SK. Following the suspension, the SK shall issue a new CRL pursuant to the procedure provided in clause 2.4.2, which contains the serial number of the suspended certificate.

4.5. Termination of Suspension

4.5.1. Conditions of Termination of Suspension

The suspension of a certificate shall be terminated upon the written request of a person or body that applied for suspension by entering the relevant data in the certificate database.

By presenting the written request, the certificate holder confirms that all digital signatures created during the time of certificate suspension are invalid.

4.5.2. Authority to Terminate Suspension

The suspension of a certificate may be terminated by:

- The certificate holder suspending the certificate;
- A senior executive of the Registry of Certification Services;
- A senior executive of the SK or its contractual partner named in the Certificate Policy;
- According to the Digital Signature Act, any other officer with relevant authority who acted upon suspension in accordance with clause 4.4.1.2.

4.5.3. Application for Termination of Suspension

The request for termination of suspension shall be filed in writing on a relevant request form after identification and verification of authority in the Client Service Point of the SK.

The request filed for recognition of termination of suspension shall set out the following:

- Name of the person filing the request;
- Signature of the person filing the request;
- The name and ID-code of the holder of the suspended certificate;
- The distinguished name of the SK authority that has issued the suspended certificate;
- Grounds for termination of suspension.

If the request was not filed by the certificate holder but by an authorized official or senior executive of the SK, the documents authorizing termination of the suspension shall be enclosed in the request.

Upon registration of the request the data of the documents used for identification of the person submitting the request shall be recorded.

4.5.4. Procedure of Termination of Suspension

The procedure of termination of suspension shall be the following:

- The initiator of the termination of suspension fills in and signs a written form for termination of suspension of the certificate in the Client Service Point of the SK;
- The authority to terminate the suspension is established;
- The legality of the request for termination of suspension shall be established;

- The compliance of the termination of suspension is verified in the information system of the SK;
- The fact of termination of suspension is registered in the information system of the SK;
- The certificate is published anew in a public directory;
- A new CRL is published in accordance with the provisions of clause 2.4.2.

The certificate holder shall be immediately notified of the successful completion of procedure of termination of suspension of the certificate. The Client has a possibility to ascertain on the basis of a public directory or CRL that the suspension of the certificate has been terminated.

4.5.5. Effect of Termination of Suspension

The suspension of the certificate is immediately recorded in the certificate database of the SK. Following the termination of suspension, the SK shall issue a new CRL pursuant to the procedure provided in clause 2.4.2, which does not contain the serial number of the restored certificate.

4.6. Certificate Revocation

4.6.1. Authority to Revoke Certificates

The application for revocation of a certificate may be filed by the certificate holder, his/her notarially authorized representative or another person specified in legislation.

4.6.2. Submission of Application for Revocation

The certificates are revoked on the basis of a written application.

The application for revocation of the certificate shall set out:

- The applicant's name;
- The applicant's signature;
- The name and ID code of the holder of the revoked certificate;
- The distinguishing name of the SK authority that has issued the revoked certificate;
- Causes of revocation;
- If necessary, evidence to the causes of revocation.

The applicant for revocation is identified in the Client Service Point of the SK on the basis of a personal ID document. Upon registration of the application the data of the document identification document shall be recorded

4.6.3. Procedure of Revocation

The certificate revocation procedure shall be the following:

- The applicant fills in and signs a written form for revocation of a certificate in the Client Service Point of the SK;
- The legality of the request for termination of suspension shall be established;
- The application for revocation is registered in the information system of the SK;
- The certificate is recorded as invalid in a public directory;
- A new CRL is published in accordance with the provisions of clause 2.4.2;
- The documentation on which the applications for revocation were based is archived.

The client has a possibility to ascertain on the basis of a public directory or CRL that the certificate has been revoked.

4.6.4. Effect of Revocation

The revocation of a certificate is immediately recorded in the certificate database of the SK. After revocation of the certificate, the SK shall issue a new CRL in accordance with the procedure described in clause 2.4.2. The new CRL shall also contain the serial number of the certificate.

4.7. Procedures Ensuring Tracking

4.7.1. Preservation of Documents

The SK shall preserve the documents related to the supply of the certification service until termination of its activity.

The documents evidencing the causes of revocation of the certificates shall be preserved until the termination of the SK's activity, unless the law provides otherwise.

If the SK has received a complaint on a certificate or the certificate is submitted as evidence in a legal dispute, the information and documentation pertaining to the certificate shall be preserved until the final judgment has been made.

After termination of the SK's activity all the documents facilitating digital signing shall be handed over to the Registry of Certification Services in accordance with law and pursuant to the established procedure.

4.7.2. Activities Leaving Audit Trail

The SK's information systems leave an audit trail of:

- All the life cycle stages and use of the certification keys of the SK;
- All life cycle stages of the client's keys;
- All security events, such as user authorizations or failed attempts of authorization;
- The activities of system users with special rights.

The SK uses information security solutions confirming with the standards, which ensure non-recording of private keys, activation codes, access codes (e.g. PIN) or other security critical information in the audit trail.

All incidents, emergencies and problems are registered and, depending on their importance and nature, forwarded for further processing as established with the rules of internal procedures of the SK.

Audit trails are in the SK's information system for not less than 36 months.

The SK ensures with all IT and organizational means the integrity, storage and confidentiality of an audit trail.

The SK has established a procedure for regular analysis of the audit trails and detection of a possible attack.

4.7.3. Secure Log System

The SK has a special Secure Log System applied in its information system providing for sequential integrity of log records by using cryptographic methods. The following information is recorded in the Secure Log System:

- All changes in certificate validity (activation, suspension, termination of suspension, revocation);
- All certificate validity confirmations issued by the SK.

For non-repudiation purposes, a Secure Log System log record is published in at least one national newspaper and the SK's webpage at least once a year.

Secure Log System provides for the audit-ability of certificate validity information. An application in the SK's webpage allows user to securely view changes in validity of his/her certificate and list validity confirmations issued to his/her certificates.

4.8. Action in an Emergency Situation

The SK has carried out a risk analysis of the SK's certification system to prevent possible danger on the availability of the SK's operations.

In supplying the service the SK uses technical means and information system security methods to minimize the risk of losing control of the certification service.

The SK establishes internal rules, instructions and recovery plans for acting in emergency situation in order to ensure security and quality of service provisioning.

The SK's information system and the documentation used are audited by an independent auditor.

The following situations are considered as emergency situations in provisioning of certification service:

- Private key used for provisioning of the SK certification service is compromised or there is a serious suspicion of thereof;
- Destruction of the SK's certificate database;
- Complete or partial destruction of the building containing the data processing centre (server room);
- Failure of the communications channel connecting the data processing centre (server room) with the public data communications network yielding to discontinuation of the service;
- Failure in the power, conditioning system or water supply in the data processing centre (server room);
- Open fire in the SK bureau or data processing centre (server room);
- Technological attack targeted at blocking the service;
- Simultaneous disability of a considerable number of key personnel.

Recovery plans are developed for above-listed situations.

Recovery from above-listed situations and restoration of service is performed according to the current SK's regulation on resolving emergency situations and according to recovery plans mentioned above.

Other emergency situations are resolved according to the current SK's regulation on resolving emergency situations.

Minimal quality requirements for action in the event of *Force Majeure* are stipulated in the action plans.

In the event of an emergency the SK shall inform all the service users immediately, but in any event not later than within the following workday, of the emergency situation and planned solution through public information communication channels.

If the emergency caused any change in the contents of the certificate database, or issuance, suspension, suspension termination or revocation of a certificate, the SK shall immediately, but in any event not later than within the workday following the occurrence, restore the status of the certificate database and inform the certificate holders of such action on its website.

4.9. Termination of Certification Service Provider Operations

Certification service is terminated:

a) With a decision of the SK Supervisory Board;
b) With a decision of the authority exercising supervision over the supply of the service;
c) With a judicial decision;
d) Upon liquidation or termination of operations of AS Sertifitseerimiskeskus.

Upon termination of the certification service, the SK shall hand over the documentation related to the supply of the service to the Registry of Certification Services pursuant to the established procedure.

The notice of termination of the SK's service shall be published on the website of the SK at http://www.sk.ee.

In addition to the requirements prescribed by the Digital Signatures Act, the SK shall revoke all the issued and valid certificates.

Any hardware appliances possessed by the SK shall either be reinitialized or destroyed, depending on the security regulations.

The SK does not assume liability for any loss or damage sustained by the user of the service as a result of such termination provided that the SK has given the notice of termination through public information communication means at least 1 month in advance.

5. Physical and Organizational Security Measures

5.1. Security Management

In the field of security management the SK guides itself by the generally recognized standards, e.g. ISO 13335, ISO 13569.

The administration of the SK establishes security policy, which forms a basis for consistency and completeness of information security and administration support.

The SK manages the register of information property and classifies all information property into security classes according to the results of the security analysis. A responsible person has been appointed for all important information properties.

Compliance with the SK's information security documents is inspected in the course of regular audits by an independent auditor.

5.2. Physical Security Measures

5.2.1. SK Physical Entrance Control

Entrance to the SK's premises is restricted.

The premises of the SK are guarded by physical or electronic security systems.

The employees of the SK may enter the data processing centers of the SK only on the basis of an approved list. A log is kept for recording all entries to the data processing centre of the SK.

Portable media, appliances and software may be removed from the premises of the SK pursuant to the established procedure. Data media containing sensitive information may be stored only in a special fireproof safe designed for storing data media.

5.3. Requirements for Work Procedures

The information systems of the SK are used only for their intended purpose.

For development and testing purposes an independent information system, which has been totally isolated from the work system, shall be used along with totally independent private keys, passwords, codes and other access attributes.

5.3.1. Performance of Essential Operations

5.3.1.1. Shared control

Activation of the SK's certificate and private key used for verification of certificates is carried out on the basis of shared control. Relevant control measures shall be established by the rules of internal procedure of the SK.

5.3.1.2. Documentation of Procedures

An act is compiled about procedures which are regarded as important from the aspect of security. These procedures shall include at the least the following:

- All stages of the life cycle and uses of the SK's root key;
- All stages of the life cycle of the SK's service certificates;
- Solutions to emergency situations.

5.4. Personnel Security Measures

An employee engaged in the provision of the services described in this CPS may not have been punished for a willful crime. The employees shall have received adequate training and have all necessary experience for carrying out the duties specified in the employment contract and job description.

The employment contracts signed with the employees of the SK provide for an obligation to maintain the secrecy of confidential information that has come to their knowledge in the course of their performance for at least five years after termination of the employment contract.

The employees of the SK may not hold business interests in a competing company, which may affect their judgment in the supply of the service.

The employees of the SK shall have job descriptions which specify their following security critical roles:

- Chief of information security: responsible for drafting and implementing information security policy;
- System administrator: responsible for the installation, configuration and maintenance of the information system of the SK; does not have access to the security critical information;
- System operator: responsible for daily maintenance of the information system of the SK, including for making backup copies and restoration of the system;
- Internal auditor: has the right to monitor the document archives and information system audit trails.

Security-critical information is defined as information allowing for simulation or replication of service, or well as destruction or publication of the service private key.

At least the roles of the chief of information system, internal auditor and system administrator shall be fully separated and staffed with different persons.

6. Technical Security Measures

6.1. Key Management

6.1.1. Certification Keys of SK

6.1.1.1. Creating Certification Keys of SK

Upon provision of certification service the RSA algorithm keys are used with the following minimum lengths:

- The SK's certification key - 2048 bits;
- Private Key corresponding to the certificate - 1024 bits.

The certification keys of the SK, which are required for the provision of the certification service, are created in accordance with the internal regulations of the SK: "Procedure for Creating the SK Root Key" and "Procedure for Creating Keys for Intermediate Certification Authorities." Creation of the SK's keys is observed by a commission, which after the creation of the keys draws up an appropriate deed containing the certificate public key of the created pair of keys and hash of thereof. The deed of creating the keys is published on the website of the SK.

6.1.1.2. Protection of Keys

To meet the availability requirements, a backup copy shall be made of the SK's certification keys. The key is divided into three parts that are secured by different persons. A security envelope is used for storing the certification key of the SK and the opening of this envelope can be established.

The certification keys of the SK can be used only when they are activated. For activation of the certification key of the SK the presence of at least two authorized persons is required.

The certification keys of the SK are deactivated when an attempt is made to open the security module used for storage of the keys, when the configuration is changed, the power supply is disconnected or transferred or in other events endangering the security.

The security modules used in providing the certification service shall at least meet requirements established in security standard FIPS PUB 140-1 Level 3.

6.1.1.3. Destroying the certification keys of SK

All copies of the private keys of the SK are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

6.1.2. Client Keys

6.1.2.1. Creating Client Keys

The Client keys are created in accordance with the principles set out in the Certificate Policy.

The keys of the Client shall be protected with the PIN or the activation codes known only to the Client.

6.1.2.2. Protection of Client's Private Key and Activation Codes during Preparation Period

If the Client's private keys are generated by the SK, the confidentiality of the Client's private key and activation codes, as well as prevention of unauthorized use thereof until their being handed over to the Client, shall be guaranteed.

The activation codes are printed in one copy. Activation codes are protected in such way that it is impossible to read them without breaking security element. The Client has prerogative to refuse from accepting of activation codes with altered security element.

The SK shall assume no liability for maintaining the confidentiality of the client's key or its activation code, if the client's keys are generated by the client itself or by a third party that has assumed relevant responsibility.

6.1.2.3. Activation of Client's Private Key

Each actual use of the client's private key assumes entry of the activation code. It must be possible to create different activation codes for different keys of the client.

The activation codes shall meet the following conditions:

- Activation codes must be changeable by the Client;
- The length of the activation codes must not be less than 4 symbols;
- The integrity of the software and hardware components dealing with the activation codes must be guaranteed;
- Entrance of the activation codes must be hidden if possible from third persons;
- At the time of activating a private key, the client must be aware of the operation in progress: the contents of the signed document must be presented while giving the digital signature.

For the purposes of this CPS, the SK bears no liability for the security upon activation of the client's private key.

6.1.2.4. Destruction of Client's Keys

Destruction of the client's keys has been regulated in the relevant Certificate Policy. If the SK has made backup copies of the client's keys, the SK shall destroy such keys after expiry or revocation of the certificate.

6.1.2.5. Backup and Deposition of Client's Keys

No backup copies of the Client's private keys are made or deposited if the relevant private key is used for digital signing. In other cases the Client's keys may be deposited or backed up upon request of the Client or if such service has been prescribed by the Certificate Policy.

6.2. Logical Security

6.2.1. Access Control

The SK shall implement an access control system which identifies, authorizes and registers trustworthily all the SK's information system users, as well as the employees of the SK's Client Service Point.

6.2.2. Software Security

In the information system of the SK, including in all workstations, measures for guaranteeing the integrity of software and configurations, as well as for detection of fraudulent software and restricting its spread, are implemented.

Only the software directly used for performing the tasks is used in the information system. The software shall be approved by the Chief of Information Security and originate from a reliable source.

6.2.3. Network Connection Security

The transfer of sensitive information in the SK's external network is encrypted.

The cabling and active equipment along with their configuration in the SK's internal network are protected with physical and organizational measures.

The security of the SK's internal network and external connections are constantly monitored.

6.2.4. Time Synchronization

The maximum allowed time variance in all parts of the certification system is 1 second.

This is guaranteed by an internal Reference Clock service, according to which the chronologies of all parts of the certification system are synchronized.

The Reference Clock uses GPS (Global Positioning System) as a primary time source which determines preciseness of the time in the SK's system.

6.3. Description of Technical Means Used for Certification

The SK provides the certification service with Unicert software certified by Baltimore Technologies ITSEC-3. The certificates are issued in a secure network segment in the so-called CA Certification Authority's module of the certification server designated only for that purpose and being situated in the product environment.

The CA certification module is operated via the CAO operator's module, which may be used only by authorized operators and with the help of a console at the certification server. For secure storage of certification module's private keys a security module is used and it corresponds to the FIPS Pub 140-1 Level 3 standard.

Applications for the certificate are processed in a designated RA registration module in which the ARM registration operator with expanded possibilities is used.

6.4. Storage and Protection of Information Created in Course of Certification

The SK shall electronically store and record any information on certificates and activities related to the change of their status. Backup copies of this information are stored securely in two different locations.

Data protection principles can be found in the document titled “Principles of Personal Data Protection”. The SK shall store the information created in the course of certification until the termination of its activities.

7. Technical Profiles of Certificates and Revocation Lists

7.1. Profiles of Certificates

Certificate profiles have been published or referred to in relevant Certificate Policy documents.

The certificate profiles of the Certification Authorities have been introduced in the document tiled "CA Certificate Profiles of AS Sertifitseerimiskeskus."

A certificate profile must be composed in accordance with the requirements of RFC 3280 [6].

7.2. Revocation Lists (CRL)

The SK shall issue the revocation lists in accordance with the requirements established by RFC 3280 [6]. If necessary, the Certificate Policy may specify the requirements of the CRL-s.

8. Management of Certification Practice

Amendments which do not change the meaning of the certification practice, such as corrections of misspellings, translation and updating of contact details, shall be documented in the Versions and Changes section of the present document and the fraction part of the document version number shall be enlarged.

In the case of substantial changes, the new certification practice version shall be clearly distinguishable from the previous ones. The new version shall bear a serial number enlarged by one. The amended Certification Practice Statement along with the enforcement date, which cannot be earlier than 30 days after publication, shall be published electronically on the SK's website.

All amendments shall be coordinated with the Registry of Certification Services.

9. References

[1] Public Information Act, RT I 2000, 92, 597
[2] Digital Signatures Act, RT I 2000, 26, 150
[3] Personal Identification Documents Act, RT I 1999, 25, 365
[4] Personal Data Protection Principles, AS Sertifitseerimiskeskus
[5] Personal Data Protection Act, RT I 2007, 24, 127
[6] RFC 3280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile
[7] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

10. Glossary

In this CPS the following terms have the following meaning. The definition of the terms need not coincide with the definitions given in the Digital Signatures Act.

Keyword	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate	According to the DSA a document which has been issued to facilitate digital signing being enabled and the public key of which is uniquely consistent with a definite physical person. Besides DSA, certificate can be issued to legal persons and can be used for other purposes too.
Certificate Authority	A part of the SK structure issuing and verifying with its digital signature digital certificates and revocation certificates.
Certificate Policy	A set of rules that determine the field of use of issued certificates and security requirements implemented.
Certification Practice Statement	A set of regulations and conditions that guide the SK while providing the certification service.
Certification service	Issuing certificates, facilitating verification of a digital signature given on the basis of certificates and managing the suspension of certificates' validity, termination of suspension and revocation.
Chip card	A technical appliance for storing private keys and certificates. The private key never leaves the chip card.
Client	A physical person, holder of personal certificate.
Client Service Point	A service point of the SK operating on the basis of the certificate policy following the requirements of this CPS with the aim of providing services related to the certificate service.
Digital signature	Data added to the database or applied transformation allowing the receiver of the data to establish the source and integrity of the data and protect him/her against fraud.
Directive	Directive of the EU Commission "Directive 1999/93/Ec of the European Parliament and of the Council".
Directory Service	Certificate validity information publication service.
Distinguished name	A unique identifier uniquely identifying an object.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
Hash Function	Mathematical variation on the basis of which a message (any array) corresponds to a fixed length array – message abbreviation. It is hard to find two different messages with corresponding message abbreviations.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	Unique identification number describing an object, e.g. for certificate policy and certification practice identification.
Personal Certificate	A digital certificate issued to a physical person
Private key	An encryption key in the possession of a person which can be used to prove his/her identity (means of digital signing).
Public Key	Means of verifying the digital signature.
Relying Party	The party who passes a decision on the basis of a digital signature.
Revocation list	A list of invalid (revoked, suspended) certificates.

Keyword	Definition
Security event	An event that may (or may not) result in a loss or damage to an organization's property, or an operation that contravenes security procedures of an organization.
System user with special rights	System Administrator; user of a computer system who is not subject to standard limitation of rights to facilitate system management.

11. Abbreviations

Abbreviation	Definition
CA	Certification Authority
SK	AS Sertifitseerimiskeskus, provider of the certification service
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSA	Digital Signatures Act of the Republic of Estonia
RCS	Registry of Certification Services
OID	Object Identifier, a unique object identification code
PIN	Personal Identification Number, a security code consisting of 4 -12 digits used for activating a private key before every use.
RA	Registration Authority, a part of the SK's structure that accepts certificate applications, checks the applications and/or forwards the applications to the CA.
RT	Riigi Teataja, official publication for legal documents of the Republic of Estonia.
URI	Unified Resource Identifier