

AS Sertifitseerimiskeskus
Certification Practice Statement CPS

Version 2.1

07.10.2002

Versions and Changes:

Version	Date	Comments
1.0	31.08.2001	The first version
2.0	01.02.03	Redesigned into universal source document for various certification policies: <ul style="list-style-type: none">• The CA structure of the CC 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 and layout have been elaborated, inessential provisions have been omitted.
2.1.	07.10.2002	Section "Secure Log System" (4.7.3) is added

Table of Contents

TABLE OF CONTENTS	3
1 INTRODUCTION.....	6
1.1 GENERAL SURVEY	6
1.2 ORGANISATION AND AREA OF APPLICATION	7
1.2.1 Certification Centre (CC)	7
1.2.2 Registration Centre.....	7
1.2.3 User.....	8
1.2.4 Area of Application of Certificates	8
1.3 CONTACT DETAILS	9
2 GENERAL CONDITIONS.....	9
2.1 OBLIGATIONS.....	9
2.1.1 Obligations of CC.....	9
2.1.2 Requirements to Registration Centre.....	10
2.1.3 Obligations of Clients	10
2.1.4 Obligations of Relying Party	11
2.1.5 Obligations of Directory Service	11
2.2 LIABILITY	12
2.2.1 Liability of CC.....	12
2.2.2 Liability of Registration Centre	12
2.2.3 Limits of Liability.....	12
2.3 SETTLING DISPUTES	12
2.4 PUBLICATION OF INFORMATION AND DIRECTORY SERVICE	13
2.4.1 Publication of Information by CC.....	13
2.4.2 Publication Frequency.....	13
2.4.3 Rules of Access.....	13
2.4.4 Directory Service	13
2.5 AUDIT	13
2.6 CONFIDENTIALITY.....	14
2.6.1 Confidential Information	14
2.6.2 Public Information.....	14
2.6.3 Protection of Personal Data	15
3 CLIENT IDENTIFICATION.....	15
3.1 IDENTIFICATION OF CLIENT	15
3.2 PROCEDURE OF CERTIFYING CORRESPONDENCE OF APPLICANT’S PERSONAL KEY TO PUBLIC KEY	15
3.3 DISTINGUISHED NAME	15
4 PROVIDING CERTIFICATION SERVICE. PROCEDURE AND TERMS OF CERTIFICATION PROCESS.....	15
4.1 SUBMISSION OF APPLICATIONS FOR CERTIFICATES.....	15
4.2 PROCESSING OF APPLICATIONS FOR CERTIFICATES.....	16
4.2.1 Decision Making	16
4.2.2 Issuing Certificates	17

4.2.3	<i>Procedure for Registration of Certificates</i>	17
4.2.4	<i>Certificate Check-up and Verification</i>	17
4.2.5	<i>Certificate Renewal</i>	17
4.3	APPLICATIONS FOR SUSPENSION AND REVOCATION OF CERTIFICATES	18
4.3.1	<i>Establishment of Authority to Apply for Suspension or Revocation of Certificates</i>	18
4.3.2	<i>Exclusion of Misuse of Revoked, Suspended or Expired Certificate</i> ...	19
4.3.3	<i>Consequences of Illegal Revocation</i>	19
4.4	SUSPENSION OF CERTIFICATES	19
4.4.1	<i>Conditions and Procedure of Suspension</i>	19
4.5	TERMINATION OF SUSPENSION	21
4.5.1	<i>Conditions of Termination of Suspension</i>	21
4.5.2	<i>Authority to Terminate Suspension</i>	21
4.5.3	<i>Application for Termination of Suspension</i>	21
4.5.4	<i>Procedure of Termination of Suspension</i>	22
4.5.5	<i>Effect of Termination of Suspension</i>	22
4.6	CERTIFICATE REVOCATION	22
4.6.1	<i>Authority to Revoke Certificates</i>	22
4.6.2	<i>Submission of Application for Revocation</i>	22
4.6.3	<i>Procedure of Revocation</i>	23
4.6.4	<i>Effect of Revocation</i>	23
4.7	PROCEDURES ENSURING TRACKING.....	23
4.7.1	<i>Preservation of Documents</i>	23
4.7.2	<i>Activities Leaving Audit Trail</i>	24
4.7.3	<i>Secure Log System</i>	24
4.8	ACTION IN AN EMERGENCY	25
4.9	TERMINATION OF CERTIFICATION SERVICE PROVIDER OPERATIONS	25
5	PHYSICAL AND ORGANISATIONAL SECURITY MEASURES	26
5.1	SECURITY MANAGEMENT	26
5.2	PHYSICAL SECURITY MEASURES	27
5.2.1	<i>CC Physical Entrance Control</i>	27
5.3	REQUIREMENTS FOR WORK PROCEDURES.....	27
5.3.1	<i>Performance of Essential Operations</i>	27
5.4	PERSONNEL SECURITY MEASURES.....	27
6	TECHNICAL SECURITY MEASURES	28
6.1	KEY MANAGEMENT	28
6.1.1	<i>Certification Keys of CC</i>	28
6.1.2	<i>Client Keys</i>	29
6.2	SYSTEM SECURITY	30
6.2.1	<i>Access Control</i>	30
6.2.2	<i>Software Security</i>	30
6.2.3	<i>Network Connection Security</i>	31
6.2.4	<i>Time Synchronisation</i>	31
6.3	DESCRIPTION OF TECHNICAL MEANS USED FOR CERTIFICATION.....	31
6.4	STORAGE AND PROTECTION OF INFORMATION CREATED IN COURSE OF CERTIFICATION	31

7	TECHNICAL PROFILES OF CERTIFICATES AND REVOCATION LISTS (CRL)	32
7.1	PROFILES OF CERTIFICATES	32
7.2	REVOCATION LISTS (CRL)	32
8	MANAGEMENT OF CERTIFICATION PRACTICE	32
9	REFERENCES	33
10	GLOSSARY	33
11	ABBREVIATIONS	34

1 Introduction

AS Sertifitseerimiskeskus (hereafter CC) was founded on 16 February 2001. The owners of the limited liability company by equal shares of 25 percent are Hansapank, Eesti Ühispank, AS Eesti Telefon 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 concrete needs and economic aspects.

1.1 General Survey

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

This certificate policy extends only to digital certificates issued by AS Sertifitseerimiskeskus.

This CPS serves as a basis for framing different certificate policies and corresponding certification services offered by AS Sertifitseerimiskeskus.

This CPS has been registered in the Public Register of Certificates (PRC). All the certification policies issued under this CPS, which facilitate issue of certificates for digital signing within the meaning of the Digital Signatures Act, have been also registered in the PRC.

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

Reference has been made to this CPS in the Policy Qualifier field of the root certificate of AS Sertifitseerimiskeskus.

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.

1.2 Organisation and Area of Application

1.2.1 Certification Centre (CC)

The CC provides certification services in accordance with the certificate policy devised on the basis of this CPS along with related additional services (directory service).

The certification service provided by the CC 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 CC is entitled to conclude contracts, by which duties and assignments are delegated to third parties. Delegated duties 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 the certificate policies of CAs administered by the CC. The certificate policy of the relevant CA specifies the principles set out herein. In the case of conflict between this CPS and a concrete certificate policy the provisions of the certificate policy shall prevail.

The OIDs of the certificate policies have been indicated in the extension of the certificate policy key of relevant authority.

1.2.2 Registration Centre

1.2.2.1 CC Client Service Point (CSP)

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

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

The CC Client Service Points may vary with different certificate policies. The relationship between the CC Client Service Point and the CC is regulated by a bilateral agreement(s).

For information on the CC Client Service Points and their contact visit the CC's website.

1.2.2.2 Help Line

The Help Line shall act as the representative of the CC in the field of client telephone servicing and accept from clients and other parties applications for suspension of

certificates 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 CC'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 certificate issued on the basis of the certificate policy devised on the basis of this CPS.

A Client's distinctive name 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 CC shall ensure the uniqueness of the combination of the client's distinctive name and issuer name.

1.2.3.2 Relying Party

A Relying Party is a party who takes a decision relying on the certificate issued by the CC.

A relying party:

- takes account of the principles set out in the policy of a concrete certificate, this CPS and documents referred to therein or herein;
- verified the validity of the certificate in the public directory of the CC or the most recent revocation list;
- checks the certificate's correspondence to its area of application;
- in case of certificates facilitating digital signing, checks the completeness of the digitally signed data collection and identifies the signatory;
- checks the validity of a digital signature affixed at an earlier date on the basis of the validity of the certificate at the date of the signature.

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. Relevant limitation mechanisms are described in the certificate policy, which serves as a basis for issuing certificates. 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 CC 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-mail: pki@sk.ee
<http://www.sk.ee/>

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

2 General Conditions

2.1 Obligations

2.1.1 Obligations of CC

The CC 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 CC hereby undertakes to:

- publish its Certification Practice Statement 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 documents related to certification until termination of its activity;

- ensure an annual audit of the information system and present the auditor's report to the authorised employee of the state register of the certification service;
- publish the terms of the compulsory insurance policy in a public data communications network.

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

2.1.2 Requirements to Registration Centre

2.1.2.1 Obligations of Client Service Points

A Client Service Point shall accept applications for 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 check the powers and authority of the person submitting the application.

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

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

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

2.1.3 Obligations of Clients

A Client shall observe the procedures provided by the CC 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 CC may refuse to issue a certificate if the Client has knowingly 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 CC.

A client shall immediately inform the CC of a possibility of unauthorised 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 personal 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 concrete 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 the revocation list valid at the time of using the certificate or affixing a digital signature.

A Relying Party shall follow the limitations included in 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 give the clients, relying parties and other persona 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 must shall be accessible in a public data communications network 24 hours a day
- ✓ Security measures must be implemented to prevent directory service simulation and ensure integrity of the information.

2.2 Liability

2.2.1 Liability of CC

The CC 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 Liability of Registration Centre

2.2.2.1 Liability of Client Service Point

A CSP 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 CC 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 CC is not liable for the non-performance of its obligations, if such non-performance is due to faults or security problems of the Public Register of Certificates, data protection supervision authority or any other public authority.

Non-fulfilment of the obligations arising from the Certification Practice Statement is not considered a violation if such non-fulfilment is occasioned by *Force majeure*.

2.3 Settling Disputes

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 CC.

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 CC

The archives of the CC's valid and other root certificates is published on the following website: <http://www.sk.ee/certs>

The certificates valid and issued by the CC are published in a public directory. The revocation lists are published on the same website.

All documents directly related to the operation of the CC are accessible in a public data communications network at the following address: <http://www.sk.ee/cps/>

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

2.4.2 Publication Frequency

The CC shall publish all issued certificates in a public directory immediately.

Certificate revocation lists are published pursuant to the procedure provided in the certificate policy. After suspension or invalidation of a certificate, the related revocation list shall be published in the public directory.

The CC 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 a public data communications network is free of charge and access is unrestricted. In the case of other manners of publication the CC 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 CC are published in the certificates directory at the address `ldap://ldap.sk.ee`. Copies of the revocation lists are available on the website <http://www.sk.ee/crls/>.

The structure of the directory and the instructions for the use thereof have been listed on the website of the CC.

2.5 Audit

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

- ✓ The operations and activity of the CC 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.
- ✓ Once every quarter, an internal audit shall be carried out by the centre’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 CC’s operations and procedures
- d) protection of the data of the CC’s clients and the CC’s security policy, performance of work procedures and contractual obligations, as well as compliance with the CPS.

2.6 Confidentiality

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 CC) 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.

All business partners of the CC have signed a mutual non-disclosure agreement.

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;
- CC’s public keys;
- 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 CC's principles of personal data protection have been stipulated in the document titled "Personal Data Protection Principles" [4]. By ensuring the performance of the personal data protection principles the non-disclosure of confidential information not subject, relevance of the client information as well as performance of the Personal Data Protection Act [5] and Databases Act shall be guaranteed.

3 Client Identification

3.1 Identification of Client

The Client shall be identified in accordance with the provisions of the certificate policy and of the Identification Documents Act [3].

3.2 Procedure of Certifying Correspondence of Applicant's Personal Key to Public Key

The procedure of certifying the correspondence of the applicant's personal key to the public key can be found in the certificate policy.

3.3 Distinguished Name

The client's distinguished name is coined in accordance with the profile of the certificate and revocation list defined in the certificate policy.

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

The CC shall record a unique certificate serial number on every issued certificate.

4 Providing 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 CC.

A more detailed procedure for application for the certificates is established by the certificate policy.

The procedure for application for certificates shall at least conform to the following:

- An employee of the Client Service Point shall give the client an application form requisite for the certificate application procedure;
- 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 authorising the CC 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 checked.

4.2.1 Decision Making

The acceptance or rejection of the applications for certificates is the decision of the CC or its contractual partner specified in the certificate policy. The decision shall be made within at least 5 workdays.

Upon decision making the CC or the contractual partner of the CC specified in the certificate policy shall consider:

- whether or not the Client has a right to receive the certificate under Estonian law;
- whether or not the Client has supplied true and complete information about his/her person in the application for the certificate;
- whether or not the Client holds 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 set out in the certificate policy or agreed in the application.

4.2.2 Issuing Certificates

The CC shall, after the establishment of the authenticity and completeness of the application for certificate presented by the Client Service Point of the CC, automatically issue the certificates corresponding to the application. The certificates are delivered upon appearance of the Client at the Client Service Point of the CC for receipt of the certificate.

An issued certificate shall be forwarded to the Client according to the certificate policy.

The Client shall be identified before the issuance of the certificate.

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 CC.

At the time of certificate issuing, the certificate's copy is saved in a certificate directory accessible through a public data communications network to all service users 24 hours a day. 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 management requirements.

4.2.4 Certificate Check-up and Verification

Upon request of a Relying Party, the representative of the CC 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 CC.

The data formats, service charges and time limits of the certificate verification service are established by the CC. The exact terms and conditions are published on the CC'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 invalidation 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 3.

Table 1. 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 CC 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 CC.	Certificate is suspended if the check-up questions about personal details were answered correctly.	Not accepted	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
In the public data communications network using the application available on the website of the CC http://www.sk.ee	Certificate is suspended if the check-up questions about personal details were answered correctly.	Not accepted	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
In the public data communications network authenticated in the application available on the website of the CC http://www.sk.ee	Suspended.	Not accepted	Suspended.
Upon presentation of a personal identification document in a Client	Suspended.	Suspension is terminated	Revoked.

Method of Submission of Application	Application for Suspension	Application for Termination of Suspension	Application for Revocation
Service Point of the CC.			

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 CC.

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 CC or its contractual partner named in the certificate policy has reasonable doubts that the certificate contains incorrect data or the personal 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 authorised representative;
- Suspension of the certificate is requested by the data protection supervision authority or a senior processor of the State Register of Certificates in the case of reasonable doubt that the certificate contains incorrect data or the personal 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:

- A client (certificate holder);
- A senior executive of the CC or its contractual partner named in the certificate policy;
- Senior processor of the State Register of Certificates;
- An authorised public servant named in the DSA 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 CC.

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 CC.

Upon registration of an application the data of the document used for identification of the person submitting the application shall be recorded.

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 CC, 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 call is registered by the Help Line operator or suspension is registered by an employee of the Client Service Point of the CC;
- the data related to the person filing an application for suspension are checked;
- the compliance of the application for suspension of the certificate with the certificate policy is verified in an information system of the CC;
- the application for suspension is registered in the information system of the CC;
- 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 materials on which the applications for suspension were based are archived.

4.4.1.5 Effect of Suspension

The suspension of the certificate is immediately recorded in the certificate database of the CC.

Following the suspension, the CC 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 State Register of Certificates
- A senior executive of the CC or its contractual partner named in the certificate policy;
- According to the DSA, 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 CC.

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 CC that has issued the suspended certificate;
- Grounds for termination of suspension;

If the request was not filed by the certificate holder but by an authorised official or senior executive of the CC, the documents authorising 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 CC;
- 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 CC;
- The fact of termination of suspension is registered in the information system of the CC;
- The certificate is published anew in a public directory;
- A new CRL is published in accordance with the provisions of clause 2.4.2.

After registration of the request for termination of suspension the client shall be notified of the moment at which no valid CRL restricts the use of the certificate. The client has a possibility to establish on the basis of the directory or CRL whether a certificate is active or not.

4.5.5 Effect of Termination of Suspension

The suspension of the certificate is immediately recorded in the certificate database of the CC. Following the termination of suspension, the CC 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 duly authorised 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 CC 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 CC 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 CC;
- The truth and correctness of the application for revocation is established in the information system of the CC;
- The application for revocation is registered in the information system of the CC;
- 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 materials on which the application for revocation was based shall be archived.

The client has a possibility to ascertain on the basis of a public catalogue 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 CC. After revocation of the certificate, the CC 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 CC 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 CC's activity, unless the law provides otherwise.

If the CC 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 CC's activity all the documents facilitating digital signing shall be delivered to the State Register of Certificates in accordance with law and pursuant to the established procedure.

4.7.2 Activities Leaving Audit Trail

The CC's information systems leave an audit trail:

- Of all the life cycle stages and use of CC certification keys;
- Of all life cycle stages of the client's keys;
- Of all security events, such as user authorisations or failed attempts of authorisation
- Of the activities of system users with special rights.

The CC uses standard informational protection solutions, which ensure non-recording of personal 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 procedure of the CC.

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

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

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

4.7.3 Secure Log System

The CC 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 confirmation issued by CC

For non-repudiation purposes, a Secure Log System log record is published in printed media and CC's webpage at least once a year.

Secure Log System provides for the auditability of certificate validity information. An user interface in CC's webpage is allowing for verification of existence of previously issued certificate validity confirmation in the Secure Log System of CC.

4.8 Action in an Emergency

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

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

The CC has drafted the following internal documents: "Management Information Security Policy of AS Sertifitseerimiskeskus," "Management Strategy and Policy of AS Sertifitseerimiskeskus," "IT System Restoration Policy of AS Sertifitseerimiskeskus" and special guidelines and restoration schemes for emergency operations with the aim of securing the security and quality of the service. The information system and the documents used have been audited by an independent auditor.

These guides and restoration schemes comprise action plans for the following emergencies:

- Disclosure or suspected disclosure of the CC's certification key;
- Possible imitation of CC's operations;
- Destruction of the personal key of a CC functionary;
- Destruction of the CC's certificate database;
- Imitation or suspected imitation of the CC's service;
- Complete or partial destruction of the building containing the data processing centre;
- Failure of the communications channel connecting the data processing centre with the public data communications network;
- Failure in the power or water supply to the production environment;
- Information technology attack targeted at blocking the service;
- Simultaneous disability of a considerable number of personnel.

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

In the event of an emergency the CC 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 CC 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:

- 1) with a decision of the CC;
- 2) with a decision of the authority exercising supervision over the supply of the service;
- 3) with a judicial decision;
- 4) upon liquidation or termination of operations of AS Sertifitseerimiskeskus.

Upon termination of the certification service, the CC shall deliver the documentation related to the supply of the service to the State Register of Certificates pursuant to the established procedure.

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

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

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

The CC 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 CC has given the notice of termination through public information communication means at least 1 month in advance.

5 Physical and Organisational Security Measures

5.1 Security Management

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

The administration of the CC has compiled the information security concept, which forms a basis for consistency and completeness of information security and administration support.

The CC 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 CC's information security documents is inspected in the course of regular audits by an independent auditor.

5.2 Physical Security Measures

5.2.1 CC Physical Entrance Control

Entrance to the CC's premises is restricted.

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

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

Portable media, appliances and software may be removed from the premises of the CC 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 CC 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 personal keys, passwords, codes and other access attributes.

5.3.1 Performance of Essential Operations

5.3.1.1 Shared control

Activation of the CC's certificate and personal 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 CC.

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 CC's certification key;
- 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 CC 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 10 years after termination of the employment contract.

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

The employees of the CC 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 CC; does not have access to the security critical information;
- System operator: responsible for daily maintenance of the information system of the CC, 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.

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 CC

6.1.1.1 Creating Certification Keys of CC

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

- The CC's certification key - 2048 bits
- Secret key corresponding to the certificate - 1024 bits

The certification keys of the CC, which are required for the provision of the certification service, are created in accordance with the internal regulations of the CC: "*Procedure for Creating CC Root Key*" and "*Procedure for Creating Keys for Subsilog Certification Authorities.*" Creation of the CC'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**. The deed of creating the keys is published on the website of the CC.

6.1.1.2 Protection of Keys

To meet the management requirements, a backup copy shall be made of the CC'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 CC and the opening of this envelope can be established.

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

The certification keys of the CC 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 meet the requirements established in security standard FIPS PUB 140-1 Level 3.

6.1.1.3 Destroying the certification keys of CC

All copies of the personal keys of the CC 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 personal keys are generated by the CC, the confidentiality of the Client's personal key and activation codes, as well as prevention of unauthorised use thereof until their being handed over to the Client, shall be guaranteed.

The activation codes are printed in one copy directly into the security envelope that is handed over to the Client unopened.

The CC 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 Secret Key

The actual use of the client's personal 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 and more than 12 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 personal 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 CC bears no liability for the security upon activation of the client's secret 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 CC has made backup copies of the client's keys, the CC 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 personal keys are made or deposited if the relevant personal 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 System Security

6.2.1 Access Control

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

6.2.2 Software Security

In the information system of the CC, 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 CC's external network is encrypted.

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

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

6.2.4 Time Synchronisation

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 chronology of all parts of the certification system are synchronised.

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

6.3 Description of Technical Means Used for Certification

The CC 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 authorised 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.

The directory service is provided with the help of *iPlanet*'s directory service server named *iPlanet Directory Server*.

The certification service is provided using SUN servers and IBM-type workstations.

6.4 Storage and Protection of Information Created in Course of Certification

The CC 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 CC shall store the information created in the course of certification until the termination of its activities.

7 Technical Profiles of Certificates and Revocation Lists (CRL)

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 titled “CA Certificate Profiles of AS Sertifitseerimiskeskus.”

A certificate profile must be composed in accordance with the requirements of RFC 2459 [6].

7.2 Revocation Lists (CRL)

The CC shall issue the revocation lists in accordance with the requirements established by RFC 2459 [6].

If necessary, the certificate policy may specify the requirements of the CRLs.

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 Amendments’ 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 CC’s website.

All amendments shall be coordinated with the State Register of Certificates.

9 References

- [1] Databases Act, RT 1 1997, 28, 423
- [2] Digital Signatures Act of the Republic of Estonia, RT 1 2000, 26, 150.
- [3] Personal Identification Documents Act L, RT 1 1999,25,365
- [4] Directive of the EU Commission “*Directive 1999/93/Ec of the European Parliament and of the Council*”
- [5] Personal Data Protection Principles, AS Sertifitseerimiskeskus
- [6] Personal Data Protection Act RT 1 1996, 48, 944.
- [7] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
- [8] 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.

Key Word	Definition
Authenticate	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 CC 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 CC 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 personal keys and certificates. The personal key never leaves the chip card.
Client	A physical person, holder of personal certificate
Client Service Point	A service point of the CC operating on the basis of the certificate policy following the requirements of this CPS

Key Word	Definition
	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 “ <i>Directive 1999/93/EC of the European Parliament and of the Council.</i> ”
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	(OID)– 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
Personal 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 (CRL)	A list of invalid (revoked, suspended) certificates.
Security event	An event that may (or may not) result in a loss or damage to an organisation’s property, or an operation that contravenes security procedures of an organisation.
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
CC	AS Sertifitseerimiskeskus, provider of the certification service
CP	Certificate Policy
CPS	Certification Practise Statement
CRL	Certificate Revocation List
DSA	Digital Signatures Act of the Republic of Estonia

OID	Object Identifier, a unique object identification code
PIN	Personal Identification Number, a security code consisting of 4 - 12 digits used for activating a personal key before every use. Revealing the PIN equals personal key disclosure.
RA	Registration Authority, a part of the CC's structure that accepts certificate applications, checks the applications and/or forwards the applications to the CA.
RT	<i>Riigi Teataja</i> , official publication for legal documents of the Republic of Estonia
SRC	State Register of Certificates
URI	Unified Resource Identifier