Certificate Policy of Organisation Certificates

Version 2.5

OID: 1.3.6.1.4.1.10015.7.1.2.5

Versions and amendments:

Version	Date	Comments
1.0	10.04.2002	First version
1.1.	13.10.2006	Amended version
2.1	13.08.2009	The policy was brought into conformance with the requirements arising from the Digital Signatures Act. The term “appliance certificate” was removed.
2.2	10.05.2010	The following clauses were amended: 1.3.4 – different areas of applications may be combined in one certificate (except digital seal certificate) 4.2.2 – the term “chip card” was replaced with the term “secure signature creation device”
2.3	20.07.2012	The following clauses were amended: 4.6.1 – more granular conditions for certificate revocation
2.4	28.09.2012	The following clauses were amended: 4.2.4 – difference from CPS for validation certificate issuance removed
2.5	21.12.2012	The following clauses were amended:

		2.4.4 – changed the rules of publishing certificates in public directory

Table of contents

1 Introduction

1.1 Overview

This document (hereinafter the "Certificate Policy" or "CP") is a set of rules that establishes major principles and concepts of providing certification services required for issuing organisation certificates.

This CP is based upon the Certification Practice Statement of AS Sertifitseerimiskeskus [1], a document registered in the register of certification service providers. The Certification Practice Statement (hereinafter: CPS) serves as a basis for providing certification services and this CP further specifies the practice described in the CPS.

In the case of contradiction between the CP and the CPS, the provisions of the CP shall have prevalence.

Web server certificates and digital seal certificates for the purposes of the Digital Signatures Act [3] are **special forms** of organisation certificates. A more detailed description is provided in Clause 1.3.4. of this CP.

This document draws upon RFC 2527 [5], an advisory document of the IETF (Internet Engineering Task Force).

1.2 Identification of the Certificate Policy

The identifier of this CP is **OID: 1.3.6.1.4.1.10015.7.1.2.5**

The CP's identifier has been composed according to the following Table 1.

Parameter	Reference in OID
Internet identifier	1.3.6.1
Company identifier	4
Company identifier registered by the IANA, which manages companies	1
Identifier assigned to AS Sertifitseerimiskeskus in the IANA register	10015
Certification service identifier	7.1
CP version identifier	2.5

Table 1. Composition of the CP identifier

1.3 Organisation and Area of Application

1.3.1 Sertifitseerimiskeskus (SK)

See Clause 1.2.1 of the CPS.

1.3.2 Registration Centre

1.3.2.1 Client Service Point

The Client Service Point of the SK is Sertifitseerimiskeskus AS.

1.3.2.2 Help Line

The help line service is not provided under this CP.

1.3.3 User

1.3.3.1 Client

See Clause 1.2.3.1 of the CPS.

On the basis of this CP, certificates are issued to Clients that are legal persons.

A Client is the owner of a certificate issued on the basis of this CP.

One Client may be issued several organisation certificates.

1.3.3.2 Relying Party

See Clause 1.2.3.2 of the CPS.

1.3.4 Area of Application of Certificates

See Clause 1.2.4 of the CPS.
On the basis of this CP, certificates are issued to legal persons with an unlimited area of application. This CP imposes special requirements on the issuing of the following certificates:

- **Web server certificate** – a certificate issued to an HTTPS server to certify the authenticity of the web server's owner;
- **Digital seal certificate** – this certificate is used to certify the integrity of a digital document and to link the holder of the certificate to such document.

A digital seal certificate may be used in accordance with the Digital Signatures Act [3].

Different areas of applications may be combined in one certificate. Digital seal certificates may not be combined with other areas of application.

Upon agreement with a Client, it is allowed to issue specific certificates for which areas of application have not been specified in the certificate profile.

1.4 Contact Details

See Clause 1.3 of the CPS.

2 General Provisions

2.1 Obligations and Requirements

2.1.1 SK Obligations

See Clause 2.1.1 of the CPS.

The SK shall additionally ensure that:

- the supply of the certification service complies with the Certification Practice Statement of AS Sertifitseerimiskeskus;
- the supply of the certification service complies with this CP.

The SK additionally undertakes:

- to accept and satisfy the Client's certificate applications over a secure electronic data communications channel;
- to supply directory service around the clock;
- to ensure that certification keys used for the supply of the certification service are protected by hardware security modules and remain under the control of the SK;
- to revoke all the issued certificates if it has lost control over the certification keys;
- to ensure that all activated certification keys are located in the territory of the Republic of Estonia;
- to ensure that all the certification keys used in the supply of the certification service are activated on the basis of shared control;

2.1.2 Obligations of Registration Centre

2.1.2.1 Obligations of the Client Service Point of the SK

The 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 an employee of the Client Service Point shall identify the person submitting an application and check their powers and authority.

2.1.2.2 Obligations of the Help Line

The Help Line is not provided.

2.1.3 Obligations of Client

See Clause 2.1.3 of the CPS.
A client shall be a registered legal person that is not bankrupt or being liquidated under the law of its home country, the business activities of which have not been suspended and which is not in any similar situation.
The client shall observe the conditions and procedures established by the SK in this CP. The client shall submit true and complete information to the SK and promptly notify the SK of any changes in such information.
The client shall agree with the Terms of Use of Organisation Certificates (TUOC).

2.1.4 Obligations of Relying Party

See Clause 2.1.4 of the CPS.

2.1.5 Obligations of Directory Service

See Clause 2.1.5 of the CPS.

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 Registration Centre Liability

2.2.2.1 Liability of the Client Service Point

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

2.2.2.2 Liability of the Help Line

The Help Line is not provided.

2.2.3 Limits of Liability

See Clause 2.2.3 of the CPS.

2.3 Settling disputes

See Clause 2.3 of the CPS.

2.4 Publication of Information and Directory Service

2.4.1 Publication of Information by SK

See Clause 2.4.1 of the CPS.
The valid revocation list is available through directory service and at http://www.sk.ee/crls/.

2.4.2 Publication Frequency

See Clause 2.4.2 of the CPS.

The revocation list is updated every 12 hours.

2.4.3 Rules of Access

See Clause 2.4.3 of the CPS.

2.4.4 Directory Service

See Clause 2.4.4 of the CPS.

The certificates issued under this CP shall be published in public directory at ldap://ldap.sk.ee.

Suspended and revoked certificates are deleted from the public directory. In case of termination of suspension of certificates, the certificates shall be re-published in the public directory.

Expired certificates shall be deleted from the public directory on the date subsequent to the date of certificate expiry.

2.5 Audit

See Clause 2.5 of the CPS.

2.6 Confidentiality

See Clause 2.6 of the CPS.

3 Client Identification

3.1 Identification of Client

During the procedure of application for an organisation certificate the following is verified:

- The registered status of the client in accordance with legal acts of its home country;
- The identity of the Client's representative;
- The authority of the Client's representative to apply for a certificate on behalf of the Client.

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

To apply for an organisation certificate, the Client shall electronically submit the Certificate Signing Request (CSR) to the SK that includes the public key of the applicant and is signed by the respective personal key. If correspondence of the signing request has been established, the SK may assume that the respective personal key is in the applicant's possession.

If the SK has received from the Client authority to generate a public and private key for the Client, the correspondence is ensured by the internal procedures of the SK and the Client shall not electronically submit to the SK the Certificate Signing Request (CSR).

3.3 Distinguished Name

See Clause 3.3 of the CPS.
The distinguished name of a certificate is composed in accordance with the document "Profiles of Organisation Certificates" [2].

The uniqueness of a distinguished name is not guaranteed in the case of web server certificates.

A web server certificate is assigned a distinguished name on the basis of a link between the Client and the domain name and/or IP address of the Client's appliance if the appliance is accessible through a public computer network.

A digital seal certificate is assigned a distinguished name on the basis of the name entered in the register of the Client's home country.

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

4.1 Submission of Applications for Certificates

See Clause 4.1 of the CPS.
Certificates for applications shall be submitted to the SK in an electronic form that enables verification of the identity of the Client's representative. In addition to the Client's details, an application shall include the CSR in the PKCS#10 [7] format or the distinguished name and expiration date of the certificate that is applied for.

If the Client wants a digital seal on the basis of the CSR, the Client's representative shall confirm on the application form that a secure signature creation device will be used for the management of the certificate.

4.2 Processing of Applications for Certificates

Applications for certificates are processed within 5 business days after their receipt by the SK. Correctness and completeness of data submitted by the Client are verified during the processing of applications for certificates.

4.2.1 Decision Making

The acceptance or rejection of the applications for certificates is the decision of the SK. Prior to making a decision, the SK checks the following:

- The identity of the Client (including the registered status of the legal person in accordance with the legislation of its home country)
- The identity of the Client's representative
- The authority of the Client's representative to apply for a certificate and/or for the revocation of a certificate on behalf of the Client
- Correctness and completeness of data submitted by the Client
- Whether the Client has the right to receive a certificate according to the legislation of the Republic of Estonia and/or this CP

In the case of applications for digital seals, the uniqueness of the distinguished name of a certificate is also verified.

In the case of applications for web server certificates, the link between the Client and the domain name and/or IP address of the Client's appliance is verified if the appliance is accessible through a public computer network.

The decision of the SK is subject to the results of the aforementioned checks and the SK has the right to refuse to issue a certificate.

4.2.2 Issuing Certificates

See Clause 4.2.2 of the CPS.
The certificate (or link to the certificate) is sent to the Client's e-mail address as specified in the Client's contact information. The certificate is published in the public directory of the SK within 1 hour after that.

The Client shall visit the Client Service Point to receive his/her secure signature creation device (including chip card) and organisation certificate issued by the SK.

Upon the issue of a digital seal certificate issued on a secure signature creation device, an employee of the Client Service Point checks the identity of the Client's

representative on the basis of an identity document and his/her authority to receive the certificate.

The Client's representative confirms by his/her signature on the certificate of acceptance that (s)he has received the digital seal certificate and read this CP and The Terms of Use of Organisation Certificates.

4.2.3 Procedure for Registration of Certificates

See Clause 4.2.3 of the CPS.
Access to directory is not limited.

4.2.4 Certificate Check-up and Verification

See Clause 4.2.4 of the CPS.

4.2.5 Certificate Renewal

See Clause 4.2.5 of the CPS.
4 weeks before the expiry of a certificate the SK sends a notice of the forthcoming expiration of the certificate by e-mail to the Client's contact address.

For the purposes of this CP, certificates are not renewed and the Client shall apply for new certificates.

4.3 Applications for Suspension and Revocation of Certificates

See Clause 4.3 of the CPS.

Organisation certificates cannot be suspended, except digital seal certificates.

To revoke or suspend digital seal certificates, the Client's legal representative or the authorised person specified in the application for the certificate shall submit a respective written or digitally signed application to the SK.

4.4 Suspension of Certificates

Organisation certificates cannot be suspended, except digital seal certificates.

Digital seal certificates may be suspended in the Client Service Point of the SK. See Clause 4.4 of the CPS.

A digital seal certificate is suspended immediately after the legality of the certificate suspension request has been established and information about the suspension of the suspended certificate is entered into the database of certificates managed by the SK.

4.5 Termination of Suspension

See Clause 4.5 of the CPS.

Organisation certificates cannot be suspended and their suspension cannot be terminated, except digital seal certificates.

To terminate suspension of a digital seal certificate the Client's representative shall submit a written application in the Client Service Point or send to the SK an application digitally signed by the Client's representative to the address specified in the contact information.

Suspension of a digital seal certificate is terminated immediately after the legality of the request to terminate the certificate suspension has been established and information about the termination of the certificate suspension is entered into the database of certificates managed by the SK.

4.6 Certificate Revocation

4.6.1 Authority to Revoke Certificates

See Clause 4.6.1 of the CPS.
SK may revoke certificates for the following reasons:

- According to the TUOC [6];
- Client indicates that the original certificate application was not authorized and does not retroactively grant authorization;
- SK obtains reasonable evidence that Client's private key (corresponding to the public key in the certificate) has been compromised or is suspected of compromise, or that the certificate has otherwise been misused;
- SK receives notice or otherwise becomes aware that Client has violated one or more of its material obligations under the TUOC [6];
- SK receives notice or otherwise becomes aware of any circumstance indicating that use of the domain name and/or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked Client's right to use the domain name listed in the certificate, a relevant licensing or services agreement with the registrant has terminated);
- SK receives notice or otherwise becomes aware of a material change in the information contained in the certificate;
- a determination, in the SK's sole discretion, that the certificate was not issued in accordance with the present CP or CPS;
- SK determines that any of the information appearing in the certificate is not accurate, with the exception of the organizationalUnitName field, if present.
- SK ceases operations for any reason and has not arranged for another CA to provide revocation support for the certificate;
- SK private key used in issuing the certificate is suspected to have been compromised.

4.6.2 Submission of Application for Revocation

See Clause 4.6.2 of the CPS.
An application for revocation of a certificate may be also digitally signed and sent to the e-mail address of the SK as specified in the contact information.

4.6.3 Procedure of Revocation

See Clause 4.6.3 of the CPS.

4.6.4 Effect of Revocation

See Clause 4.6.4 of the CPS.

4.7 Procedures Ensuring Tracking

See Clause 4.7 of the CPS.

4.8 Actions in an Emergency

See Clause 4.8 of the CPS.

4.9 Termination of Certification Service Provider Operations

See Clause 4.9 of the CPS.

5 Physical and Organisational Security Measures

5.1 Security Management

See Clause 5.1 of the CPS.

5.2 Physical Security Measures

5.2.1 SK Physical Entrance Control

See Clause 5.2.1 of the CPS.

5.3 Requirements for Work Procedures

See Clause 5.3 of the CPS.

5.4 Personnel Security Measures

See Clause 5.4 of the CPS.

6 Technical Security Measures

6.1 Key Management

6.1.1 Certification Keys of SK

See Clause 6.1.1 of the CPS.

6.1.2 Client Keys

If the SK has been authorised by the Client to generate its public and private key, the SK shall ensure that the keys are not used before the delivery to the Client and no copies of the keys are made.

The Client is fully responsible for the preservation and secure use of its secret key.

If the Client generates the key pair for its digital seal by itself, it shall ensure management of its personal key in a secure signature creation device.

Activation of the Client's private key may be done in a secure signature creation device without the need to enter the activation code each time.

6.2 Logical Security

See Clause 6.2 of the CPS.

6.3 Description of Technical Means Used for Certification

See Clause 6.3 of the CPS.

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

See Clause 6.4 of the CPS.

7 Technical Profiles of Certificates and Revocation Lists (CRL)

7.1 Profiles of Certificates

See Clause 7.1 of the CPS.

Organisation certificates are issued for a period of up to **1125 days** (3 years and 30 days).

The precise profile of certificates is provided in the document "Profiles of Organisation Certificates" [2].

7.2 Revocation Lists (CRL)

See Clause 7.2 of the CPS.

The format of the Certificate Revocation List (CRL) is x.509v2 (defined in RFC2459 [4]).

The precise profile of the revocation list is provided in the document "Profiles of Organisation Certificates" [2].

8 Management of Certificate Policy

Amendments that 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 fractional part of the document version number shall be increased.

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 version number increased by one. The amended Certification Practice Statement along with the date of its entering into force, which cannot be earlier than 30 days after publication, shall be published electronically on the website of the SK.

9 Glossary

See Clause 10 of the CPS.
Secure signature creation device – See the Digital Signatures Act [3].

10 Abbreviations

See Clause 11 of the CPS.

Abbreviation	Definition
CSR	Certificate Signing Request
TUOC	Terms of Use of Organisation Certificates
SK	AS Sertifitseerimiskeskus

11 References

Referenced documents:
[1] Certification Practice Statement (CPS) of AS Sertifitseerimiskeskus.
[2] Profiles of Organisation Certificates.
[3] Republic of Estonia Digital Signatures Act, RT 1 2000, 26, 150.
[4] RFC 2459 – Request For Comments 2459, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile; http://www.ietf.org/rfc.
[5] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.

[6] Terms of Use of Organisation Certificates. AS Sertifitseerimiskeskus.
[7] PKCS#10 – Certification Request Syntax Standard. http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/