Certification Policy for Organisation Certificates

Version 2.6
OID: 1.3.6.1.4.1.10015.7.1.2.6
Valid from 20.06.2014

Version information		
Date	**Version**	**Changes/amendments**
20.06.2014	2.6	Updated chapter 4.6.1 – updated terms for certificate revocation; Updated chapter 8 – updated certification policy management policy; web server certificate is now stated as SSL server certificate; Updated chapter 4.2.2 – adjusted certificate issuance requirements separately for each certificate type. Minor changes/adjustments in accordance to new RFC versions; restructuring.
21.12.2012	2.5	Updated chapter 2.4.4 – updated rules for certificate publication in public catalogue.
28.09.2012	2.4	Updated chapter 4.2.4 – retired discrepancy with the CPS.
20.07.2012	2.3	Updated chapter 4.6.1 – added authority descriptions for revoking certificates.
10.05.2010	2.2	Updated chapters: 1.3.4 – single certificate may contain multiple usage areas (except digital stamp certificate); 4.2.2 – the term “smart card” has been replaced with “secure signature creation device”.
13.08.2009	2.1	Removed discrepancies with Digital Signatures Act. The term “device certificates” is no longer in use.
13.10.2006	1.1	Corrected version.
10.04.2002	1.0	Primary version.

1. Introduction

The following contains the requirements for issuance and servicing of organisation certificates issued by the organisation certification authority of AS Sertifitseerimiskeskus.

1.1. Table of Contents

1.2. Executive Summary

The document in hand (hereafter Certification Policy, CP) is a set of rules that specifies the basic operating principles and concepts of provisioning the certification service required to issue certificates to the intermediate certification authorities by the Root Certification Authority of AS Sertifitseerimiskeskus.

This CP is based on the document titled "AS Sertifitseerimiskeskus, Certification Practice Statement CPS" (hereafter CPS) [1] which is registered in the Registry of Certification Services. The CPS serves as the basis for providing the certification service. This CP specifies in detail the matters related to the service provided.

In the case of conflict between this 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.

Organisation certificates appear in forms of SSL server certificates and digital stamps in the meaning of DSA [7]. Detailed description of the certificates is in chapter 1.5.4 of this CP.

Internet Engineering Task Force recommended document RFC 3647 [3] has been used during drafting this CP.

1.3. Terms and Abbreviations

1.3.1. Terms

Refer to CPS p.10

Term	Description
Object identifier	An identifier used to name an object (OID).
Certification Authority	An entity that issues digital certificates.
Certification Policy	A document which states the different actors of a public key infrastructure (PKI), their roles and duties; certificate usage and common security requirements.
Certification Practice Statement	Practice description for certificate issuing, managing, revoking, renewing and re-key operations and conditions of a certification authority.
Shared control	A security measure, which ensures the access to security objects only in presence of at least two or more trust agents.

1.3.2. Abbreviations

Refer to CPS p.11

Abbreviation	Description
CP	Certification Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
DSA	Digital Signatures Act of the Republic of Estonia.
IANA	The Internet Assigned Numbers Authority is an organisation, which oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers.
OID	Object Identifier.
SK	AS Sertifitseerimiskeskus, provider of certification services.
CSR	Certificate Signing Request
TCU	Terms and Conditions of Use of Organisation Certificates.

1.4. Document Title and Version

1.4.1. CP Identification

Document title: Certification Policy for Organisation Certificates.

This CP is identified by OID: 1.3.6.1.4.1.10015.7.1.2.6

OID is composed according to the contents of the following table 1.

Parameter	OID reference
Internet attribute	1.3.6.1
Private entity attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	7.1
CP version attribute	2.6

1.5. Organization and Area of Application

1.5.1. Sertifitseerimiskeskus (SK)

Refer to CPS p.1.2.1.

1.5.2. SK Registration Centre

1.5.2.1. Client Service Points

Refer to CPS p.1.2.2.1.

AS Sertifitseerimiskeskus operates as client service point.

1.5.2.2. Help Line

Refer to CPS p.1.2.2.2.

No help line service is used in terms of this CP.

1.5.3. User

1.5.3.1. Client

Refer to CPS p.1.2.3.1.

In terms of CP, the certificates are issued to legal bodies.

The client is the owner of the certificate issued in terms of this CP.

Multiple organisation certificates can be issued to a single client.

1.5.3.2. Relying Party

Refer to CPS p.1.2.3.2.

1.5.4. Area of Application of Certificates

Refer to CPS p.1.2.4.

The area of application of the certificates issued to legal bodies in terms of this CP is not limited. This CP sets the special requirements to the issuance of the following certificates:

-
- **SSL server certificate** – a certificate issued to SSL server (HTTPS, IMAPS, FTPS, etc.) for proof of authenticity of SSL server owner.

- **Digital stamp certificate** – used for proof of integrity of a digital document and the relation with the owner of such document.

The usage of digital stamp certificate is determined by DSA [7].

Various areas of application may be combined into a single certificate. The area of application of digital stamp certificate may not be combined with other areas of application.

Specific certificates without determined area of application may be issued in dedicated arrangement with the client.

1.6. Contact Details

Refer to CPS p. 1.3.

AS Sertifitseerimiskeskus
Commercial registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Tel +372 610 1880
Fax +372 610 1881
E-post: pki@sk.ee
http://www.sk.ee/

2. General Terms

2.1. Obligations and Requirements

2.1.1. Obligations of SK

Refer to CPS p.2.1.1.

SK shall warrant in addition that:
- The certification service is provided in accordance with the Certification Practice Statement of AS Sertifitseerimiskeskus;
- The certification service is provided in accordance with this CP.

SK hereby additionally undertakes to:
- Accept and process certificate requests from the Client over a secured communications channel;
- Provide round the clock public directory service;
- Ensure that the certification keys are protected by hardware security modules and under sole control of SK;
- Revoke all certificates issued in case of compromise of certification keys;

- Ensure that all the activated certification keys are located within the borders of the Republic of Estonia;
- Ensure that the certification keys used in the supply of the certification service are activated on the basis of shared control.

2.1.2. Obligations of the Registration Centre

2.1.2.1. Obligations of the Client Service Point

Client service point must accept applications for certificate issuance, suspension, termination of suspension and revocation; and verify the authenticity and integrity of these requests. The clerk of the client service point obligates to verify the identity and authority of the applicant.

2.1.2.2. Obligations of the Help Line

Help Line is not used.

2.1.3. Obligations of Clients

Refer to CPS p.2.1.3.

The Client is obligated to follow the conditions and procedures set by SK within this CP. The client is obligated to present correct and up to date information and to inform SK in case of change of presented information.

The Client has to accept the "Terms and Conditions of Use of Organisation Certificates" (TCU) [5].

2.1.4. Obligations of Relying Party

Refer to CPS p.2.1.4.

2.1.5. Obligations of Public Directory

Refer to CPS p.2.1.5.

No additional requirements are foreseen for operating public directory service.

2.2. Liability

2.2.1. Liability of SK

Refer to CPS p.2.2.1.

SK is liable for all obligations described in chapter 2.1.1 and 2.1.2 of this CP within the limits of legislation of the Republic of Estonia.

2.2.2. Liability of the Registration Centre

2.2.2.1. Liability of the Client Service Point

Client service point is liable for all obligations described in chapter 2.1.2.1 of this CP.

2.2.2.2. Liability of the Help Line

Help Line is not used.

2.2.3. Limits of Liability

Refer to CPS p.2.2.3.

In addition, SK is liable for keeping the secrecy private keys and possible misuse of the certificates of the root certification authority.

2.3. Settling Disputes

Refer to CPS p.2.3.

2.4. Publication of Information and Directory Service

2.4.1. Publication of information by SK

Refer to CPS p.2.4.1.

Valid certification revocation list is accessible on the website http://www.sk.ee/repository/crls.

2.4.2. Publication Frequency

Refer to CPS p.2.4.2.

The certificate revocation list are updated and published regularly and not less than in every 12 hours.

2.4.3. Access Rules

Refer to CPS p.2.4.3.

2.4.4. Directory Service

Refer to CPS p.2.4.4.

The certificates issued in terms of this CP, are published in public directory at ldap://ldap.sk.ee upon activation.

Upon certificate revocation, the certificate will be deleted from the public directory.

Expired certificates are deleted from the public directory on the day after expiring.

2.5. Audit

Refer to CPS p.2.5.

2.6. Confidentiality

Refer to CPS p.2.6.

3. Client Identification

3.1. Client Identity Verification

During processing of organisation certificate application the following shall be verified:

- Registration of the client in accordance with legislation of country of origin;
- The identity of the client representative;
- The authority of the client representative for applying for the certificate in the name of the client.

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

In order to apply for the organisation certificate, the client must electronically submit a Certificate Signing Request (CSR), which contains the public key of the applicant and which is signed with the corresponding private key. The conformity with the signing request allows SK to presume that the corresponding private key is in applicant's possession.

In case if SK has received the authority to generate the public and private key for the Client, the conformity is guaranteed by the internal procedures of SK and the Client does not have to electronically submit the Certificate Signing Request (CSR).

3.3. Distinguished Name

Refer to CPS p.3.3.

The distinguished name of the certificate is compiled in accordance with the document titled "The Organisation Certificate and CRL Profile of SK" [2].

The uniqueness of distinguished name of SSL server certificates is not warranted.

The client's relation to the device's domain name or IP address serves as the basis during assignment of SSL server certificate's distinguished name while the distinguished name must be resolvable by public DNS service and the IPv4 or IPv6 address may not be marked as 'reserved' by IANA.

During assignment of the distinguished name of a digital stamp, the client's name listed in the registry of country of origin shall be based on.

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

4.1. Submission of Applications for Certificates

Refer to CPS p.4.1.

An electronic application for certificate which allows verifying the identity of the client representative is submitted to SK. In addition to the client's data, the application contains the signed certificate signing request (CSR) in PKCS#10 [6] format or the distinguished name and validity period of the certificate requested.

If the client is requesting for a digital stamp based on a CSR, the client's representative must confirm on the certificate application form that the certificate shall be stored on a secure signature creation device.

4.2. Processing of Applications for Certificates

The certificate application shall be processed within 5 working days after its acceptance by SK. During the processing of the certificate application, the correctness and the integrity of the data submitted by the client is verified.

4.2.1. Decision Making

Refer to CPS p.4.2.1.

The acceptance or rejection of an application for certificates shall be decided by SK. During deciding SK verifies:

- The identity of the client (including the registration status of the legal body in accordance to the legislation of the country of origin);
- The identity of the client representative;
- The authority of the client representative for requesting and/or revoking a certificate;
- The correctness and integrity of the data presented by the client;
- If the client has the right to have a certificate in accordance with the legislation of the Republic of Estonia and/or with the CP in hand.

The uniqueness of the distinguished name of the certificate is also verified in case of the digital stamp application.

The client's device's domain name or IP address shall be used as the basis for assignment of SSL server certificate's distinguished name if the distinguished is resolvable by public DNS service and the IPv4 or IPv6 address is not marked as 'reserved' by IANA.

During the decision making, SK relies on the verification results of conditions listed above and reserves the right to reject the certificate application.

4.2.2. Certificate Issuance

Refer to CPS p.4.2.2.

For issuing a digital stamp certificate, the legal body:

- Must be registered in the Estonian Commercial Register;
- Must be findable from the business registry of Republic of Estonia;

- May not be bankrupted or in the process of liquidation; its activities may not be suspended or in other similar state.

The application for digital stamp certificate must be digitally signed in the meaning of DSA [7] by the organisation's representative with the power to sign or by a person authorised by digital signature of such.

For issuing SSL server certificate, the legal body:

- Must be registered in the Estonian, Latvian, Lithuanian, Finnish or Swedish Commercial Registry and discoverable from the European Commercial Registry;
- May not be bankrupted or in the process of liquidation; its activities may not be suspended or in other similar state in terms of legislation of its country of origin.

In addition, for issuing an SSL server certificate:

- The data of the registrar of the domain must be discoverable from the IANA's registry;
- The domain must be registered in the domain registry of the corresponding country;
- The certificate application must be digitally signed by the contact person listed in the domain registrant's records.

If the contact person of the domain does not have the ability to digitally sign the certificate application in the meaning of DSA [7], SK has the right to adopt additional checks prior to the certificate issuance.

For all other organisation certificates, the legal body:

- Must be registered in the Estonian, Latvian, Lithuanian, Finnish or Swedish Commercial Registry and discoverable from the European Commercial Registry;
- May not be bankrupted or in the process of liquidation; its activities may not be suspended or in other similar state in terms of legislation of its country of origin.

The application for the certificate must be digitally signed in the meaning of DSA [7] by the organisation's representative with the power to sign or by a person authorised by digital signature of such. If the person with the power to sign does not have the ability to digitally sign the certificate application in the meaning of DSA [7], SK has the right to adopt additional checks prior to the certificate issuance.

The certificate (or a reference to) shall be delivered to the e-mail address of the client stated in the certificate application. Latest within 1 hour, the certificate shall be published in the public directory of SK.

The organisation certificate issued by SK to a secure signature creation device has to be retrieved it personally by the client from the client service point of SK.

Prior to the issuance of a digital stamp certificate loaded to a secure signature creation device, the clerk of the client service point must verify the identity and authority of the client representative for acceptance of the certificate. In case of letter of attorney, the client representative must be authorised by the person with the power to sign of the client and by the person signed the certificate application.

On the certificate acceptance, the client representative confirms with a signature to agree with the terms of this CP and with the "Terms and Conditions of Use of Organisation Certificates" (TCU) [5].

4.2.3. Procedure for Registration of Certificates

Refer to CPS p.4.2.3.

The access to the public directory is not limited.

4.2.4. Certificate Check-up and Verification

Refer to CPS p.4.2.4.

4.2.5. Certificate Renewal

An e-mail shall be sent by SK to the contact address of the client 4 weeks prior to the certificate expiry to inform the client.

The certificate renewal is not applied in the meaning of this CP. The client has to apply for the new certificates.

4.3. Applications for Suspension and Revocation of Certificates

Refer to CPS p.4.3.

Except for digital stamp certificates, the organisation certificates cannot be suspended.

In order to revoke or suspend digital stamp certificates, the legal representative of the client or the authorised person indicated on the certificate application, must present a written or digitally signed application to SK.

4.4. Suspension of Certificates

Except for digital stamp certificates, the organisation certificates cannot be suspended.

The certificates of digital stamps can be suspended in client service point of SK. Refer to CPS p.4.4.

The certificates of the digital stamp shall be suspended immediately after the request's legality has been verified and the details about the suspension shall be recorded in the registry held by SK.

4.5. Termination of Suspension

Refer to CPS p.4.5.

Except for digital stamp certificates, the suspension or termination of suspension of organisation certificates cannot be applied.

In order to terminate the suspension of digital stamp certificates the client representative has to present a written application to the client service point of SK or submit a digitally signed application to the address listed in SK's contact details.

The suspension of digital stamp certificates shall be terminated immediately after the request's legality has been verified and t

The certificates of the digital stamp shall be suspended immediately after the request's legality has been verified and the details about the termination of suspension shall be recorded in the registry held by SK.

4.6. The Certificate Revocation

4.6.1. Authority to Revoke Certificates

Refer to CPS p.4.6.1.

SK has the authority to revoke certificates on following reasons:

- In accordance with "Terms and Conditions of Use of Organisation Certificates" (TCU) [5];
- The client informs SK of the fact that the initial certificate application was not authorised and client does not apply for retroactive authorisation;
- SK finds that control over the client's private key (which corresponds to the certificate's public key) has been lost or it has been compromised;
- SK receives a notice of or finds out otherwise that the client has violated one or more significant condition of "Terms and Conditions of Use of Organisation Certificates" (TCU) [5];
- SK receives a notice of or finds out otherwise of circumstances that refer to the fact that the usage of domain name and/or IP address is no longer legal (i.e. the right to use the domain name described in the certificate has been revoked by court order or the contractual relationship between the domain registry has been terminated);
- SK receives a notice of or finds out otherwise of significant changes of data listed in the certificate;
- SK determinates with sole discretion that the certificate issued is not compliant with this CP or CPS;
- SK detects that some of the data recorded in the certificate is incorrect except for organizationalUnitName if it exists;
- SK terminates its operations in whatever reason and has not delegated the certificate revocation service to another certification service provider;
- There is suspicion that the private key of SK that has been used for signing the certificates has been compromised;
- SK finds out that the certificate has been used for criminal activities such as fraud, spyware, malware and virus distribution, etc.

4.6.2. Submission of Application for Revocation

Refer to CPS p.4.6.2.

The application for certificate revocation can also be signed digitally and submitted to e-mail address listed in SK's contact details.

4.6.3. Procedure of Revocation

Refer to CPS p.4.6.3.

4.6.4. Effect of Revocation

Refer to CPS p.4.6.4.

4.7. Procedures Ensuring Tracking

Refer to CPS p.4.7.

4.8. Action in an Emergency Situation

Refer to CPS p.4.8.

4.9. Termination of Certification Service Provider Operations

Refer to CPS p.4.9.

5. Physical and Organizational Security Measures

5.1. Security Management

Refer to CPS p.5.1.

5.2. Physical Security Measures

5.2.1. SK Physical Entrance Control

Refer to CPS p.5.2.1.

5.3. Requirements for Work Procedures

Refer to CPS p.5.3.

5.4. Personnel Security Measures

Refer to CPS p.5.4.

6. Technical Security Measures

6.1. Key Management

6.1.1. Certification Keys of SK

Refer to CPS p.6.1.1.

6.1.2. Client Keys

If SK has authorised by client to generate the public and private key, SK ensures that the keys are not used prior to the delivery to the client and no copies of the keys shall be made.

The client is fully responsible for preservation and secure usage of its private keys.

If the key pair of the digital stamp is generated by the client, the client must warrant the maintaining of the private key in a secure signature creation device.

The activation of the private key of the client may be carried out without the actual input of the activation code.

6.2. Logical Security

Refer to CPS p.6.2.

6.3. Description of Technical Means used for Certification

Refer to CPS p.6.3.

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

Refer to CPS p.6.4.

7. Technical Profiles of Certificates and Revocation Lists

7.1. Certificate Profiles

Refer to CPS p.7.1.

The maximum validity period for organisation certificate is 1125 days (3 years and 30 days). For B4B certificates, the maximum validity period is 1855 days (5 years and 30 days.)

The technical profile of certificates is described in document “Organisation Certificates and CRL profiles of SK” [2].

7.2. CRL Profiles

Refer to CPS p.7.2.

The CRL is in x.509v2 format defined by RFC5280-s [4].

The technical profile of CRLs is described in document "Organisation Certificates and CRL profiles of SK" [2].

8. Management of Certification Policy

Refer to CPS p.8.

This CP and the referred documents "Certification Practice Statement" [1] and "Organisation Certificates and CRL profiles of SK" [2] are published on web page of SK.

Changes not affecting the meaning of this CP like spelling corrections, translations and updates of contact details shall be documented in the version information section of this document and the document version number's fraction shall be increased accordingly.

In case of substantive changes, the updated version must be clearly distinguishable from the previous version. The new main version number shall be increased accordingly.

The full text of amendment to substantive changes of CP shall be electronically published on SK's web site 90 days prior to the planned effective date.

Within 30 days of amendment publication, the client has the chance to provide reasoned comments followed by maximum 30 day period for comment analysis by SK. 60 days after the amendment publication, the new version of CP shall be published electronically on SK's web page, otherwise the amendment is withdrawn.

8. Referred and Related Documents

[1] AS Sertifitseerimiskeskus, Certification Practice Statement;

[2] Organisation Certificates and CRL profiles of SK;

[3] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[4] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[5] Terms and Conditions of Use of Organisation Certificates. AS Sertifitseerimiskeskus;

[6] PKCS#10 – Certification Request Syntax Standard. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm;

[7] Digital Signatures Act of Republic of Estonia, RT I 2000, 26, 150