

Certificate Policy for Device Certificates

Version 1.0

OID: 1.3.6.1.4.1.10015.2.1.1.1

Versions and Alterations:

Version	Date	Comments
1.0	10.04.2002	First version

Table of Contents

TABLE OF CONTENTS	2
1 INTRODUCTION.....	4
1.1 GENERAL SURVEY	4
1.2 CERTIFICATE POLICY IDENTIFIER.....	4
1.3 ORGANISATION AND AREA OF APPLICATION	5
1.3.1 Certification Centre (CC)	5
1.3.2 CC Registration Centre.....	5
1.3.3 User.....	5
1.3.4 Area of Application of Certificates	5
1.4 CONTACT DETAILS	6
2 GENERAL CONDITIONS.....	6
2.1 OBLIGATIONS AND REQUIREMENTS	6
2.1.1 Obligations of CC	6
2.1.2 Obligations of Registration Centre	6
2.1.3 Obligations of Client.....	7
2.1.4 Obligations of Relying party.....	7
2.2 LIABILITY	7
2.2.1 Liability of CC.....	7
2.2.2 Liability of Registration Centre	7
2.2.3 Limits of Liability.....	7
2.3 RESOLUTION OF DISPUTES	8
2.4 INFORMATION PUBLICATION AND DIRECTORY SERVICE	8
2.4.1 Publication of CC's Information	8
2.4.2 Frequency of Publication.....	8
2.4.3 Access Rules.....	8
2.4.4 Directory Service	8
2.5 AUDIT	8
2.6 CONFIDENTIALITY.....	8
2.7 PROPRIETORSHIP	8
3 CLIENT IDENTIFICATION	8
3.1 IDENTIFICATION OF PERSON.....	8
3.2 PROCEDURE OF CERTIFYING APPLICANT'S PERSONAL KEY TO PUBLIC KEY ..	9
3.3 DISTINGUISHED NAME	9
4 PROVIDING CERTIFICATION SERVICE. PROCEDURE AND TERMS OF CERTIFICATION	9
4.1 SUBMISSION OF APPLICATION FOR CERTIFICATE	9
4.2 PROCESSING OF CERTIFICATE APPLICATIONS	9
4.2.1 Decision Making	10
4.2.2 Certificate Issuing.....	10
4.2.3 Procedure for Registration of Certificates	10
4.2.4 Certificate Check-up and Verification.....	10

4.2.5	<i>Renewal of Certificate</i>	10
4.3	REQUESTS FOR CERTIFICATE SUSPENSION AND REVOCATION	10
4.4	CERTIFICATE SUSPENSION	11
4.5	TERMINATION OF CERTIFICATE SUSPENSION	11
4.6	CERTIFICATE REVOCATION.....	11
4.6.1	<i>Authority to Revoke Certificates</i>	11
4.6.2	<i>Submission of Request for Revocation of Certificate</i>	11
4.6.3	<i>Processing of Requests for Certificate Revocation</i>	11
4.6.4	<i>Operativeness of Certificate Revocation Process</i>	11
4.7	PROCEDURES GUARANTEEING TRACKING	11
4.8	ACTION IN AN EMERGENCY SITUATION	11
4.9	TERMINATION OF OPERATIONS OF CERTIFICATION SERVICE PROVIDER	12
5	PHYSICAL AND ORGANISATIONAL SECURITY MEASURES	12
5.1	SECURITY MANAGEMENT	12
5.2	PHYSICAL SECURITY MEASURES	12
5.2.1	<i>CC Physical Entrance Control</i>	12
5.3	REQUIREMENTS TO WORK PROCEDURES	12
5.4	PERSONNEL SECURITY MEASURES.....	12
6	TECHNICAL SECURITY MEASURES	12
6.1	KEY MANAGEMENT	12
6.1.1	<i>CC's Verification Keys</i>	12
6.1.2	<i>Client Keys</i>	12
6.2	SYSTEM SECURITY	12
6.3	DESCRIPTION OF TECHNICAL MEANS USED FOR PROVIDING CERTIFICATION SERVICE.....	12
6.4	STORAGE AND PROTECTION OF INFORMATION CREATED IN COURSE OF PROVIDING CERTIFICATION SERVICE	13
7	TECHNICAL PROFILES OF CERTIFICATES AND REVOCATION LISTS (CRL)	13
7.1	PROFILES OF CERTIFICATES	13
7.2	REVOCATION LISTS (CRL)	13
8	ADMINISTRATION OF CERTIFICATION POLICY	13
9	GLOSSARY	13
10	ABBREVIATIONS	13
11	REFERENCES	14

1 Introduction

1.1 General Survey

This document (hereinafter Certificate Policy, CP) is a set of rules which specifies the fundamental operating principles and concepts of the certification service provision essential for device certificates.

This CP is founded on the document titled “Certificate Practice Statement of AS Sertifitseerimiskeskus. Version 1.2”[1] which has been registered in the public register of certification service providers. These certificate principles (hereinafter the CPS) shall serve as a basis for supply of certification service. This CP supplements the principles set out in the CPS.

In the case of conflict between the CP and the CPS the provisions of this CP shall prevail.

This CP extends only to the digital certificates issued by AS Sertifitseerimiskeskus (Certification Centre).

IETF (Internet Engineering Task Force) recommended document RFC 2527 has been used in drafting this CP.

1.2 Certificate Policy Identifier

The identification code of this CP is **OID: 1.3.6.1.4.1.10015.2.1.1.1**

The OID code of the CP has been composed according to the following Table 1.

Parameter	Reference in OID
Internet attribute	1.3.6.1
Private business attribute	4
Registered business attribute given by private business manager IANA	1
CC attribute in IANA register	10015
Certification service attribute	2.1
CP version attribute	1.1

Table 1. Composition of the CP identification code

1.3 Organisation and Area of Application

1.3.1 Certification Centre (CC)

See clause 1.2.1 of the CPS.

1.3.2 CC Registration Centre

1.3.2.1 CC Client Service Point (CSP)

AS Sertifitseerimiskeskus carries out duties of the Client Service Point.

1.3.2.2 Help Line

As suspension of the device certificates is not foreseen, no additional help line is in existence.

1.3.3 User

1.3.3.1 Client

See clause 1.2.3.1 of the CPS

Certificates are issued only to legal persons according to this CP.

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

A Client's distinctive name on the certificate is composed according to the certificate profile annexed hereto.

1.3.3.2 Relying party

See clause 1.2.3.2 of the CPS.

A Relying party shall have examined this CP.

1.3.4 Area of Application of Certificates

See clause 1.2.4 of the CPS.

Certificates issued according to this CP shall be used for securing data communication between devices (computers).

Device certificates cannot be used for digital signature as defined in the Digital Signatures Act [3].

1.4 Contact Details

See clause 1.3 of the CPS.

2 General Conditions

2.1 Obligations and Requirements

2.1.1 Obligations of CC

See clause 2.1.1 of the CPS.

CC hereinafter additionally represents and warrants that

- The certification service is provided in accordance with the certification principles of AS Sertifitseerimiskeskus (CC);
- The certification service is provided in accordance with this CP.

The CC hereby additionally undertakes to:

- Accept and act on the certificate requests of the Client via a secure electronic data communications channel;
- Supply the directory service 24-hours a day;
- Ensure that the signing keys used in the supply of certification service were secured by software safety modules and did not go out of the CC's control;
- If the signing keys go out of the CC control, revoke the validity of all the certificates issued;
- Ensure that all activated signing keys were based in the territory of the Republic of Estonia;
- Ensure that the signing keys used in the supply of certification service are activated on the basis of shared control;

2.1.2 Obligations of Registration Centre

2.1.2.1 Obligations of CC Client Service Point

The CSP must accept application for issuance and revocation of certificates and check correctness and integrity of those applications. CSP obliges to verify personal identity of the applicant and verify his/her mandates to act on behalf of legal person.

2.1.2.2 Obligations of the Help Line

Help Line does not exist.

2.1.3 Obligations of Client

See clause 2.1.3 of the CPS

A Client shall observe the procedures enacted by CC in this CP. Client is obliged to present correct and complete data to CC and inform CC immediately about changes in those data.

2.1.4 Obligations of Relying party

See clause 2.1.4 of the CPS.

A Relying party shall take account of the liabilities and risks related to the acceptance of certificates and defined in this CP.

2.1.4.1 Requirements to the Directory Service

See clause 2.1.4 of the CPS.

2.2 Liability

2.2.1 Liability of CC

See clause 2.2.1 of the CPS.

CC shall be liable for the performance of all its obligations specified in clauses 2.1.1 and 2.1.2 above to the extent provided in the applicable legislation of the Republic of Estonia.

2.2.2 Liability of Registration Centre

2.2.2.1 Liability of Client Service Point

See clause 2.2.2.1 of the CPS.

A Customer Service Point shall be liable for performing all its obligations specified in clause 2.1.2.1.

2.2.2.2 Liability of the Help Line

Help Line does not exist.

2.2.3 Limits of Liability

See clause 2.2.3 of the CPS.

2.3 Resolution of Disputes

See clause 2.3 of the CPS.

2.4 Information Publication and Directory Service

2.4.1 Publication of CC's Information

See clause 2.4.1 of the CPS.

The valid CRL is accessible via the directory service and on the website <http://www.sk.ee/crls/klass3/klass3.crl>.

2.4.2 Frequency of Publication

See clause 2.4.2 of the CPS.

Certificate Revocation Lists are generally published within 10 minutes after submission or satisfaction of a relevant request for cancellation. The guaranteed frequency of publication is 12 hours.

2.4.3 Access Rules

See clause 2.4.3 of the CPS.

2.4.4 Directory Service

See clause 2.4.4 of the CPS.

2.5 Audit

See clause 2.5 of the CPS.

The results of external audits are published on the website of CC.

2.6 Confidentiality

See clause 2.6 of the CPS.

2.7 Proprietorship

AS Sertifitseerimiskeskus has been granted all rights, including proprietary and copyrights, with respect to the integral technical solutions and documentation.

3 Client Identification

3.1 Identification of Person

The Client and data presented by him are verified in accordance with the rules set in the document "Terms of Use for Device Certificates" [6].

The following checks are performed during certificate application processing:

- Data about the Client as a legal person
- Personal identity of device administrator and his/her mandates for applying for the legal person for certificate issuance/revocation.
- Ownership of the domain name and/or IP address in case the device is accessible over public network

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

The Client presents a CSR (*Certificate Signing Request*) to CC electronically. The CSR contains public key of the applicant and is signed with private key of the applicant. CC ensures that private key is in control of applicant by successful decipherment of the CSR.

3.3 Distinguished Name

See clause 3.3 of the CPS.

The client's distinguished name is composed in accordance with the document titled "Profile of Device Certificates" [2]

4 Providing Certification Service. Procedure and Terms of Certification

4.1 Submission of Application for Certificate

See clause 4.1 of the CPS.

The request for certificate issuance is submitted in CC's web environment. A Client enters required contact data and uploads Certificate Signing Request in designated web form. Upon submission of all necessary data, the system will produce application form to be signed by applicant manually or digitally according to the Digital Signature Act [3]. Signed application form shall be sent to CC for processing.

4.2 Processing of Certificate Applications

The application for certificate issuance is processed in 2 working days from retrieval of signed application form. Validity and integrity of data is checked during processing of the application.

4.2.1 Decision Making

Decision on approval of the certificate issuance application is made by CC. The following aspects will be taken into account:

- Organizational status of the Client
- In case the device to be certified is accessible over a public network: ownership of the domain name and/or IP-address of the device
- Administrator of the device and his/her mandates to represent the Client.

4.2.2 Certificate Issuing

See clause 4.2.3 of the CPS.

Certificate (or reference to it) will be sent to the Client using e-mail address given in contact data. At the same time the certificate is published in the public directory of CC.

4.2.3 Procedure for Registration of Certificates

See clause 4.2.3 of the CPS.

Access to public directory is not restricted.

4.2.4 Certificate Check-up and Verification

Validity of the certificate can be checked by relying party using CC's public directory and Certificate Revocation List (CRL) in the same directory. CC does not issue digitally signed validity confirmations for device certificates.

4.2.5 Renewal of Certificate

CC will send an e-mail message to the Client two weeks before expiration of the certificate with warning message about the expiration and with link to CC's web page for certificate renewal.

Renewal of certificates is performed by using existing key pair and for certificates not revoked. New certificate shall be applied for in other cases.

Applying for certificate renewal is available using web page of CC. The application for certificate renewal is processed in 2 working days from registration of the application in the information system of CC.

4.3 Requests for Certificate Suspension and Revocation

Device certificates cannot be suspended.

For revocation of device certificate a written application shall be supplied to CC by the person applied for certificate of by the lawful representative of the legal person.

4.4 Certificate Suspension

Device certificates cannot be suspended.

4.5 Termination of Certificate Suspension

Device certificates cannot be suspended.

4.6 Certificate Revocation

4.6.1 Authority to Revoke Certificates

See clause 4.6.1 of the CPS.

CC can also revoke certificate as stated in “Terms of Use for Device Certificates”[6].

4.6.2 Submission of Request for Revocation of Certificate

The Client shall submit a written application for certificate revocation containing:

- name of applicant
- signature of applicant
- owner name and serial number of the certificate to be revoked
- distinguished name of the issuer of the certificate
- reason for revocation
- other evidential material on reasons for revocation if needed

The applicant is identified by CC.

4.6.3 Processing of Requests for Certificate Revocation

See clause 4.6.3 of the CPS.

4.6.4 Operativeness of Certificate Revocation Process

See clause 4.6.4 of the CPS.

4.7 Procedures Guaranteeing Tracking

See clause 4.7 of the CPS.

4.8 Action in an Emergency Situation

See clause 4.8 of the CPS.

4.9 Termination of Operations of Certification Service Provider

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 CC Physical Entrance Control

See clause 5.2.1 of the CPS.

5.3 Requirements to 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 CC's Verification Keys

See clause 6.1.1 of the CPS.

6.1.2 Client Keys

The Client generates the key pair itself and is solely responsible for security of it's private key.

6.2 System Security

See clause 6.2 of the CPS.

6.3 Description of Technical Means Used for Providing Certification Service

See clause 6.3 of the CPS.

6.4 Storage and Protection of Information Created in Course of Providing Certification Service

See clause 6.4 of the CPS.

7 Technical Profiles of Certificates and Revocation Lists (CRL)

7.1 Profiles of Certificates

Device certificates are valid for maximum of 369 days (one year and four days).

Profile of certificates is described in detail in the document “Profile of Device Certificates” [2].

7.2 Revocation Lists (CRL)

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

Profile of certificate revocation lists is described in detail in the document “Profile of Device Certificates” [2].

8 Administration of Certification Policy

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 Policy along with the enforcement date, which cannot be earlier than 30 days after publication, shall be published electronically on the CC’s website.

9 Glossary

See clause 9 of the CPS.

10 Abbreviations

See clause 10 of the CPS.

Abbreviation	Definition
CSR	Certificate Signing Request

11 References

Documents:

- [1] Certification Practice Statement of AS Sertifitseerimiskeskus
- [2] Profile of Device Certificates
- [3] Digital Signatures Act of the Republic of Estonia, 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 for Device Certificates

Related documents:

- Information Protection Policy of AS Sertifitseerimiskeskus (CC).
- Management Strategy and Policy of AS Sertifitseerimiskeskus
- IT Systems Recovery Policy of AS Sertifitseerimiskeskus
- Databases Act, RT 1 1997, 28, 423
- Identity Documents Act, RT 1 1999,25,365
- Personal Data Protection Principles
- Personal Data Protection Act RT 1 1996, 48, 944.