AS Sertifitseerimiskeskus
Certification Policy for Mobile-ID

Version 2.0
OID: 1.3.6.1.4.1.10015.11.1.2
Valid from 16.12.2009

Version information		
Date	**Version**	**Changes/Updates/Amendments**
16.11.2009	2.0	Improvements due to practice of Mobile-ID service startup. Lingual corrections.
11.04.2007	1.0	First public edition
15.03.2007	0.9	Draft

Requirements on the Mobile-ID certification service with the purpose of issuing and servicing certificates which facilitate digital signature and digital identification of persons.

1. Introduction

1.1. Overview

This document (hereafter CP) is a set of rules which specifies the fundamental operating principles and concepts of the certification service provision essential for issuance and servicing Mobile-ID certificates.

This CP is based on the document titled “AS Sertifitseerimiskeskus – Certification Practice Statement” [1] which is registered in the Registry of Certification Services). This Certification Practice Statement (hereafter the CPS) shall serve as a basis for supply of certification service. This CP supplements the principles set out in the CPS for Mobile-ID certification services.

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

This CP extends only to the digital certificates of Mobile-ID issued by AS Sertifitseerimiskeskus.

IETF (Internet Engineering Task Force) recommended document RFC 2527 [2] has been used in drafting this CP.

1.2. Terminology

Refer to CPS p.10.

Term	Definition
Client Service Point	A client service point of a mobile operator operating on the basis of this CP and is authorized to provide Mobile-ID related services, refer to clause 1.5.2.1.
Mobile-ID SIM card	A SIM card for a mobile phone which in addition to regular cellular service usage facilitates functionality of digital signature and digital identification of persons.
Terms of use of the certificates	Document that describes the obligations and responsibilities for the client while using Mobile-ID certificates. Client has to be familiar with its contents and accept the terms and conditions described within.
Certificate application	Written application which has to be filled and signed manually by client for acquiring Mobile-ID service and certificates.

1.3. Abbreviations

Refer to CPS p.11.

Abbreviation	Definition
MO	Electronic communications company that provides mobile

	telephone services, and with whom contracts have been concluded for issuing Mobile-ID SIM cards and for servicing of the Mobile-ID certificates.

1.4. Identifying the Certification Policy

This CP is identified by **OID: 1.3.6.1.4.1.10015.11.1.2**

The OID of this CP is composed as described in table 1.

Parameter	OID section
Internet attribute	1.3.6.1
Private business attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	11.1
CP version attribute	2

Table 1. Composition of the CP identification code.

1.5. Organization and Area of Application

1.5.1. Sertifitseerimiskeskus (SK)

Refer to CPS p.1.2.1.

SK has contractually delegated obligations described in clause 1.5.2 to MO.

1.5.2. Registration Centre

1.5.2.1. Client Service Points

Refer to CPS p.1.2.2.1.

Accepting applications for Mobile-ID certificates, issuance of the Mobile-ID SIM cards and servicing of the Mobile-ID certificates (suspensions, terminations of suspension, revocations and change of the mobile telephone number) takes place in authorized MO client service points (hereafter client service point). The list and operating hours of client service points are referred from the websites of SK http://www.sk.ee and MO.

MO ensures security with its internal security procedures while providing the service.

1.5.2.2. Help Line

Help Line is a telephone service representing MO, which round the clock shall accept applications for suspending certificates by checking applicant’s identity in advance according to the procedure of identity verification (refer to clause 3.1).

Help Line shall provide additional information for solving problems regarding Mobile-ID if necessary.

Information about Help Line and its contact details is presented on the website of MO. Also there shall be instructions for contacting the Help Line.

1.5.3. User

1.5.3.1. Client

Refer to CPS p.1.2.3.1.

Client is a physical person the Mobile-ID certificates are issued to as a public service. Every client can have one valid Mobile-ID certificate that facilitates digital signature and one valid Mobil-ID certificate that facilitates digital identification.

Client is the holder of the certificate issued under this CP.

Client's distinguished name is compiled according to the certificate profile described in this document in clause 7.1.

The client has to have an opportunity to get acquainted with "The terms and conditions of use of Mobile-ID certificates" [3] prior to signing the Mobile-ID contract.

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.

There are two types of certificates issued under this CP:

a) Certificates for digital signature.
b) Certificates for digital identification of persons.

Certificates for digital signature can be used for digital signature as defined in the Digital Signatures Act [6].

This CP does not limit the use of the certificates issued in different software applications or fields of application.

1.6. Contact Details

Refer to CPS p.1.3

SK

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Phone +372 610 1880
Fax +372 610 1881
E-mail: pki@sk.ee
http://www.sk.ee

Help Line
The obligations of the Help Line shall be carried out by the MO's hotline. The contact details of the Help Line are referred from the websites of SK http://www.sk.ee and MO.

MO
The contact details of MO are referred from the website of SK http://www.sk.ee. The change of MO's contact details must be announced immediately on MO's website.

Client Service Points
The list and contact details of the client service points are referred from SK's website http://www.sk.ee and from the MO's website. The change of contact details must be announced immediately on MO's website.

2. General Terms

2.1. Obligations

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 register the certificate applications presented by MO and issue respective certificates;
- Provide pertinent web application for activation of the Mobile-ID certificates;
- Accept, register and process applications presented by MO for suspension, termination of suspension, revocation of Mobile-ID certificates and the applications for change of phone number linked to the Mobile-ID SIM card;
- Ensure that the certification keys are protected by hardware security modules and under sole control of SK;
- Suspending all the certificates issued in case of compromise of the 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 MO Client Service Point

Refer to CPS p.2.1.2.1.

The client service point of MO shall accept the applications for suspension, termination of suspension and revocation of Mobile-ID certificates and verify the correctness and integrity of these applications. While processing all these operations, the client service point obligates to verify the applicant's identity and powers for carrying out the operation.

The MO client service point shall warrant the required training for its employees for providing the quality service.

The employee of the MO client service point may not have been punished for an intentional crime.

MO client service point hereby additionally undertakes to:

- Forward the certificate request to SK and hand over the Mobile-ID SIM card to the client;
- Support the primary help and consultancy for handling the Mobile-ID SIM-card and for using e-services that support Mobile-ID;
- Prepare and ensure the availability of information booklets about the service to the client.

2.1.2.2. Obligations of MO Help Line

Refer to CPS p.2.1.2.2.

2.1.3. Obligations of MO

MO undertakes to:

- Follow the availability and security requirements on the information system related to the Mobile-ID service at least to the level of the requirements described in this CP;
- Ensure the security with its internal security procedures. MO is responsible for all operations and procedures regarding the production of the Mobile-ID SIM cards, including the secure key generation on the Mobile-ID SIM card;
- Ensure that the employees, who will accept the applications regarding Mobile-ID certificates (issuance, suspension, termination of suspension and revocation) and/or are involved with information related to certification service, are not punished for intentional crime.
- Assure the availability of the information related to Mobile-ID in the public data network.

2.1.4. Obligations of Clients

Refer to CPS p.2.1.3.

Upon application for Mobile-ID certificates a client shall submit to the MO client service point true and correct information. In case of a change in his/her personal details immediately notify the MO client service point of the changed details and pretend to new Mobile-ID certificates.

2.1.5. Obligations of Relying Party

Refer to CPS p.2.1.4.

2.1.6. Obligations of Directory Service

Directory service is not applied.

2.2. Liability

2.2.1. Liability of SK

Refer to CPS p.2.2.1.

SK is liable for all obligations described in clause 2.1.1 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 MO Client Service Point

Refer to CPS p.2.2.2.1.

MO is liable for all obligations of its authorized client service point described in clause 2.1.2.1 of this CP.

2.2.2.2. Liability of the MO Help Line

Refer to CPS p.2.2.2.2.

MO is liable for all obligations of its Help Line described in clause 2.1.2.2 of this CP.

2.2.3. Liability of MO

MO is liable for all obligations described in clause 2.1.3 and elsewhere within this CP.

2.2.4. Limits of Liability

Refer to CPS p.2.2.3.

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/crls/eid/eid2007.crl.

Directory service is not applied.

2.4.2. Publication Frequency

The certificate revocation lists are published after each 12 hours.

2.4.3. Access Rules

Access to the information described in clause 2.4.1 is free of charge and not limited via public data network.

2.4.4. Directory Service

Directory service is not applied.

2.5. Audit

Refer to CPS p.2.5.

2.6. Confidentiality

Refer to CPS p.2.6.

3. Client identification

3.1. Identification of Client

The identity of the client shall be verified according to the identity verification procedure agreed with the MO.

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

The certificates are issued only to the public keys generated for client by MO.

3.3. Distinguished Name

Refer to CPS p.3.3.

The distinguished name of the client is composed according to the clause 7 of this document.

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

This clause describes the processing and terms of the certificate application.

4.1. Submission of Applications for Certificates

Refer to CPS p.4.1.

The application for certificates can only be submitted in the client service point of MO.
Client fills and signs the application for Mobile-ID service. A signed application for Mobile-ID service serves as a basis for the preparation of an application for the certificate. Identity verification procedure (refer to clause 3.1) must take place prior to the submission of the certificate application.

The contents and procedure of submission of the application for certificate must meet the minimum requirements of the Digital Signatures Act [6].

Client agrees with “The terms and conditions of use of Mobile-ID certificates [3] along with the submission of the application for certificate.

Additional information is available on the web pages of MO and http://www.sk.ee

4.2. Processing of Applications for Certificates

Upon processing the applications for certificates the correctness and completeness of the information supplied 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 MO. The decision is based on the results of identity verification, correctness of the information supplied and on the client’s right to have Mobile-ID certificates according to the legislation of the area of operation of the MO.

The client shall be informed of the decision immediately in the MO client service point.

4.2.2. Certificate Issuance

The private keys of the generated key pair shall be loaded onto the Mobile-ID SIM card and the public keys forwarded to the MO by the producer of the Mobile-ID SIM card. The certificates corresponding to the application are issued by SK upon automated authenticity and integrity verification of application data forwarded by MO. The certificates are issued to the client upon issuance of the Mobile-ID SIM card.

The certificates issued by SK shall be in inactive state. The certificates can not be used prior to activation of certificates. The activation of Mobile-ID certificates is carried out as a separate process (refer to clause 4.2.3).

Upon application for new certificates for a Mobile-ID SIM card that already has valid certificates; new Mobile-ID SIM card shall be issued in the client service point of MO.

4.2.3. Certificate Activation

A separate web application is to be used by the certificate holder for activating the certificates which aims to enhance the verification of identity. The certificates can be activated via the web application using the national ID-card of Republic of Estonia only.

The certificates can not be used prior to the completion of the certificate activation process.

4.2.4. Certificate Check-up and Verification

Refer to CPS p.4.2.4.

4.2.5. Certificate Renewal

The certificate renewal is not applied.

The certificates that are expired or revoked will be replaced with issuance of a new Mobile-ID SIM card in the client service point of MO.

4.3. Applications for Suspension and Revocation of Certificates

Refer to CPS p.4.3.

4.4. Suspension of Certificates

Refer to CPS p.4.4.

Suspension of certificates is possible:

- In client service points of MO;
- By telephoning the MO Help Line.

The identity of the applicant shall be verified according to the identity verification procedure (refer to clause 3.1) while calling the MO Help Line and in client service point of MO. The personal data details shall be compared to the data recorded into the subscription contract of Mobile-ID.

The document's data used within identity verification process shall not be recorded while accepting the application for suspension of certificates in the client service point of MO.

4.5. Termination of Suspension

Refer to CPS p.4.5.

The suspension of certificates can be terminated in a client service point of MO.

The identity of the applicant shall be verified according to the identity verification procedure (refer to clause 3.1).

The application for termination of suspension of certificates must include:

- Applicant's forename and surname;
- The signature of the applicant;
- The name and the personal id-code of the suspended certificate holder;
- The basis for termination of suspension of certificates.

The document's data used within identity verification process shall be recorded in the client service point while accepting the application.

4.6. The Certificate Revocation

4.6.1. The Powers of Revoking a Certificate

Refer to CPS p.4.6.1.

In addition, the MO is authorized to revoke a certificate without the certificate holder's participation in the following cases:

- The subscription contract is terminated with MO according the general conditions of MO and the client has authorized MO for such operation;
- The subscription of Mobile-ID service is terminated by the holder of the phone number;
- Client substitutes the SIM card;
- Client substitutes the communications service provider.

4.6.2. Submission of Application for Revocation

Refer to CPS p.4.6.2.

Revocation of certificates is possible in the client service point of MO.

The identity of the applicant shall be verified according to the identity verification procedure (refer to clause 3.1).

The application for revoking a certificate must contain:

- Applicant's forename and surname;
- The signature of the applicant;
- The name and the personal id-code of the certificate holder;
- The basis for revocation of certificates.

The document's data used within identity verification process shall be recorded in the client service point while accepting the application.

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

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.

5.2.2. Other Requirements. Storage of Mobile-ID SIM cards

The Mobile-ID SIM cards shall be stored in the client service point of MO according to the internal security regulations.

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

Refer to CPS p.6.1.2.

6.1.2.1. Creating the Client Keys

The keys created in the formation of at least 1024-bit RSA algorithm key length. The Mobile-ID SIM card manufacturer is required to submit the confirmation that the keys are generated according to best practice and are unique along with the SIM cards and corresponding public keys.

The client keys are protected with PIN codes or activation codes known only to the client.

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

The confidentiality and unauthorized non-usage of the generated private keys and activation codes until the handover of the Mobile-ID SIM card used for storing keys and activation codes of the keys to the client is warranted by MO and by the manufacturer of the Mobile-ID SIM card.

The activation codes shall be printed in one copy straight to the security area of the Mobile-ID SIM card which is handed over to the client unopened. The client has the obligation to refuse to adopt a Mobile-ID SIM card with the breached security area.

6.1.2.3. Activation of Client's Private Key

Subsequent to insertion of three false activation codes (PIN codes) the Mobile-ID functionality of the SIM card shall be blocked. The PUK code of the Mobile-ID SIM card handed over to the client can be used to unblock the Mobile-ID functionality.

The functions of authentication and signing shall be blocked independently. Subsequent to insertion of three false PUK-codes, the Mobile-ID functionality shall be blocked permanently.

If the PUK codes are lost or the PUK code is blocked, the client has to refer to the client service point for a substitute new Mobile-ID SIM card.

6.1.2.4. Backup and Deposition of Client's Keys

There shall be neither backup nor depositions of the private keys of the client under any circumstance.

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. Profile of Certificates

SK shall issue certificates matching X.509 version 3 according to the guidelines of suggestive standard RFC 3280 [4]. An issued Mobile-ID certificate contains at least the following data:

Field	OID	Description
Version		Version number of the certificate format: V3
Serial number		Unique identifier of the certificate assigned by the certification authority, the serial number of the certificate.
Signature Algorithm		The signature algorithm of the certificate: sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer		The data of the certificate issuer.
id-at-countryName	2.5.4.6	Country identifier: EE
id-atorganizationName	2.5.4.10	The name of the issuer: AS Sertifitseerimiskeskus
id-atorganizationalUnitNam	2.5.4.11	Description of the certification service: Sertifitseerimisteenused

e		
id-at-commonName	2.5.4.3	Common name of certification authority: EID-SK 2007
Subject		The data of the certificate holder
id-at-serialNumber	2.5.4.5	Personal ID-code of the client
id-at-givenName	2.5.4.42	Forenames of the client
id-at-surname	2.5.4.4	Surname of the client
id-at-commonName	2.5.4.3	Common name of the certificate in the format of: <SURNAME>,<FORENAMES>,<ID-CODE>
id-atorganizationalUnitName	2.5.4.11	Application area of the certificate In a certificate facilitating digital authorization: *mobile authentication* In a certificate facilitating digital signature: *mobile signature*
id-atorganizationName	2.5.4.10	The name of the communications service provicer
id-at-countryName	2.5.4.6	The issuer country code on the certificate application according to the guidelines in RFC 3280 of the personal ID-code.
Valid from		The starting time of validity of the certificate. Information is coded according to the guidelines in RFC 3280.
Valid to		The ending time of validity of the certificate. Information is coded according to the guidelines in RFC 3280. In general 1825 days (5 years) counting from the certificate issuance.
Public key		Public key in form of ASN.1 which contains a modulus at least 1024 bits and exponent of 3 bytes (65537).
Key Usage	2.5.29.15	Major area of application of the certificate In a certificate facilitating digital authentication there are set following attributes denoting key usage: *Digital Signature, Key Encipherment, Data Encipherment;* In a certificate facilitating digital signature there is set following attribute denoting key usage: *Non-Repudiation*
Extended Key Usage	2.5.29.37	Extended area of application of certificate. In use only in the certificate facilitating digital authentication: Client Authentication (1.3.6.1.5.5.7.3.2) E-mail Protection (1.3.6.1.5.5.7.3.4)
Certificate Policies	2.5.29.32	Reference to the principles based on while issuing the certificate. The referring shall contain the unique identifier as well as the location at the public web site of SK of the policy document: Policy Identifier= 1.3.6.1.4.1.10015.11.1.1.2 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/mid/
Authority Key Identifier	2.5.29.35	Hash of the public key of the certification authority.
Subject Key Identifier	2.5.29.14	Hash of the public key of this certificate.
CRL Distribution Points	2.5.29.31	http://www.sk.ee/crls/eid/eid2007.crl
Basic Constraints	2.5.29.19	Limitation which defines the type of the certificate (end user certificate): *Subject Type=End*

		Entity, Path Length Constraint=None
1.3.6.1.5.5.7.1.3 id-pe-qcStatements	1.3.6.1.5.5.7.1.3	Identifier of a qualified certificate. Extension that indicates the compliance to the requirements set to the qualified certificates of the certificate issued (refer to RFC 3739).
Thumbprint algorithm		Sha1 algorithm is used to generate the key hash.
Thumbprint		Hash of the certificate.

7.2. *Profile of Revocation Lists*

The certificate revocation list (CRL) is published twice a day and contains the certificates which are suspended as well as the certificates which are revoked. The revocation list is formed accordingly to the format of x.509 version 2 revocation lists (refer to RFC 3280) [4].

CRL component	OID	RFC 3280	Notes
CertificateList		5.1.1	
tBSCertList		5.1.1.1	Follow the table
signatureAlgorithm		5.1.1.2	Signature algorithm of the CRL: sha1WithRSAEncryption
signatureValue		5.1.1.3	Signature
tBSCertList		5.1.2	
version		5.1.2.1	Format version of the CRL: V2
signature		5.1.2.2	Value depends on the algorithm used.
Issuer		5.1.2.3	The common name of the issuer in UTF8 encoding.
id-at-countryName	2.5.4.6		EE
id-at-organizationName	2.5.4.10		AS Sertifitseerimiskeskus
id-atorganizationalUnitName	2.5.4.11		Sertifitseerimisteenused
id-at-commonName	2.5.4.3		EID-SK 2007
thisUpdate		5.1.2.4	The date and time of the issuance of the CRL. UTC is used until 2049. The GeneralisedTime shall be used later on.
nextUpdate		5.1.2.5	Date and time of the issuance of the next CRL. UTC is used until 2049. The GeneralisedTime shall be used later on.
revokedCertificates		5.1.2.6	The list of revoked or suspended certificates.
Revocation Date	2.5.29.24		The date and time of revocation/suspension of the certificate.
Reason code	2.5.29.21		The basis of operation (suspended certificates are

			marked with reason code 6 – Certificate Hold)
Serial Number			The serial number of the revoked or suspended certificate.
CRL Number	2.5.29.20	5.2.3	The serial number of the CRL, unique identifier assigned by the certification authority.
Authority Key Identifier	2.5.29.35	5.1.2.7	The identifier corresponding to the public key (of the corresponding private key used for signing this CRL) which is important to create a chain of certificates issued by SK.
Issiuing Distribution Point	2.5.29.28		Distribution point of the CRL.

On the field authorityKeyIdentifier the identifier corresponding to the public key (of the corresponding private key used for signing this CRL) is used which is important to create a chain of certificates issued by SK.

The field CRL number is monotonously increasing and determines the serial number of specific CRL issued by SK.

The provider of certification services may also use the CRL Entry extensions if possible following the requirements and recommendations of RFC 3820.

8. Management of Certification Policy

Refer to CPS p.8.

This CP and referred documents [1], [2], [4], [5] are published on the website of SK and document [3] is published on the web pages of SK and MO.

Any substantive changes shall be in the coordination with the MO.

9. Referred and Related Documents

Referred documents:

[1] Certification Practice Statement of AS Sertifitseerimiskeskus (CPS)

[2] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[3] Terms and Conditions of Use of the Mobile-ID Certificates. AS Sertifitseerimiskeskus

[4] RFC 3280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile

[5] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

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