AS Sertifitseerimiskeskus
Certification Policy of the digital identity card in form of the Mobile-ID

Version 1.1
OID: 1.3.6.1.4.1.10015.1.3.1.1
Effective since 01.02.2011

Version Information		
Date	Version	Changes/Updates/Amendments
01.02.2011	1.1	Final version
11.01.2011	0.1	Initial draft

Requirements for the digital certificates, identity verification, and allow for servicing of the digital identity cards in form of the Mobile-ID (hereinafter referred to as Mobile-ID) issued by Republic of Estonia (hereinafter referred to as EV).

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” 9 which is registered in the National Register of Certification (NRC). 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 chapter 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	A written application filed and digitally signed by the client in the web-based PPA environment for acquiring Mobile-ID 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.
PPA	The Police and Border Guard Board of the Republic of Estonia, the issuer of the Mobile-ID.

SK	AS Sertifitseerimiskeskus - provider of the certification services.
STO	A provider of certification services that is registered in the Register of the Certification.

1.4. *Identifying the Certification Policy*

This CP is identified by OID: 1.3.6.1.4.1.10015.1.3.1.1

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
CC attribute in IANA register	10015
Certification service attribute	1.3
CP version attribute	1.1

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.

The certificates are issued to the Mobile-ID. The SK provides the certification service as a registered STO under a contract signed between PPA and SK. The PPA is responsible for the issuance of the Mobile-ID. For issuance of the Mobile-ID SIM cards there are contracts signed between SK and MO. SK has contractually delegated the responsibilities described in section 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.

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 oral applications for suspending certificates by checking applicant's identity in advance according to the procedure of identity verification (refer to chapter 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. PPA

PPA

- Accepts the applications for Mobile-ID certificates, decides the approval of the applications and forwards the approved certificate applications to the SK.
- Accepts the applications of revocation of the Mobile-ID certificates, decides the approval of the applications and forwards the approved certificate revocation applications to the SK.

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

1.5.4. User

1.5.4.1. 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 if he/she has a legal right. The certificates are assigned to the Mobile-ID SIM card. 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 a separate document named as „Sertifikaadid Eesti Vabariigi isikutunnistusel" [7].

The client has to have an opportunity to get acquainted with "The terms and conditions of using certificates of the digital identity card in the form of Mobile-ID" [3] prior to signing the Mobile-ID contract.

1.5.4.2. Relying Party

Refer to CPS p.1.2.3.2.

1.5.5. 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.

PPA kodakondsus- ja migratsiooniosakond

Endla 13,
15179 Tallinn
Help line +372 612 3000
Phone +372 612 3300
Fax +372 612 3009
E-mail: teeninduskeskus@politsei.ee
http://www.politsei.ee

The PPA help line for solving matters regarding Mobile-ID certificate requests, processing the applications and for advisory of the service point employees is accepting calls on business days from 08:00 – 17:00, phone +372 612 3000.

Client Service Points
The list and contact details of the client service points are referred from SK's website http://www.sk.ee and on 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 issuance of the Mobile-ID SIM cards and corresponding public keys presented by MO;
- Accept and register the certificate requests presented by PPA and issue the corresponding certificates;
- Accept, register and process applications presented by MO for suspending, terminating 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.

MO client service point hereby additionally undertakes to accept requests for:

- Mobile-ID SIM card issuance;
- Suspension of the certificates;
- Termination of suspension of the certificates;
- Change of phone number linked to the Mobile-ID SIM card.

While processing the abovementioned requests the MO client service point must verify:

- The accuracy and integrity of the requests;
- The identity of the applicant and his/her powers to carry 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 Mobile-ID SIM card 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 PPA

PPA is obligated to:

- Accept the digitally signed applications from clients for the issuance of the certificates assigned to the Mobile-ID SIM card;
- Accept the digitally signed applications from clients for the revocation of the certificates assigned to the Mobile-ID SIM card;
- Ensure the availability of the information about the service to the client.

While processing the abovementioned applications PPA must verify:

- The accuracy and integrity of the applications;
- The identity of the applicant and his/her powers to carry out the operation in accordance with the legislation effective.

PPA hereby additionally 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;
- Follow the availability and security requirements on the PPA's web based application submission system at least to the level of the requirements described in this CP
- Ensure that the employees, who 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 on address http://www.politsei.ee;
- Ensure the security with its internal security procedures while providing the service.

2.1.4. 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 SIM cards and certificates (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.

2.1.5. Obligations of Clients

Refer to CPS p.2.1.3.

The client is obligated to:

- Present the true and correct personal data to the MO while submitting an application for the Mobile-ID SIM card;
- Present the true and correct personal data to the PPA while submitting an application for the Mobile-ID certificates;
- Notify the PPA in case of change of the personal data in accordance with the effective legislation;
- Notify the MO or the PPA in case of Mobile-ID becoming unusable, lost or destroyed in accordance with the effective legislation.
-

In case of a change in his/her personal details stored in the certificate the client must pretend to new a new Mobile-ID SIM card and Mobile-ID certificates in order to continue usage of the Mobile-ID service.

2.1.6. Obligations of Relying Party

Refer to CPS p.2.1.4.

2.1.7. Obligations of Public Directory

Refer to CPS p.2.1.5.

No additional requirements are foreseen for operation of the public directory.

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 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 chapter 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 chapter 2.1.2.2 of this CP.

2.2.3. Liability of MO

MO is liable for all obligations described in chapter 2.1.4 and elsewhere within this CP.

2.2.4. Liability of PPA

PPA is liable for all obligations described in chapter 2.1.3 and elsewhere within this CP.

2.2.5. 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

2.4.2. Publication Frequency

Refer to CPS p.2.4.1

The certificate revocation lists are published after each 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 accordance of this CP are published in the public directory that is available at ldap://ldap.sk.ee.

The certificates that are suspended or revoked shall be deleted from the public directory. The certificates that have their suspension terminated shall be republished.
The expired certificates shall be deleted from the public directory on the next day following the expiration.

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

PPA shall verify the client's identity in accordance with the effective legislation.

MO shall verify the client's identity in accordance with the internal procedure of the identity verification.

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.

Client's distinguished name is compiled according to the certificate profile described in a separate document named as „Sertifikaadid Eesti Vabariigi isikutunnistusel" [7].

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

This chapter 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 web based application submission environment of PPA.

Client fills and signs digitally the application for Mobile-ID certificates. A signed application for Mobile-ID certificates serves as a basis for the preparation of an application for the certificates. The verification of identity takes place electronically prior to the submission of the application.

The contents and procedure of submission of the application for certificate must meet the minimum requirements of the digital signatures act.

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

Additional information is available on the web page of the PPA http://www.politsei.ee

4.2. Processing of Applications for Certificates

The processing terms and conditions are stated by the effective legislation. 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 PPA. 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 Republic of Estonia.

In case of positive decision, the PPA forwards the request for one certificate that facilitates digital signature and one that facilitates digital identification to the SK.

During the decision making, there is an automated application verification mechanism in progress. The client shall be notified via the web based application submission environment of the PPA.

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 MO issues the Mobile-ID SIM card to the client and forwards the public keys to the SK. The client submits an application for certificates in the web based application submission environment of the PPA. The certificates corresponding to the application are issued by SK upon automated authenticity and integrity verification of application data forwarded by PPA.

The certificates issued by SK shall be in active state.

4.2.3. Certificate Activation

The certificates issued in active state.

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.

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:

- At 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 chapter 3.1) while calling the MO helpline 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 chapter 3.1).

The application for termination of suspension of certificates must include:

- Holder'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.

The PPA is authorized to revoke a certificate after the Mobile-ID is revoked.

4.6.2. Submission of Application for Revocation

Refer to CPS p.4.6.2.

Revocation of certificates is possible in the web based application submission environment of the PPA. The identity of the applicant shall be verified in accordance with the effective legislation.

The application for revoking a certificate must contain:

- Holder'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.

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 hand over 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 Mobile-ID SIM card and to the web based application submission environment of the PPA for applying for the new certificates.

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

The technical profiles of certificates and revocation lists are described in a separate document named as „Sertifikaadid Eesti Vabariigi isikutunnistusel" [7].

8. Management of Certification Policy

Refer to CPS p.8.

This CP and referred documents [1], [7] are published on the website of SK and document [3] is published on the web pages of SK, PPA and MO.

Any substantive changes shall be in the coordination with the PPA and 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 Certificates issued to a digital identity card in form of Mobile-ID. 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.
[7] Sertifikaadid Eesti Vabariigi isikutunnistusel;
[8] The Identity Documents Act, RT I 1999, 25, 365.