Agreement on Cooperation concluded on 15th September 2006 between AS Sertifitseerimiskeskus and JSC Omnitel

Appendix 18

Certification Policy for Lithuanian Mobile-ID

Version 2.0
OID: 1.3.6.1.4.1.10015.14.1.2
Valid from 01.01.2016

Version information		
Date	**Version**	**Changes/Updates/Amendments**
01.12.2015	2.0	Updated chapter 6.1.2.1 - Changed the description of creating the client keys. Updated chapter 8 - updated management of this certification policy.
16.03.2015	1.1	Cosmetic changes and update to the document structure.
01.10.2007	1.0	First public edition.

Requirements on the Lithuanian Mobile-ID certification service with the purpose of issuing and servicing certificates which facilitate digital signature and digital identity verification of persons. The service is provided by Lithuanian mobile operator Omnitel.

1. Introduction

1.1. Overview

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

This CP is based on the document titled "AS Sertifitseerimiskeskus – Certification Practice Statement" [1] (hereafter the CPS) that is registered at the Estonian National Register of Certification (NRC). The CPS forms the basis for the provision of certification services, whereas this CP further specifies the principles outlined in the CPS for Lithuanian Mobile-ID certification service.

In the case of any discrepancies between the CP and CPS the provisions of this CP shall prevail. In case of any discrepancies between the English original document and the Lithuanian translation the English original shall prevail.

This CP extends only to the digital certificates of Lithuanian Mobile-ID (hereafter Mobile-ID) operated by Omnitel and 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 servicing 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 identity verification of persons.
Activation code	sPIN code known only to the Client for activation of Client's private key.
Mobile-ID SIM card application	Written application which has to be filled and signed manually by Client for acquiring Mobile-ID SIM card.
Client	For the purposes of this CP the Client is the Mobile-ID user.
Certificate application	Electronically sent application which has to be signed digitally with sPIN 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 – Omnitel.
SK	AS Sertifitseerimiskeskus – provider of certification services.

1.4. Identifying the Certification Policy

This CP is identified by **OID: 1.3.6.1.4.1.10015.14.1.2**

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
CC attribute in IANA register	10015
Certification service attribute	14.1
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 chapter 1.5.2 to MO.

1.5.2. SK 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 (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 revocation 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.

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 identity verification.

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

Client's distinguished name is compiled according to the "Profiles of Lithuanian Mobile-ID Certificates and Certificate Revocation List" [6].

The Client has to have an opportunity to get acquainted with the general terms and conditions of certificate usage 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 identity verification of persons.

Certificates for digital signature can be used for digital signature as defined in the Law on Electronic Signature of Republic of Lithuania.

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
Commercial registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Phone +372 610 1880
Fax +372 610 1881
E-mail: info@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 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.

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 register the certificate applications presented by MO and issue respective certificates;
- Accept, register and process applications presented by MO for 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 revocation of Mobile-ID certificates and verify the correctness and integrity of these applications. While processing operation, 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 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.

The client must be informed, that both private keys (and their corresponding certificates) can be activated by using the same activation code; it is the client's responsibility to notice and prevent illegal attempts of producing legally binding signatures.

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 apply for new Mobile-ID certificates.

2.1.5. Obligations of Relying Party

Refer to CPS p.2.1.4.

2.1.6. Obligations of Public Directory

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 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 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 2.1.3 and elsewhere within this CP.

2.2.4. Limits of Liability

Refer to CPS p.2.2.3

SK has liability for security incidents according to insurance policy. Upper limit of liability is at least 40 000 euros per certificate per security incident.

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/repositoorium/CRL/.

Directory service is not applied.

2.4.2. Publication Frequency

Refer to CPS p.2.4.2

The certificate revocation lists are published not less than in every 12 hours.

2.4.3. Access Rules

Access to the information described in chapter 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. Identity Verification

3.1. Client Identity Verification

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 "Profiles of Lithuanian Mobile-ID Certificates and Certificate Revocation List" [6].

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.

Client fills and signs Mobile-ID SIM card application in the Client Service Point of MO. The verification of identity according to the identity verification procedure (refer to chapter 3.1) must take place prior to the issuance of the Mobile-ID SIM card.

Certificate application can only be submitted by the Client.
The digital verification of identity 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 Law on Electronic Signature of Republic of Lithuania.

Client agrees with general terms and conditions of certificate usage along with the submission of the application for certificate.

Additional information is available on the web pages of MO.

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 public keys are issued by SK upon automated authenticity and integrity verification of application data forwarded by Client. The certificates are issued to the Client after submission of certificate application.

The certificates issued by SK shall be in active state.

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 Check-up and Verification

Refer to CPS p.4.2.4.

4.2.4. 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.

Suspension of Certificates is not applied.

4.4. The Certificate Revocation

4.4.1. 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.

4.4.2. Submission of Application for Revocation

Refer to CPS p.4.6.2.

Revocation of certificates is possible:

- At Client Service Point 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).

At Client Service Point 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.

By MO help line in the case of revocation of certificates the identity of the applicant shall be verified according to the identity verification procedure (refer to chapter 3.1).

The document's data used within identity verification process shall be recorded in the Client Service Point while accepting the application.

4.4.3. Procedure of Revocation

Refer to CPS p.4.6.3.

4.4.4. Effect of Revocation

Refer to CPS p.4.6.4.

Directory service is not applied.

4.5. Procedures Ensuring Tracking

Refer to CPS p.4.7.

4.6. Action in an Emergency

Refer to CPS p.4.8.

4.7. 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 Client keys must be generated on the SIM card or in a dedicated hardware security module, from which the generated keys are transferred to the SIM card.

In case if a dedicated hardware module is used, it must be ensured that the generated keys have been erased from the security module after transfer and there is no possibility to store the keys outside the SIM card during the transfer.

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 sPIN code or activation code known only to the Client.

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

The confidentiality and non-utilisation of the generated private keys and activation code until the hand over of the Mobile-ID SIM card used for storing keys and activation code of the keys to the Client is warranted by MO and by the manufacturer of the Mobile-ID SIM card.

The activation code 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

There is only one activation code for different keys of the Client.

Subsequent to insertion of five false activation codes (sPIN codes) the Mobile-ID functionality of the SIM card shall be blocked.

If the SIM card has the Mobile-ID functionality blocked, the Client has to refer to the Client Service Point for Mobile-ID SIM card replacement.

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 the certificates and certificate revocation lists (CRLs) are described in „Lithuanian Mobile-ID Certificates and Certificate Revocation List Profiles" [6].

8. Management of Certification Policy

Refer to CPS p.8.

This CP and referred documents [1], [6] are published on the website of SK; the general terms and conditions of certificate usage is published on the website of MO.

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.

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

SK shall inform MO about any substantive changes in Certification Practice Statement of AS Sertifitseerimiskeskus (CPS) that may concern this CP.

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] RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile;
[4] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
[5] Law on Electronic Signature of Republic of Lithuania;
[6] Profiles of Lithuanian Mobile-ID Certificates and Certificate Revocation List.