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

Appendix 17

AS Sertifitseerimiskeskus Profiles of Lithuanian Mobile-ID Certificates and Certificate Revocation List

Version 1.1
Valid from 16.03.2015

Version information		
Date	**Version**	**Modifications**
16.03.2015	1.1	Minor updates and cosmetic changes.
01.10.2007	1.0	Version 1.0

1. General Information

This document describes the profiles and minimum requirements for Lithuanian Mobile-ID, operated by Omnitel, certificates and certificate revocation lists.

2. Definitions and Abbreviations

Abbreviation	Definition
Mobile-ID	Service on Mobile phone which in addition to regular cellular service usage facilitates functionality of digital signature and digital identity verification of persons.
Certificate owner	User of Omnitel Mobile-ID, whose personal information is related to the Mobile-ID digital data.

3. Technical Profile of Certificates

SK issues X.509 version 3 certificates in accordance to guidelines outlined in advisory standard RFC 5280 [1].

3.1. Mandatory Information

Certificates issued to Lithuanian Mobile-ID must contain at least the following information:

Field	OID	Description
Version		Certificate format version number: V3
Serial number		Certificate serial number, unique ID number assigned to the certificate by the issuer.
Signature Algorithm		Certificate signature algorithm:sha1RSA (OID: 1.2.840.113549.1.1.5)
Issuer		Certificate issuer data.
e-mailAddress	1.2.840.113549.1.9.1	e-mail address of the issuer: pki@sk.ee
id-at-countryName	2.5.4.6	Country code: EE
id-atorganizationName	2.5.4.10	The name of the issuer: AS Sertifitseerimiskeskus
id-at-commonName	2.5.4.3	Distinguished name of the issuer: EID-SK 2011
Subject		Certificate owner data.
id-at-serialNumber	2.5.4.5	Personal identity number of certificate owner.
id-at-givenName	2.5.4.42	Forenames of certificate owner.
id-at-surname	2.5.4.4	Surname of certificate owner.
id-at-commonName	2.5.4.3	common name of Certificate in the form of: <SURNAME>,<FORENAMES>,<PERSONAL IDENTITY NUMBER>
id-atorganizationalUnitName	2.5.4.11	Certificate area of use: Digital identity verification certificate: *Mobile Authentication;* Digital signing certificate: *Mobile Signature.*
id-atorganizationName	2.5.4.10	The name of the communications service provider.
id-at-countryName	2.5.4.6	Code of the country that has issued the personal identification number indicated in the certificate application in accordance to RFC 5280 guidelines.
Valid from		The beginning of the certificate validity period. Information coded pursuant to RFC 5280 guidelines.
Valid until		The end of the certificate validity period. Information coded pursuant to RFC 5280 guidelines. Generally date of issuance + 1825 days (5 years).
Public key		Public key in ASN.1 format composed of at least 1024 bit module.
Key Usage	2.5.29.15	Key usage of Certificate In case of Certificate enabling digital identity verification the following key usage areas are

Field	OID	Description
		indicated: *Digital Signature, Key Encipherment, Data Encipherment;* In case of Certificate enabling digital signing only one key usage area is indicated: *Non-Repudiation*
Enhanced Key Usage	2.5.29.37	Enhanced Key Usage. Used only in Certificates enabling digital identity verification: Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	2.5.29.32	Certification Policies. Reference to the guiding principles upon issue of Certificate. Reference both to the unique identifier – OID – and also its location on SK public website: Policy Identifier= 1.3.6.1.4.1.10015.14.1.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/cps/mid
Authority Key Identifier	2.5.29.35	Certifying authority public key hash.
Subject Key Identifier	2.5.29.14	Current certificate public key hash.
CRL Distribution Points	2.5.29.31	http://www.sk.ee/repository/crls/eid2011.crl
Basic Constraints	2.5.29.19	Constraint indicating the type of Certificate (End User Certificate): *Subject Type=End Entity, Path Length Constraint=None*
Thumbprint algorithm		Sha1 algorithm is utilised for hashing.
Thumbprint		Certificate hash.

3.2. Optional Information

In addition to mandatory information the certificates issued to Lithuanian Mobile-ID may also contain the following information:

Field	OID	Description
1.3.6.1.5.5.7.1.3 id-pe-qcStatements	1.3.6.1.5.5.7.1.3	Qualified Certificate Identifier. The certificate shall contain the following identifiers: - Qualified Certificate Identifier pursuant to Annex I and II of the EU directive on electronic signatures 1999/93/EC {id-etsi-qcs-QcCompliance }, {0.4.0.1862.1.1} -Identifier that indicates that the Private Key linked to the Certificate is located on a secure signing device pursuant to Annex III EU directive on electronic signatures 1999/93/EC {id-etsi-qcs-QcSSCD}, {0.4.0.1862.1.4}

3.3. Example certificate

Certificate Field	Example of content	Comments
VERSION	**V3**	Constant
SERIAL NUMBER	**41db f209**	Unique number inside CA
SIGNATURE ALGORITHM	**sha1RSA**	Constant

ISSUER	CN = **EID-SK**
	SN = **1**
	O = **AS Sertifitseerimiskeskus**
	C = **EE**
		Constant

VALID FROM	***10 may 2005. a. 17:48:14***	Date, Time in GMT/CET
VALID TO	***11 may 2010. a. 17:48:14***	Defined by RA, see RP
SUBJECT	*Serial Number*=**37102230096** *GN* = ***Ramūnas*** *SN* = ***Šablinskas*** *CN* = ***Ramunas,Sablinskas,37102230096*** *OU* = ***mobile signature*** O = **OMNITEL** C = **LT**	Note: GN and SN fields contain national characters. CN contains only latin characters.
PUBLIC KEY	**3081 8902 8181 00C2 AFE1 0488 4987 6C2D 4382 78FF D4E6 9F2C AEE7 2676 F3E7 33C1 8A38 706C 0F95 DF89 596A 95B8 B808 5A09 9FC7 4390 B642 AE78 AB46 00AF 647A 283B 7A44 7E25 1827 C0F5 06A0 30C1 75C1 8159 FAC5 455F 6BDB 844A 8665 1A36 2126 1370 A480 E9D5 719C 6F7D E8F5 04BF 87BF 25C3 3F20 9635 A273 05EE EB64 20BE A39E 42C6 B1D2 58A6 5425 B302 0301 0001**	*RSA(1024 bits)*
EXTENDED KEY USAGE	Client Authentication(**1.3.6.1.5.5.7.3.2**)	
CERTIFICATE POLICIES	Policy Identifier=1.3.6.1.4.1.10015.10.1.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/repository/eid-sk-1.0.pdf	
QUALIFIED CERTIFICATE STATEMENT	(1.3.6.1.5.5.7.1.3)	Constant As of RFC3739
AUTHORITY KEY IDENTIFIER	***KeyID=b4 bc 27 70 9e 07 cb c5 64 c3 32 19 6c dc 1f 7a 29 2e 37 a5***	Example
SUBJECT KEY IDENTIFIER	***17 b2 52 f8 40 b6 82 94 6e d6 a9 41 71 85 74 e4 79 82 4f b8***	Example
KEY USAGE	**Digital Signature , Key Encipherment , Data Encipherment(B0), Non-Repudiation (40)**	Constant
CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/eid-sk/eid.crl	Constant (example)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None	Constant
THUMBPRINT ALGORITHM	**sha1**	Constant
THUMBPRINT	**973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1**	Example

4. Certificate Revocation List (CRL) Profile

The Certificate Revocation List is published twice daily and it lists those certificates that have either been suspended or revoked. The list is compiled in accordance to the certificate revocation list format x.509 version 2 (refer to RFC 5280) [1].

CRL component	**OID**	**Ref RFC 5280**	**Notes**
CertificateList		5.1.1	
tBSCertList		5.1.1.1	Please see next section of the table.
signatureAlgorithm		5.1.1.2	Certificate Revocation List signing algorithm: sha1WithRSAEncryption.
signatureValue		5.1.1.3	Signature.
tBSCertList		5.1.2	
version		5.1.2.1	CRL format version: V2.
Signature		5.1.2.2	Value depends on algorithm used.
Issuer		5.1.2.3	UTF8 coded CRL issuer distinguished name.
e-mailAddress	1.2.840.113549.1.9.1		pki@sk.ee
id-at-countryName	2.5.4.6		EE
id-at-organizationName	2.5.4.10		AS Sertifitseerimiskeskus
id-at-commonName	2.5.4.3		EID-SK 2011
thisUpdate		5.1.2.4	CRL publication date and time. UTC time.
nextUpdate		5.1.2.5	Date of the next CRL update. UTC time. The update interval for the CRL is defined in the Certification Policy [3].
revokedCertificates		5.1.2.6	List of revoked or suspended certificates.
Revocation Date	2.5.29.24		Date and time of suspension/revocation.
Reason code	2.5.29.21		Reason (in case of certificates with suspended validity 6 – Certificate Hold)
Serial Number			Serial number of the revoked/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		CRL distribution point: http://www.sk.ee/repository/crls/eid2011.crl

Field „AuthorityKeyIdentifier" contains the relevant SK public key (equivalent private key used for signing the CRL) identifier, an important component in the process of establishing SK certificate chain.

Field „CRL number" is a monotonously growing number that is used for determining the specific CRL serial number issued by SK.

In addition, the certification service provider may use CRL Entry extension according to RFC 5280 [1] guidelines and recommendations.

5. Referenced Documents

Referenced documents:

[1] RFC 5280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile;
[2] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
[3] Certification Policy for Lithuanian Mobile-ID.