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

Appendix 18

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

Version 2.0
Valid from 01.01.2016

Version information		
Date	**Version**	**Modifications**
01.12.2015	2.0	Updated chapter 3.1 - updated mandatory information in certificate. Changed signature algorithm type, certificate valid until time, public key types, removed thumbprint information, changed certificate policies. Updated chapter 3.2 - changed optional Information. Updated chapter 3.3 - updated example certificates. Updated chapter 4 - specified time of publication of CRL and changed signature algorithm of CRL. Updated chapter 5 - updated references of documents.
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: sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
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.

Field	OID	Description
		Information coded pursuant to RFC 5280 guidelines. Generally date of issuance + 1825 days (5 years).
Public key		The field contains the public key of the certificate owner along with its presentation algorithm. The following encryption algorithm identifiers (**AlgorithmIdentifier**) are used in certificates of the Documents: • **rsaEncryption** {1.2.840.113549.1.1.1} • **ecPublicKey** {1.2.840.10045.2.1}, prime256v1 {1.2.840.10045.3.1.7}. Public key in ASN.1 format composed. In case of rsaEncryption public key is composed of at least 2048 bit module and in case of ecPublicKey at least 256 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 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 and Certification Practice Statement. 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=1.3.6.1.4.1.10015.14.1.2 Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier:Notice text=https://www.sk.ee/en/repository/CP/ Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sk.ee/en/repository/CPS/
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*

3.2. Optional Information

In addition to mandatory information the certificates for digital signing 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}

3.3. Example certificate

Digital Signature Certificate

Certificate Field	Example of content	Comments
VERSION	**V3**	Constant
SERIAL NUMBER	**05 35 e2 69 25 b2 f9 22 56 3c 64 52 45 de c3 4d**	Unique number inside CA
SIGNATURE ALGORITHM	**sha256RSA**	Constant
ISSUER	E = pki@sk.ee CN = EID-SK 2011 O = AS Sertifitseerimiskeskus C = EE	Constant
VALID FROM	***14 december 2015. a. 17:48:14***	Date, Time in GMT/CET
VALID TO	***12 december 2020. a. 23:59:59***	Defined by RA, see RP
SUBJECT	*SERIALNUMBER* = **37102230096** *G* = ***Ramūnas*** *SN* = ***Šablinskas*** *CN* = ***Ramūnas,Šablinskas ,37102230096*** *OU* = ***mobile signature*** O = **OMNITEL** C = **LT**	
PUBLIC KEY	**30 82 01 0a 02 82 01 01 00 ba ea e3 d1 c4 c2 75 71 74 2b 68 14 1f be c3 a1 03 f1 e7 a6 bd 50 8a 98 ab e8 64 08 69 c3 92 52 9e f3 f2 4a 4f ee b6 f8 47 6a 65 d9 62 df b3 a2 9c a6 5c 36 4d 95 22 b4 cd 97 e8 49 0d 6d 63 2d 60 4c fb 31 57 f5 74 33 34 15 dd 76 99 c2 69 57 c0 96 37 54 e5 76 e7 36 59 0b e7 77 98 26 23 ad 07 a9 8c bc 9c d8 1a 8c ac 4f 04 8b 9a 741c f5 25 ce 76 f4 39 bd 9e f0 34 34 58 7d bf 86 65 c4 a5 52 04 28 ac 25 59 4a 15 58 39 79 82 34 f8 87 24 69 1a 52 33 84 08 90 ab 8a d9 f7 d7 c6 92 60 c4 d4 03 bb 3e 32 91 de 8b b6 37 2e f4 b7 9a c7 fb 7d 28 34 84 11 83 1e b0 71 2d 6d c2 d1 b6 6b 40 7d 90 6b 1e 68 59 53 e3 66 83 3b 6c 0b 09 ef 09 7d ae 6e 7b 8b 53 ac 51 ad 83 f8**	RSA(2048 bits)

	cc bd be b2 b3 80 b9 2b 52 e9 a5 57 a8 29 b3 a6 63 ac 49 5a 88 c8 c6 9d 55 e7 5b 03 b7 3b c7 34 42 61 e2 99 02 03 01 00 01	
ENHANCED KEY USAGE	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	
CERTIFICATE POLICIES	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.10015.14.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice text=https://www.sk.ee/en/repository/CP/ [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sk.ee/en/repository/CPS/	
QUALIFIED CERTIFICATE STATEMENT	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	Constant As of RFC3739
AUTHORITY KEY IDENTIFIER	***KeyID=b1 10 97 02 fa dd 86 c6 78 41 a4 c3 32 88 fb fe 1f e7 c0 05***	Example
SUBJECT KEY IDENTIFIER	***1d c8 91 e9 25 ee 25 27 6f 97 de b2 c7 23 c2 23 24 5a 80 2c***	Example
KEY USAGE	**Non-Repudiation (40)**	Constant
CRL DISTRIBUTION POINTS	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/eid2011.crl	Constant (example)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None	Constant

Digital Authentication Certificate

Certificate Field	Example of content	Comments
VERSION	**V3**	Constant
SERIAL NUMBER	**18 a7 5a e7 9c 9d c4 9e 56 3c 64 53 76 78 0f a6**	Unique number inside CA
SIGNATURE ALGORITHM	**sha256RSA**	Constant
ISSUER	E = pki@sk.ee CN = EID-SK 2011 O = AS Sertifitseerimiskeskus C = EE	Constant
VALID FROM	***14 december 2015. a. 17:48:14***	Date, Time in GMT/CET
VALID TO	***12 december 2020. a. 23:59:59***	Defined by RA, see RP
SUBJECT	*SERIALNUMBER* = **37102230096** *G* = ***Ramūnas*** *SN* = ***Šablinskas*** *CN* = ***Ramūnas,Šablinskas*** **,37102230096** OU = **mobile authentication**	

	O = **OMNITEL** C = **LT**	
PUBLIC KEY	**30 82 01 0a 02 82 01 01 00 ba ea e3 d1 c4 c2 75 71 74 2b 68 14 1f be c3 a1 03 f1 e7 a6 bd 50 8a 98 ab e8 64 08 69 c3 92 52 9e f3 f2 4a 4f ee b6 f8 47 6a 65 d9 62 df b3 a2 9c a6 5c 36 4d 95 22 b4 cd 97 e8 49 0d 6d 63 2d 60 4c fb 31 57 f5 74 33 1c f5 25 ce 76 f4 39 bd 9e f0 34 34 58 7d bf 86 65 c4 a5 52 04 28 ac 25 59 4a 15 58 39 79 82 34 f8 87 24 69 1a 52 33 84 08 90 ab 8a d9 f7 d7 c6 92 60 c4 d4 03 bb 3e 32 91 de 8b b6 37 2e f4 b7 9a c7 fb 7d 28 34 84 11 83 1e b0 71 2d 6d c2 d1 b6 6b 40 34 15 dd 76 99 c2 69 57 c0 96 37 54 e5 76 e7 36 59 0b e7 77 98 26 23 ad 07 a9 8c bc 9c d8 1a 8c ac 4f 04 8b 9a 74 7d 90 6b 1e 68 59 53 e3 66 83 3b 6c 0b 09 ef 09 7d ae 6e 7b 8b 53 ac 51 ad 83 f8 cc bd be b2 b3 80 b9 2b 52 e9 a5 57 a8 29 b3 a6 63 ac 49 5a 88 c8 c6 9d 55 e7 5b 03 b7 3b c7 34 42 61 e2 99 02 03 01 00 01**	RSA(2048 bits)
ENHANCED KEY USAGE	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	
CERTIFICATE POLICIES	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.10015.14.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice text=https://www.sk.ee/en/repository/CP/ [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sk.ee/en/repository/CPS/	
AUTHORITY KEY IDENTIFIER	***KeyID=b1 10 97 02 fa dd 86 c6 78 41 a4 c3 32 88 fb fe 1f e7 c0 05***	Example
SUBJECT KEY IDENTIFIER	***b2 c7 23 c2 23 24 1d c8 91 e9 25 ee 25 27 6f 97 de 5a 80 2c***	Example
KEY USAGE	Digital Signature, Key Encipherment, Data Encipherment(B0)	Constant
CRL DISTRIBUTION POINTS	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/repository/crls/eid2011.crl	Constant (example)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None	Constant

4. Certificate Revocation List (CRL) Profile

The Certificate Revocation List is updated and published regularly and not less than once in every 12 hours 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	Notes

		RFC 5280	
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: sha256WithRSAEncryption.
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 5280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc5280.txt;;
[2] RFC 3739 – Request For Comments 3739. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, http://www.ietf.org/rfc/rfc3739.txt;
[3] Certification Policy for Lithuanian Mobile-ID, https://sk.ee/en/repository/CP/.