



Certificate and OCSP Profile for Mobile-ID of Lithuania

Version 1.0

1st March 2018

Version History		
Date	Version	Changes
01/03/2018	1.0	First public edition.

1. Introduction
 - 1.1. Terms and Abbreviations
2. Technical Profile of the Certificate
 - 2.1. Certificate Body
 - 2.2. Certificate Extensions
 - 2.2.1. Extensions
 - 2.2.2. Variable Extensions
 - 2.2.3. Certificate Policy
3. OCSP Profile
4. Referred and Related Documents

1. Introduction

The document describes the profiles of the digital certificates of Lithuanian Mobile-ID. This document complements Certificate Policy [2] and Certification Practice Statement [1].

The certificates are being issued by SK.

1.1. Terms and Abbreviations

Refer to p 1.6 in Certification Practice Statement [1] and Certificate policy [2]

2. Technical Profile of the Certificate

Natural person certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280 [4], ETSI EN 319 412-2 [6] and ETSI EN 319 411-2 (chapter 6.6) [12].

2.1. Certificate Body

Field	OID	Mandatory	Value	Changeable	Description
Version		yes	V3	no	Certificate format version
Serial Number		yes		no	Unique serial number of the certificate
Signature Algorithm	1.2.840.113549.1.1.11	yes	sha256WithRSAEncryption	no	Signature algorithm in accordance to RFC 5280
Issuer Distinguished name					
Common Name (CN)	2.5.4.3	yes	EID-SK 2016		Certificate authority name

Organisation Identifier	2.5.4.97	yes	NTREE-10747013	no	Identification of the issuer organisation different from the organisation name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1 [5]
Organisation (O)	2.5.4.10	yes	AS Sertifitseerimiskeskus		Issuer organisation name
Country (C)	2.5.4.6	yes	EE		Country code: EE - Estonia (2 character ISO 3166 country code [3])
Valid from		yes			First date of certificate validity.
Valid to		yes			The last date of certificate validity. Generally date of issuance + 1826 days (5 years).
Subject Distinguished Name		yes		yes	Unique subject name in the infrastructure of certificates.
Serial Number (S)	2.5.4.5	yes		yes	Person identity code as specified in clause 5.1.3 of ETSI EN 319 412-1 [5]
Given Name (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC5280.
SurName (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC5280.
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated given names and surnames Example: MINDAUGA S,BUTKUS
Country (C)	2.5.4.6	yes		yes	Country of origin for the personal identity code in accordance with ISO 3166 [3].

Subject Public Key		yes	RSA 2048, NIST P-256	yes	RSA algorithm in accordance with RFC 4055 [8] and ECC algorithm created in accordance with RFC 5480 [9]
--------------------	--	-----	-------------------------	-----	--

2.2. Certificate Extensions

2.2.1. Extensions

The following table describes the extensions used in the certificates:

Extension	OID	Values and Limitations	Criticality	Mandatory
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Non-critical	yes
Certificate Policy	2.5.29.32	Refer to p 2.2.3 "Certificate policy"	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions"	Critical	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	Refer to p 2.2.2 "Variable Extensions"	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35	SHA-1 hash of the public key used to sign the certificate	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key used to sign the certificate	Non-critical	yes
Authority Information Access	1.3.6.1.5. 5.7.1.1		Non-critical	yes
ocsp	1.3.6.1.5. 5.7.48.1	http://aia.sk.ee/eid2016		yes
calssuers	1.3.6.1.5. 5.7.48.2	http://c.sk.ee/EID-SK_2016.der.crt		yes

2.2.2. Variable Extensions

Following variable extensions for Lithuanian Mobile-ID certificates

Extension	DIGITAL AUTHENTICATION	DIGITAL SIGNATURE [20]
For ECC keys: Key Usage	DigitalSignature	nonRepudiation
For RSA keys: Key Usage	DigitalSignature	nonRepudiation
Qualified Certificate Statement [18]		
id-etsi-qcs-QcCompliance		yes

id-etsi-qcs-QcSSCD		yes
id-etsi-qcs-QcType [19]		1
id-etsi-qcs-QcPDS	https://sk.ee/en/repository/conditions-for-use-of-certificates/	https://sk.ee/en/repository/conditions-for-use-of-certificates/

18 - qcStatements according to clause 6.6.1 specified in ETSI EN 319 411-2 [12]

19 - Types according to clause 4.2.3 specified in ETSI EN 319 412-5 [11]

20 - Qualified Electronic Signatures compliant with eIDAS [10]

2.2.3. Certificate Policy

Profile	PolicyIdentifier (authentication)	PolicyIdentifier (digital signature)	PolicyQualifier
Lithuanian Mobile-ID	1.3.6.1.4.1.10015.18.1 0.4.0.2042.1.2	1.3.6.1.4.1.10015.18.1 0.4.0.194112.1.2	https://sk.ee/en/repository/CPS/

3. OCSP Profile

OCSP v1 according to [RFC 6960] [7]

Field	Mandatory	Value	Description
ResponseStatus	yes	0 for successful or error code	Result of the query
ResponseBytes			
ResponseType	yes	id-pkix-ocsp-basic	Type of the response
Response Data	yes		
Version	yes	1	Version of the response format
Responder ID	yes	CN = EID-SK 2016 AIA OCSP RESPONDER YYYYMM OU = OCSP 2.5.4.97 = NTREE-10747013 O = SK ID Solutions AS C = EE	Distinguished name of the OCSP responder. Note: the Common Name will vary each month and includes the month in YYYYMM format.
Produced At	yes		Date when the OCSP response was signed
Responses	yes		
CertID	yes		Serial number of the certificate
Cert Status	yes		Status of the certificate [21]
Revocation Time	no		Date of revocation or expiration of certificate
Revocation Reason	no		Code for revocation Reason according to RFC 5280 [4]

This Update	yes		Date when the status was queried from database
Signature Algorithm	yes	sha256WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [4]
signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response.

*OCSP does not support using *nonce* extension.

21 -Exceptions: In case of expired certificate „revoked“ status is used and Revocation time is set to *notAfter* value of the certificate if the responder has access to the full certificate.

4. Referred and Related Documents

- 1 SK ID Solutions AS - Certification Practice Statement for EID: <https://sk.ee/en/repository/CPS/>;
- 2 SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania: <https://sk.ee/en/repository/CP/>;
- 3 ISO 3166 Codes http://www.iso.org/iso/country_codes;
- 4 RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- 5 ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;
- 6 ETSI EN 319 412-2 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- 7 RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- 8 RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- 9 RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;
- 10 eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- 11 ETSI EN 319 412-5 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 5: QCStatements;
- 12 ETSI EN 319 411-2 v2.6.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.