SK ID Solutions - Certificate and OCSP Profile for Mobile-ID

Version 2.1

15.04.2024

Version History		
Date	**Version**	**Changes**
15.04.2024	2.1	• Regular review and update of references performed; • Chapter 2.2.2 – removed Qualified Certificate Statement from digital authentication certificate profile; • Chapters 2.2.2, 2.2.3 – updated URLs; • Chapter 4 – OCSP Profile: Archive Cutoff extension changed to mandatory.
02.07.2022	2.0	• Converted Lithuanian Mobile ID certificate profile to a generic Mobile-ID profile. • Corrected all references and replaced the section “Referred and Related Documents” with standardized citation. • Subsections 2.2.2 – separated variable extensions for digital signature and authentication into different tables. • Added missing OID-s. • Added a titel page
17.02.2022	1.5	• Chapter 2.1 - added random to certificate serial number description
12.05.2021	1.4	• Chapter 2.2 - changed sk.ee domain to skidsolutions.eu; • amended document overall wording and references.
30.06.2020	1.3	• Added Chapter 3 - Profile of Certificate Revocation List; • chapter 2.1 - updated Serial Number attribute description in Subject DN; • chapter 4 - removed OU field from OCSP ResponderID value; • changed sk.ee domain to skidsolutions.eu.
17.10.2019	1.2	• Chapter 3 - added nonce extension support for OCSP; • chapter 4 - updated ETSI document versions in "Referred and Related Documents"
24.10.2018	1.1	• Chapter 2.2.1 - corrections and improvements of AuthorityKeyIdentifier and SubjectKeyIdentifier descriptions; • chapter 3 - new extensions are added: Archive Cutoff and Extended Revoked Definition; CertStatus description is renewed.
01.03.2018	1.0	• First public edition.

1. Introduction

The Certificate and OCSP Profile for Mobile-ID document describes the profiles of the digital certificates for Mobile-ID. There are two types of certificates issued within Mobile-ID service. A digital authentication certificate and a digital signature certificate that is compliant with eIDAS Qualified Electronic Signatures [1].

This document complements the Certificate Policy [2] and SK-s Certification Practice Statement [3].

The certificates are issued by SK ID Solutions.

1.1. Terms and Abbreviations

Refer to subsection1.6 in the Certificate policy [2] and in the Certification Practice Statement [3].

2. Technical Profile of the Certificate

Mobile-ID natural person certificate is compiled in accordance with the following rules and regulations: X.509 version 3 [4], IETF RFC 5280 [5], ETSI EN 319 412-2 [6] and ETSI EN 319 411-2 (subsection 6.6) [7].

2.1. Certificate Body

Field	OID	Mandatory	Value	Changeable	Description
Version		yes	V3	no	Certificate format version
Serial Number	2.5.4.5	yes		no	Unique and random serial number of the certificate
Signature Algorithm	1.2.840.113549.1.1.11	yes	sha256WithRSAEncryption	no	Signature algorithm in accordance to RFC 5280 [5]
Issuer Distinguished name	2.5.4.49				
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 [8].
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 [9])
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	2.5.4.49	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 [8] Example: SERIALNUMBER = PNOLT-47101010033
Given Name (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC5280 [5].
Surename (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC5280 [5].
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated given names and surnames Example: MINDAUGAS,BUTKUS

Country (C)	2.5.4.6	yes		yes	Country of origin for the personal identity code in accordance with ISO 3166 [9].
Subject Public Key		yes	RSA 2048, NIST P-256	yes	RSA algorithm in accordance with RFC 4055 [10] and ECC algorithm created in accordance with RFC 5480 [11]

2.2. Certificate Extensions

2.2.1. Extensions

The following table describes the extensions used in the Mobile-ID 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 the table in subsection 2.2.3 "Certificate policy"	Non-critical	yes
Key Usage	2.5.29.15	Refer to the table in subsection 2.2.2 "Variable Extensions"	Critical	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	Refer to table in in subsection 2.2.2 "Variable Extensions"	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35	SHA-1 hash of the public key	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key	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

The following tables describe the variable extensions for Mobile-ID certificates. Tables are divided into two separated descriptors to clarify the difference between authentication and signature certificates' variable extensions.

The following table describes the extensions for the **digital authentication certificate**.

Extension	OID	Value	Mandatory
Key Usage (id-ce-keyUsage)	2.5.29.15	DigitalSignature	yes

The following table describes the variable extensions for the **digital signature certificate**. The digital signature extensions are compliant with eIDAS Qualified Electronic Signatures [1]. The extensions are compliant with *ETSI EN 319 411-2* [7] *and* ETSI EN 319 412-5 [12].

Extension	OID	Value	Mandatory
Key Usage (id-ce-keyUsage)	2.5.29.15	nonRepudiation	yes
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3		
id-etsi-qcs-QcCompliance	0.4.0.1862.1.1	PRESENT	yes
id-etsi-qcs-QcSSCD	0.4.0.1862.1.4	PRESENT	yes
id-etsi-qcs-QcType	0.4.0.1862.1.6	1	yes
id-etsi-qcs-QcPDS	0.4.0.1862.1.5	https://www.skidsolutions.eu/resources/conditions-for-use-of-certificates/	yes

2.2.3. Certificate Policy

Profile	PolicyIdentifier (authentification)	PolicyIdentifier (digital signature)	PolicyQualifier
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://www.skidsolutions.eu/resources/certification-practice-statement/

3. Profile of Certificate Revocation List

Certificate Revocation List (CRL) for issuing CA's EID-SK 2016 is not applicable.

4. OCSP Profile

OCSP v1 according to RFC 6960 [13]

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		CertID fields accordance with RFC 6960 [13] clause 4.1.1.
Cert Status	yes		Status of the certificate as follows: *Good* - certificate is issued and has not been revoked or suspended *Revoked* - certificate is revoked, suspended, or not issued by this CA *Unknown* - the issuer of certificate is unrecognized by this OCSP responder
Revocation Time	no		Date of revocation of certificate, for non-issued certificate revocation time is January 1, 1970.
Revocation Reason	no		Code for revocation Reason according to RFC 5280 [5].
This Update	yes		Date when the status was queried from database.
Archive Cutoff	yes	CA's certificate "valid from" date.	ArchiveCutOff date - the CA's certificate "valid from" date. Pursuant to RFC 6960 [13] clause 4.4.4.

Field	Mandatory	Value	Description
Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP Response conforms to extended definition in RFC6960 [13] clause 2.2.
Nonce	no		Value is copied from request if it is included. Pursuant to RFC 6960 [13] clause 4.4.1.
Signature Algorithm	yes	Sha256WithRSAEncryption or Sha512WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [5].
Signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response.

References

[1] "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," Official Journal of the European Union, 08 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[2] "Certificate Policy for Mobile-ID," SK ID Solutions AS, [Online]. Available: https://skidsolutions.eu/en/repository/CP/.

[3] "EID-Q SK Certification Practice Statement," SK ID Solutions AS, [Online]. Available: https://www.skidsolutions.eu/en/repository/CPS/.

[4] "The Directory: Public-key and attribute certificate frameworks," ITU, 10 2019. [Online]. Available: https://www.itu.int/rec/T-REC-X.509.

[5] "Internet X.509 Public Key Infrastructure Certificate," IETF, 05 2008. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280.

[6] "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons," ETSI, 07 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941202/02.02.01_60/en_31941202v020201p.pdf.

[7] "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," ETSI, 05 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.03.01_60/en_31941102v020301p.pdf.

[8] "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures," ETSI, 07 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.04.02_20/en_31941201v010402a.pdf.

[9] "ISO 3166 — Country Codes," 08 2020. [Online]. Available: https://www.iso.org/iso-3166-country-codes.html.

[10] "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF, 06 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4055.

[11] "Elliptic Curve Cryptography Subject Public Key Information," IETF, 04 2009. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5480.

[12] "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements," ETSI, 01 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.02.03_20/en_31941205v020203a.pdf.

[13] "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," IETF, 06 2013. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6960.