Certificate and OCSP Profile for SEB-cards

Version 6.1

24. October 2018

Version History		
Date	**Version**	**Changes**
24.10.2018	6.1	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.
01.11.2017	6.0	- Throughout the document removed AS SEB banka, AB SEB bankas. - Chapter 2.1 - removed RSA algorithm and added NIST P-384 key algorithm.
01.10.2017	5.0	Removed Organisational Unit (OU) field from certificate subject.
01.04.2017	4.0	Clause 2.2.2 - changed QcPDS URL.
01.01.2017	3.0	Document name change. Document structure change. - Chapter 2.2.3 - new OID's added in certificate policies. - Chapter 4 - added OCSP profile description; improved and added missing table fields. - Chapter 2.2.1 - removed CRL distribution point extension. Removed chapter 3 "CRL main fields".
26.02.2015	2.0	Editorial corrections and improvements to document formatting. Document is aligned with RFC 5280 [3]. - Chapter 3.1 - updated Signature Algorithm and id-atorganizationName information. - Chapter 4 - changed signing algorithm of CRL. - Chapter 5 - updated list of referred and related documents.
21.09.2012	1.0	Version 1.0

1. Introduction
    1.1. Terms and Abbrevations
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 in hand describes the profiles of the employee card issued by SEB linked to Certificates facilitate electronic signatures and electronic identification of natural persons (hereinafter referred as SEB card) issued by AS SEB Pank (hereinafter referred as SEB).

These documents are not deemed identity documents in the legal sense.

Also describes OCSP responses, all issued by EID-SK 2016 [11].

This document complements Certification Practice Statement [1] and Certificate Policy [2].

[11] - Intermediate CA name EID-SK 2016

1.1. Terms and Abbrevations

Refer to clause 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 [3], ETSI EN 319 412-2 [4], ETSI EN 319 412-1 [8] and ETSI EN 411-2 (chapter 6.6) [10].

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 [3].
Issuer Distinguished name				no	
E-mail address	1.2.840.113549.1.9.1	yes	pki@sk.ee		e-mail address of the issuer: pki@sk.ee
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 [5] country code).
Valid from		yes			First date of certificate validity.
Valid to		yes			The last date of certificate validity. Generally date of issuance + 1825 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	Personal identity code
Given Name (G)	2.5.4.42	yes		yes	Person given names in UTF8 format according to RFC 5280 [3]. International letters SHALL be encoded according to ICAO transcription rules where necessary.
SurName (SN)	2.5.4.4	yes		yes	Person surnames in UTF8 format according to RFC 5280 [3]. International letters SHALL be encoded according to ICAO transcription rules where necessary.
Common Name (CN)	2.5.4.3	yes		yes	Comma-separated surnames, first names and personal identity code.
Organisation Name (O)	2.5.4.10	yes	EID	yes	Name of the issuing organisation: EID (10004252; AS SEB Pank)
Country (C)	2.5.4.6	yes		yes	Country of origin in accordance with ISO 3166 [5].

Subject Public Key		yes	NIST P-384	yes	ECC algorithm created in accordance with RFC 5480 [6].

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 Policies	2.5.29.32	Refer to p 2.2.3 "Certificate policy"	Non-critical	yes
Subject Alternative Name	2.5.29.17	Refer to p 2.2.2 "Variable Extensions"	Non-critical	yes
SubjectKeyIdentifier	2.5.29.14	SHA-1 hash of the public key	Non-critical	yes
Key Usage	2.5.29.15	Refer to p 2.2.2 "Variable Extensions"	Critical	yes
Extended Key Usage	2.5.29.37	Refer to p 2.2.2 "Variable Extensions"	Critical	yes
Qualified Certificate Statement	-	Refer to p 2.2.2 "Variable Extensions	Non-critical	yes
AuthorityKeyIdentifier	2.5.29.35	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	https://sk.ee/upload/files/EID-SK_2016.der.crt		yes

2.2.2. Variable Extensions

Following variable extensions for SEB-card

Extension	DIGITAL AUTHENTICATION	DIGITAL SIGNATURE
Subject Alternative Name	The e-mail address of the certificate owner (SEB employee) is presented in this field. [12]	
Key Usage	DigitalSignature	nonRepudiation
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
Qualified Certificate Statement [13]		
id-etsi-qcs-QcCompliance		yes

id-etsi-qcs-QcSSCD		yes
id-etsi-qcs-QcType [14]		1
id-etsi-qcs-QcPDS	https://c.sk.ee/TCU-SEB-CARD-EN-20170401.pdf	https://c.sk.ee/TCU-SEB-CARD-EN-20170401.pdf

[12] -The e-mail address is composed of person's given- and surnames (forenames.surnames@seb.ee) in accordance to the values of the G and SN fields of the certificate. Utilises RFC 822 Name identifier.

The subdomain for the addresses can be: seb.ee

[13] - qcStatements according to clause 6.6.1 specified in ETSI EN 319 411-2 [10]

[14] - Types according to clause 4.2.3 specified in ETSI EN 319 412-5 [9].

2.2.3. Certificate Policy

Profile	PolicyIdentifier	PolicyQualifier
SEB-card	0.4.0.2042.1.2	
	0.4.0.194112.1.2	
	1.3.6.1.4.1.10015.13.1	https://www.sk.ee/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	C = EE, ST = Harjumaa, L = Tallinn, O = AS Sertifitseerimiskeskus, OU = OCSP, CN = EID-SK 2016 AIA OCSP RESPONDER YYYYMM, emailAddress = pki@sk.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 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 or expiration of certificate [15]
Revocation Reason	no		Code for revocation Reason according to RFC 5280 [3]
This Update	yes		Date when the status was queried from database
Archive Cutoff	no	CA's certificate "valid from" date.	ArchiveCutOff date - the CA's certificate "valid from" date. Pursuant to RFC 6960 [7] clause 4.4.4
Extended Revoked Definition	no	NULL	Identification that the semantics of certificate status in OCSP response conforms to extended definition in RFC6960 clause 2.2
Signature Algorithm	yes	sha256WithRSAEncryption	Signing algorithm pursuant to RFC 5280 [3]
signature	yes		
Certificate	yes		Certificate corresponding to the private key used to sign the response

4. Referred and Related Documents

1. SK ID Solutions AS - EID-SK Certification Practice Statement, published: https://sk.ee/en/repository/CPS/;
2. SK ID Solutions AS - Certificate Policy for the SEB card, published: https://sk.ee/en/repository/CP/;
3. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
4. 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;
5. ISO 3166 Codes, published: http://www.iso.org/iso/country_codes;
6. RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;
7. RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
8. ETSI EN 319 412-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
9. ETSI EN 319 412-5 v2.1.1 Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 5: QCStatements;
10. 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;