# AS Sertifitseerimiskeskus
# SEB-card Certificate and Certificate Revocation List Profile

Version 2.0
Effective since 30.03.2015

| Version information | | |
|---|---|---|
| **Date** | **Version** | **Modifications** |
| 26.02.2015 | 2.0 | Editorial corrections and improvements to document formatting.<br>Document is aligned with RFC5280.<br>- Chapter 3.1 - updated Signature Algorithm and *id-atorganizationName* information;<br>- Chapter 4 - changed signing algorithm of CRL;<br>- Chapter 5 - updated list of referred and related documents. |
| 21.09.2012 | 1.0 | Version 1.0 |

# 1. General Information

This document describes the profiles and minimum requirements for SEB-card certificates.

# 2. Definitions and Abbreviations

| Abbreviation | Definition |
|---|---|
| SEB card | Card issued by SEB and linked to Certificates enabling digital identity verification and digital signing. |
| Certificate owner | SEB-card user, whose personal data is linked to the digital data contained on the card. |

# 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 SEB-cards 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 | Name of the issuer at Registry of Certification Services: 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 | First names of Certificate owner. |
| *id-at-surname* | 2.5.4.4 | Last name of Certificate owner. |
| *id-at-commonName* | 2.5.4.3 | common name of Certificate in the form of: <LAST NAME>,<FIRST NAMES>,<PERSONAL IDENTITY CODE> |
| *id-atorganizationalUnitName* | 2.5.4.11 | Certificate area of use:<br>Digital identity verification certificate:<br>*Authentication;*<br>Digital signing certificate:<br>*Digital signature.* |

| Field | OID | Description |
|---|---|---|
| *id-atorganizationName* | 2.5.4.10 | Name of the issuing organization one of the following:<br>*EID (10004252; AS SEB Pank)*<br>*EID (40003151743; AS SEB banka)*<br>*EID (112021238; AB SEB bankas)* |
| *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 2048 bit module. |
| Key Usage | 2.5.29.15 | Key usage of Certificate<br>In case of Certificate enabling digital identity verification only one key usage area is indicated: *Digital Signature;*<br>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.<br>Used only in Certificates enabling digital identity verification:<br>Client Authentication (1.3.6.1.5.5.7.3.2)<br>Secure Email (1.3.6.1.5.5.7.3.4)<br>Microsoft smart card logon (1.3.6.1.4.1.311.20.2.2) |
| Subject Alternative Name | 2.5.29.17 | e-mail address of Certificate Owner.<br>Used only in Certificates enabling digital identity verification: Utilises RFC822 Name identifier containing the official e-mail address of the Certificate owner. |
| 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:<br>Policy Identifier= 1.3.6.1.4.1.10015.13.1.2 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/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):<br>*Subject Type=End*<br>*Entity, Path Length Constraint=None* |

### 3.2. Optional Information

In addition to mandatory information the certificates issued to SEB-cards 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:<br>- 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}<br>- 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} |

# 4. Certificate Revocation List (CRL) Profile

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: sha256WithRSAEncryption. |
| signatureValue | | 5.1.1.3 | Signature. |
| tBSCertList | | 5.1.2 | |
| version | | 5.1.2.1 | Certificate Revocation List format version: V2. |
| Signature | | 5.1.2.2 | Value depends on selected algorithm. |
| Issuer | | 5.1.2.3 | UTF8 coded CRL issuer distinguishing name. |
| e-mailAddress | 1.2.840.11 3549.1 .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 | Certificate Revocation List publication date and time. UTC time. |
| *nextUpdate* | | 5.1.2.5 | Date of the next Certificate Revocation List update. UTC time. The update interval for the Certificate Revocation List is |

| | | | |
|---|---|---|---|
| | | | defined in the Certification Policy. |
| 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 | Certificate serial number, unique identifier assigned by the issuer. |
| Authority Key Identifier | 2.5.29.35 | 5.1.2.7 | relevant SK public key identifier (equivalent private key used for signing the CRL) |
| Issiuing Distribution Point | 2.5.29.28 | | Certificate Revocation List 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 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (http://www.ietf.org/rfc/rfc5280.txt);
[2] RFC 3739 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (http://www.ietf.org/rfc/rfc3739.txt).