AS Sertifitseerimiskeskus - EID-SK Certification Practice Statement

Version 1.0

1.January 2017

Version History		
Date	**Version**	**Changes**
1 January 2017	1.0	

1. Introduction

AS Sertifitseerimiskeskus (hereinafter referred to as SK) was founded on March 26th 2001. The owners of the limited liability company are AS Swedbank, AS SEB Pank and Telia Eesti AS. The principal activities of SK are offering trust services and related technical solutions in the Baltic region. These services guarantee secure and verified electronic communication with public institutions as well as businesses in everyday life.

The CPS is a complete redesign of the previous "AS Sertifitseerimiskeskus - Certification Practice Statement" [1] and “SEB-card Certification Policy” [2]. Redesign of the named documents in accordance with the IETF RFC 3647 [3] and enforcement of this CPS do not substantially change provision of the respective certification service.

Inspired by the ETSI EN 319 400 series, SK has divided its documentation into three parts:

- "AS Sertifitseerimiskeskus Trust Services Practices Statement" [4] (hereinafter referred to as SK PS) describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Practice Statements describe parts that are specific to each Subordinate CA or
- Time-Stamping Unit;
- Technical Profiles are in separate documents.

Pursuant to the IETF RFC 3647 [3] this CPS is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [3], section headings that do not apply have the statement **"Not applicable"**. References to SK PS [4] and the "Certificate, CRL and OCSP profile for SEB-cards" [5] (hereinafter referred to as Certificate Profile for SEB-card) and "Certificate and OCSP Profile for Smart-ID" [13] (hereinafter referred to as Certificate Profile for Smart-ID) documents are included where applicable.

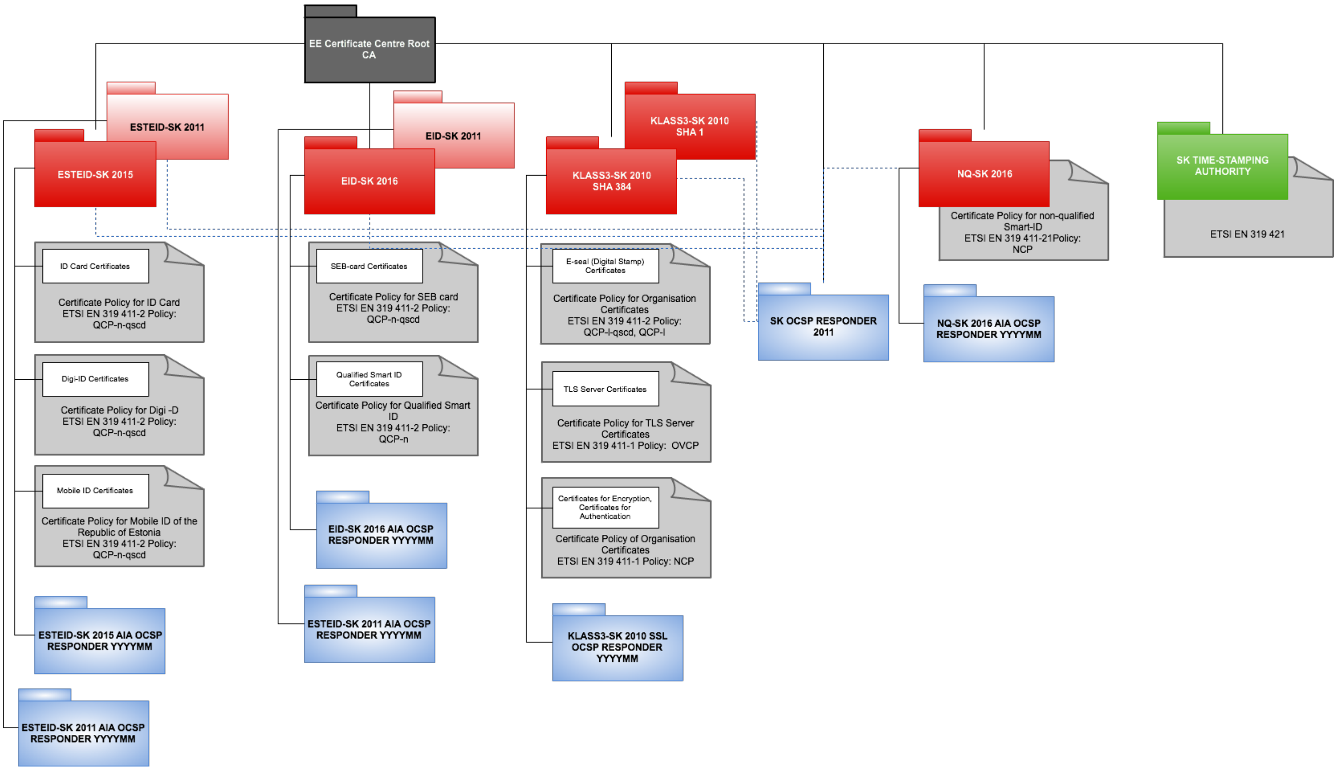
1.1. Overview

This CPS describes the practices used to comply with “AS Sertifitseerimiskeskus – Certificate Policy for the SEB card” [6] (hereinafter referred to as CP for SEB-card) and "AS Sertifitseerimiskeskus - Certificate Policy for Qualified Smart-ID" [2] (hereinafter referred to as CP for Q Smart-ID).

These policies are compliant with ETSI EN 319 411-2 Policy: QCP-n-qscd and QCP-n [7] and ETSI EN 319 411-1 Policy: NCP+ [8].

SK is currently using the following certificate chain:

EE Certification Centre Root CA chain, valid 2010-2030


EE Certificate Centre Root CA
ESTEID-SK 2011
ESTEID-SK 2015
ID Card Certificates
Certificate Policy for ID Card ETSI EN 319 411-2 Policy: QCP-n-qscd
Digi-ID Certificates
Certificate Policy for Digi -D ETSI EN 319 411-2 Policy: QCP-n-qscd
Mobile ID Certificates
Certificate Policy for Mobile ID of the Republic of Estonia ETSI EN 319 411-2 Policy: QCP-n-qscd
ESTEID-SK 2015 AIA OCSP RESPONDER YYYYMM
ESTEID-SK 2011 AIA OCSP RESPONDER YYYYMM
EID-SK 2011
EID-SK 2016
SEB-card Certificates
Certificate Policy for SEB card ETSI EN 319 411-2 Policy: QCP-n-qscd
Qualified Smart ID Certificates
Certificate Policy for Qualified Smart ID ETSI EN 319 411-2 Policy: QCP-n
EID-SK 2016 AIA OCSP RESPONDER YYYYMM
ESTEID-SK 2011 AIA OCSP RESPONDER YYYYMM
KLASS3-SK 2010 SHA 1
KLASS3-SK 2010 SHA 384
E-seal (Digital Stamp) Certificates
Certificate Policy for Organisation Certificates ETSI EN 319 411-2 Policy: QCP-l-qscd, QCP-l
TLS Server Certificates
Certificate Policy for TLS Server Certificates ETSI EN 319 411-1 Policy: OVCP
Certificates for Encryption, Certificates for Authentication
Certificate Policy of Organisation Certificates ETSI EN 319 411-1 Policy: NCP
KLASS3-SK 2010 SSL OCSP RESPONDER YYYYMM
SK OCSP RESPONDER 2011
NQ-SK 2016
Certificate Policy for non-qualified Smart-ID ETSI EN 319 411-21Policy: NCP
NQ-SK 2016 AIA OCSP RESPONDER YYYYMM
SK TIME-STAMPING AUTHORITY
ETSI EN 319 421

The certification service for Qualified Electronic Signature Certificate described in this CPS has qualified status in the Trusted List of Estonia.

In case of conflicts the documents are considered in the following order (prevailing ones first):

- QCP-n-qscd and QCP-n;
- NCP+;
- CP for SEB-card [6] and CP for Q Smart-ID [2];
- This CPS.

1.2. Document Name and Identification

This document is called “AS Sertifitseerimiskeskus – EID-SK Certification Practice Statement.” This is the first version of this document.

1.3. PKI Participants

1.3.1. Certification Authorities

SK operates as a Certification Authority that issues Certificates for the SEB-card and Qualified Smart-ID (hereinafter referred to as Q Smart-ID).

SK acts as a contractor for SEB. There is a contract signed between Trüb Baltic AS and SEB covering production and personalisation of the SEB-card.

The certification service provided by SK includes by default all the procedures related to the life cycle of the pairs of keys and Certificates, which are described in this CPS.

The Certificates are issued by the intermediate CA EID-SK 2011 that is identified by the following certificate:

EID-SK 2011

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            43:2b:d4:4e:62:43:6b:46:4d:83:2f:bf:7d:2d:2f:5a
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee
        Validity
            Not Before: Mar 18 10:11:11 2011 GMT
            Not After : Mar 18 10:11:11 2024 GMT
        Subject: C=EE, O=AS Sertifitseerimiskeskus, CN=EID-SK 2011/emailAddress=pki@sk.ee
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b6:43:5c:ca:32:de:c3:ca:d6:e7:b5:22:e8:60:
                    00:15:90:4c:15:fb:97:63:4a:bd:2f:48:81:bf:66:
                    6f:6c:78:ac:b1:fb:63:d8:f2:c5:73:5d:1a:14:0f:
                    50:8c:21:89:ec:b4:38:41:48:a3:23:9f:6f:fe:1e:
                    90:3b:a4:e8:a9:00:80:0c:ae:4e:ae:2a:7a:52:4d:
                    37:45:6d:0f:b4:7f:32:55:3e:89:01:82:c7:6c:43:
                    a4:79:4d:91:4f:07:59:ee:e7:38:11:46:54:26:58:
                    81:71:3a:90:e2:34:74:ed:d0:b3:9b:52:15:8b:5f:
                    35:1b:df:5b:dc:d5:69:9a:a3:62:18:70:3c:75:4c:
                    2b:3f:d4:4f:7e:71:a9:a2:0a:5d:81:e6:55:eb:3c:
                    45:37:c0:1a:b8:c1:a0:f9:e2:2c:d2:db:40:ca:d3:
                    9f:ba:fa:11:d1:83:e4:ea:a0:88:39:61:29:b0:6e:
                    34:ad:13:27:7f:f0:04:1e:a2:4c:15:96:8c:b2:1f:
                    8f:5b:9e:97:a5:b8:00:dc:64:98:31:c4:4f:59:52:
                    f5:56:1e:8c:58:7e:68:35:21:e4:54:ef:68:c7:4d:
                    c2:23:35:fd:5c:40:dd:be:f7:f1:6d:1d:03:27:1b:
                    30:c1:82:60:0f:a6:08:70:5a:bd:c9:b5:6d:09:5a:
                    f3:17
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.10015.100.1.1.1
                  User Notice:
                    Explicit Text:
                  CPS: https://www.sk.ee/CPS
            X509v3 Subject Key Identifier:
                B1:10:97:02:FA:DD:86:C6:78:41:A4:C3:32:88:FB:FE:1F:E7:C0:05
            X509v3 Authority Key Identifier:
                keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99
            X509v3 CRL Distribution Points:
                URI:http://www.sk.ee/repository/crls/eeccrca.crl
    Signature Algorithm: sha1WithRSAEncryption
        31:6a:ed:e8:85:d1:64:a6:f6:a2:55:44:7b:6a:b3:68:bd:05:
        19:44:21:bd:19:ed:ee:76:a1:d8:7a:6a:2f:c9:4e:cd:eb:41:
```

```
e0:a2:67:3f:64:6f:ae:ba:74:9c:01:34:d4:84:17:2f:f5:ae:
73:91:0c:5b:d5:d4:35:2d:80:d1:7c:da:fd:0a:a2:34:42:f4:
84:13:8b:7d:49:fb:b7:7c:e8:72:2e:b9:66:6f:7b:3c:c6:18:
58:2c:90:49:df:6e:6e:0e:fb:4e:fe:a1:5e:5c:b9:5c:45:73:
05:e6:75:3c:14:4d:88:c9:a6:4f:d4:21:d8:29:58:79:40:d3:
cf:42:21:99:19:2a:31:e6:83:a4:0a:f9:ad:e2:55:25:e2:56:
54:c1:58:9e:ef:9b:ac:fd:6b:6b:0f:a0:c9:79:11:01:4c:40:
c7:39:12:1f:83:c1:3d:44:0d:72:ff:bb:76:81:3f:6f:ad:4f:
2d:69:b7:92:66:50:f4:de:ac:17:7b:49:c9:f5:1b:1c:23:f3:
f4:1d:3f:2f:ba:8d:4f:1b:30:9f:6c:7f:71:16:a7:e8:67:68:
dd:27:41:f3:c6:b1:4c:f1:5b:0b:fc:0b:42:c3:47:66:af:14:
47:2e:56:73:a9:2c:34:1b:b6:f4:5b:8d:26:c0:e4:1a:b8:ed:
a0:6c:c7:e7
```

1.3.2. Registration Authorities

1.3.2.1. SEB-card

1.3.2.1.1 SEB

The certificates are issued for SEB-cards. The responsibility for issuing SEB-cards lies with SEB. SEB has concluded a contract with Trüb Baltic AS for the purposes of producing SEB-card blanks and personalisation of these cards. In addition, SEB has contracted SK for the purpose of issuing certificates to the card and servicing the issued certificates.

SEB may be contacted at:

- personal@seb.ee (in case where SEB-card is issued in AS SEB Pank); employee_cards@seb.lv
- (in case where SEB-card is issued in AS SEB Banka);
- Personalo_departamentas@seb.lt (in case where SEB-card is issued in AB SEB bankas).

1.3.2.1.2 SEB Customer Service Point

SEB Customer Service Point:

- issues personalised SEB-cards to Subscribers;
- submits applications for suspension, termination of suspension and revocation to SK.

SEB ensures the application of internal security measures when carrying out its responsibilities.

SEB Customer Service Points are published in the SEB intranet.

1.3.2.2. Qualified Smart-ID

1.3.2.2.1 Smart-ID Provider

Smart-ID Provider performs RA duties.

Refer to clause 1.3.5.2 of this CPS.

1.3.2.2.2 Customer Service Point

SK operates as a Customer Service Point.

Contact information:

Pärnu mnt 141, 11314 Tallinn, Estonia

(Mon-Fri 9.00 a.m. - 6.00 p.m. Eastern European Time)

Tel +372 610 1880

Email: info@sk.ee

1.3.2.2.3 Help Line

The Help Line acts as the representative of SK in the field of Subscriber telephone servicing. The Help Line provides user support for solving problems related to Q Smart-ID usage.

The Help Line accepts requests for revocation of Certificates of Q Smart-ID from Subscribers.

Information on the Help Line and its contact details is available on SK’s website https://sk.ee/en/kontakt/support/.

The Help Line may be contacted at 1777 or (+ 372) 677 3377.

1.3.3. Subscribers

Refer to clause 1.3.3 of the CP for SEB-card [6] and CP for Q Smart-ID [2].

1.3.4. Relying Parties

A Relying Party is a natural or legal person who takes a decision relying on the Certificate issued by SK.

1.3.5. Other Participants

1.3.5.1. SEB-card

Trüb Baltic AS:

- receives SEB-card orders;
- manufactures SEB-card blanks;
- personalises SEB-cards;
- generates SEB-card keys and requests the corresponding certificates;
- loads the certificates to SEB-card; delivers personalised SEB-cards to
- SEB.

Trüb Baltic AS activities are guided by the constraints stipulated in the contract concluded between SEB and Trüb Baltic AS.

Trüb Baltic AS ensures application of internal security measures in the fulfilment of its duties.

Trüb Baltic AS ensures that cards used are recognized as QSCD's.

Trüb Baltic AS may be contacted at:

Laki 5,

10621 Tallinn

Information: +372 658 11 30 E-mail:

info@trueb.ee

http://www.trueb.ee/trub-

homepage

1.3.5.2 Qualified Smart-ID

Smart-ID Provider is an organisation that is legally responsible for the Smart-ID System.

SK fulfills the role of Smart-ID Provider. SK maintains Smart-ID System, which consists of the Smart-ID Application and the Smart-ID Server.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Refer to clause 1.4 of the CP for SEB-card [6] and CP for Q Smart-ID [2].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS is administered by SK.

AS Sertifitseerimiskeskus

Registry code 10747013

Pärnu Ave 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@sk.ee

http://www.sk.ee/en/

1.5.2. Contact Person

Business Development Manager

Email: info@sk.ee

1.5.3. Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4. CPS Approval Procedures

Amendments which do not change the meaning of this CPS, such as spelling corrections, translation activities and contact details updates are documented in the Versions and Changes section of the present document. In this case the fractional part of the document version number is enlarged.

In case the CP for SEB-card [6] and the CP for Q Smart-ID [2] is amended, the CPS is reviewed as well in order to verify the need for its amendments.

In case of substantial changes, the new CPS version is clearly distinguishable from the previous ones and the serial number is enlarged by one. The amended CPS along with the enforcement date, which cannot be earlier than 30 days after CPS is published electronically on SK website.

All amendments to this CPS are coordinated with SEB as well as Trüb Baltic AS.

All amendments are approved by the business development manager and amended CPS is enforced by the CEO.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CPS the following terms have the following meaning.

Term	Definition
AS Sertifitseerimiskeskus Trust Services Practice Statement	A statement of practices that SK employs in providing Trust Services.
Authentication	Unique identification of a person by checking his/her alleged identity.
Trüb Baltic AS	Manufacturer and peronaliser of SEB-cards.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile for SEB-card [5] and Certificate Profile for Smart-ID [13], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.

Smart-ID Application	A technical component of the Smart-ID system. A mobile Smart-ID Application instance installed on a Subscriber's Mobile Device that provides access to non-qualified Smart-ID service.
Smart-ID Provider	An organization that is legally responsible for the Smart-ID system. SK is the Smart-ID provider.
Smart-ID Server	A technical component of the Smart-ID system, handles back-end operations.
Smart-ID System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The Smart-ID system provides services that allow Subscribers (Account owners) to authenticate themselves to E-Service Providers, to give Electronic Signatures requested by E-Service Providers, and to manage their Smart-ID accounts.
Smart-ID HSM module	The hardware security module used in the Smart-ID system. FIPS 140-2 Level 3 certified cryptographic device.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation [9].
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation [9].
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
E-Service Provider	A 3rd party, which uses services provided by the Smart-ID System to authenticate Subscribers and to allow Subscribers to electronically sign documents or transactions.
Mobile Device	A tablet computer or smartphone that runs a mobile device operating system (Apple iOS, Google Android).
SEB-card	Card issued by SEB linked to Certificates enabling digital identity verification and digital signing.
ID-1	Format which defines physical characteristics of identification cards according to the standard ISO/IEC 7816 [10].
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	An identifier used to uniquely name an object (OID).
Personal Data File	File on SEB-card that includes the Subscriber's personal data.
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key. In the Smart-ID System, the value of 'Private key' itself is never generated and the 'Private key' exists only in the form of it's components.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key. In the Smart-ID System, Public key exists only in the form of it's components and consists of the following components: 'Application's share of the public key' and 'Server's share of the public key'.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
Relying Party	Entity that relies on the information contained within a Certificate.

Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subscriber	A natural person to whom the Certificates of SEB-card or Q Smart-ID are issued.
Subject	In this document, the Subject is the same as the Subscriber.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon receipt of the Certificates.
UTF-8	Variable length character encoding which uses 8 bit code units capable of encoding all possible characters defined by Unicode.
Verified Electronic Authentication	Electronic Authentication for which the identity of a person has been verified by physical presence and personal authentication, prior to issuing electronic authentication credentials to the person. The person confirms the receipt of electronic credentials with a signature.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement. This document is a CPS.
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [9] 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
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
SEB	AS SEB Pank, AS SEB Banka, AB SEB bankas. Legal bodies tasked with issuing SEB-cards to natural persons.
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
SK	AS Sertifitseerimiskeskus, Certification Service provider
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement [4]

2. Publication and Repository Responsibilities

2.1. Repositories

Refer to clause 2.1 of SK PS [4].

2.2. Publication of Certification Information

Refer to clause 2.2 of SK PS [4].

2.2.1. Publication and Notification Policies

This CPS is published on SK's website: https://sk.ee/en/repository/CPS/.

This CPS and referred documents - the CP for SEB-card [6] and the CP for Q Smart-ID [2], the Certificate Profile for SEB-card [5] and the Certificate Profile for Smart-ID [13], the "Terms and Conditions of Use of Certificates of SEB-card" [11] (hereinafter referred to as Terms and Conditions of SEB-card) as well as the "Terms and Conditions for Use of Certificates of Qualified Smart-ID" [14] (hereinafter referred to as Terms and Conditions of Q Smart-ID) together with the enforcement dates are published on SK's website https://sk.ee/en/repository no less than 30 days prior to taking effect.

2.2.2. Items not Published in the Certification Practice Statement

Refer to clause 2.2.2 of the CP for SEB-card [6] and the CP for Q Smart-ID [2].

Refer to clause 9.3.1 of SK PS [4].

2.3. Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.4. Access Controls on Repositories

Refer to clause 2.4 of SK PS [4].

3. Identification and Authentication

3.1. Naming

3.1.1. Type of Names

Type of names assigned to the Subscriber is described in the Certificate Profile for SEB-card [5] and the Certificate Profile for Smart-ID [13].

3.1.2. Need for Names to be Meaningful

All the values in the Subscriber information section of a Certificate are meaningful.

Meaning of names in different fields of the Certificates is described in the Certificate Profile for SEB-card [5] and the Certificate Profile for Smart-ID [13].

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Subscriber names are encoded in UTF-8 and transcribed to Latin letters according to ICAO rules.

3.1.5. Uniqueness of Names

3.1.5.1 SEB-card

Subscriber's distinguished name is compiled according to the certificate profile described in the Certificate Profile for SEB-card [5]. SK does not issue Certificates with an identical Common Name (CN), Serial Number (S) and e-mail addresses in Subject Alternative Name (SAN) fields to different Subscribers.

3.1.5.2 Qualified Smart-ID

Subscriber's distinguished name is compiled according to the certificate profile described in the Certificate Profile for Smart-ID [13]. SK does not issue Certificates with an identical Common Name (CN) and Serial Number (S) fields to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Trademarks are not allowed.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

3.2.1.1 SEB-card

Private Key of the Subscriber is generated on the QSCD during personalisation in the chip of SEB-card by Trüb Baltic AS.

SEB-card is treated in a secure and traceable manner prior to handing over to the Subscriber. After having received the SEB-card, the Subscriber confirms the acceptance and integrity of the card using a digital signature created with another token. Only after having received the confirmation, SK activates the Certificates.

3.2.1.2 Qualified Smart-ID

There is a single process flow that includes key generation, Certificate Request and issuance. Both the Subscriber and Smart-ID Provider have to participate in the key generation procedure. The Certificate Request sent to CA includes a cryptographic signature created by the newly generated keys.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

3.2.3.1 SEB-card

The Subscriber´s identity is verified pursuant to current legislation and the following requirements:

- SEB card must be handed over to the Subscriber by an authorised SEB employee personally;
- The authorised SEB employee must verify the identity of the Subscriber on the basis of an identity or travel document issued by any European Union member state, given that the document includes a unique number assigned to the applicant by the document issuing country e.g. passport, identity card, residence permit (identity document);
- The authorised SEB employee shall make a photocopy of the submitted identity document, which must be signed by the Subscriber and the authorised SEB employee;
- The authorised SEB employee must prepare a legal act with regard to the delivery of the SEB-card in a format which can be reproduced in writing;
- The authorised SEB employee and Subscriber must sign this legal act;
- SEB must archive the photocopy made from the Subscriber's identity document together with the signed legal act for a period of 10 years.

3.2.3.2 Qualified Smart-ID

Certificates for Q Smart-ID can be requested only using an application signed with a Qualified Electronic Signature compliant with eIDAS Regulation [9].

SK relies on identification data provided in the signature of the application, which in turn has to be previously verified by the CA that has issued the Certificate used for signature. The requirement for Qualified Electronic Signature implies acceptable identification and authentication level required to issue Qualified Certificates.

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information is not allowed in the Certificate.

3.2.5. Validation of Authority

3.2.5.1 SEB-card

The Subscriber cannot apply for SEB-card through a representative. Prior to issuing the Certificates there must be a formal application signed by the representative of SEB.

3.2.5.2 Qualified Smart-ID

The Subscriber can apply for Q Smart-ID only personally. SK checks whether the applicant is over 18 years of age.

3.2.6. Criteria for Interoperation

Not applicable.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Refer to clause 3.2 of this CPS.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to clause 3.2 of this CPS.

3.4. Identification and Authentication for Revocation Request

Refer to clause 4.9.3 of this CPS.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

4.1.1.1 SEB-card

SEB submits an application for SEB-card.

Trüb Baltic AS submits CSRs to SK. SK accepts CSRs only from Trüb Baltic AS for which there is a previous authorization by SEB.

4.1.1.2 Qualified Smart-ID

The Subscriber can enroll herself using the functionality provided by the Smart-ID System.

SK accepts only applications coming from the Smart-ID System.

4.1.2. Enrolment Process and Responsibilities

4.1.2.1 SEB-card

The SEB-card application is submitted by SEB based on it's employee records.

The application is electronically sealed with SEB’s e-seal. The e-sealed SEB-card application is the basis for filling out an application for a certificate.

The review process for SEB-card applications is outlined in the contract concluded between SK and SEB. When processing the application for a certificate the authenticity and integrity of the submitted information must be verified.

The terms of processing of the SEB-card application are outlined in the contracts concluded between SEB, SK and Trüb Baltic AS.

The final decision regarding the approval or rejection of SEB-card applications lies with SEB.

In case of a positive decision:

- Trüb Baltic AS generates a pair of keys for the Subscriber;
- and generates the corresponding certificate requests for certificates facilitating digital signature and digital identity verification;
- and submits the requests to SK.

The corresponding certificates that are loaded onto the SEB card at Trüb Baltic AS are issued automatically by SK after the successful verification of the authenticity and integrity of the requests submitted by Trüb Baltic AS and SEB.

All issued certificates are in suspended state, i.e. included in the CRL.

4.1.2.2 Qualified Smart-ID

The Subscriber fills an application for Q Smart-ID in the Smart-ID System and signs it with a Qualified Electronic Signature compliant with eIDAS Regulation [9]. Upon signing an application for Q Smart-ID, the Subscriber confirms the correctness and integrity of the information presented to SK.

The Subscriber can apply for Q Smart-ID from the age of 18 and if Qualified Electronic Signature Certificate has been issued to him/her.

Smart-ID System validates the Subscriber's Qualified Electronic Signature and forwards the application to SK.

SK archives the Subscriber's electronically signed application.

Smart-ID Application generates keys for the Certificates and submits CSR on behalf of the Subscriber to SK.

SK verifies compliance of the data in the CSR with the data in previously archived Subscriber's application. If the data contained in the CSR and in the application is identical, SK generates Certificates corresponding to the application.

SK sends Certificates to Smart-ID System.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1 SEB-card

SEB validates the Subscriber's identity (refer to clause 3.2.3.1 of this CPS).

Trüb Baltic AS and SK rely on the identification data provided by SEB.

4.2.1.2 Qualified Smart-ID

The Subscriber is identified and authenticated by the data in the Qualified Electronic Signature of the application.

The signature is verified by both the Smart-ID System and SK.

4.2.2. Approval or Rejection of Certificate Applications

4.2.2.1 SEB-card

The acceptance or rejection of an application for the SEB-card is decided by SEB.

SK refuses to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable standards and agreements or where SK has not received the same request data from SEB and Trüb Baltic AS. If the data contained in a CSR needs to be modified, SK coordinates corresponding amendment with SEB.

SK notifies Trüb Baltic AS of the refusal to issue a Certificate.

4.2.2.2 Qualified Smart-ID

The acceptance or rejection of an application for Q Smart-ID is decided by SK.

SK refuses to issue a Certificate if:

- the Certificate request does not comply with the technical requirements set in applicable agreements;
- the Subscriber's signature of the application for Q Smart-ID is invalid or does not meet the requirements for Qualified Electronic Signature laid out in eIDAS Regulation [9];
- the signatory of the application for Q Smart-ID is another person and not the Subscriber;
- the Subscriber is under 18 years of age.

4.2.3. Time to Process Certificate Applications

Refer to clause 4.2.3 of the CP for SEB-card [6] and the CP for Q Smart-ID [2].

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

4.3.1.1 SEB-card

After checking the authenticity and integrity of the Certificate application received from Trüb Baltic AS SK automatically issues the corresponding Certificates. Certificates are loaded onto the SEB card by Trüb Baltic AS.

All issued Certificates are initially in suspended state.

4.3.1.2 Qualified Smart-ID

After verifying that the data contained in the CSR is identical with the data in the Subscriber's electronically signed application, SK automatically issues Certificates corresponding to the application.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

4.3.2.1 SEB-card

The Subscriber is notified by SEB of the issuance of the SEB-card. The SEB-card is issued to the Subscriber in SEB Customer Service Point.

The Subscriber signs the file of the SEB-card issuance, which confirms the Subscriber’s familiarisation and agreement to the Terms and Conditions of SEB-card [11].

4.3.2.2 Qualified Smart-ID

The Subscriber is immediately notified of the results by the Smart-ID Application as the whole process is done online in real time.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

4.4.1.1 SEB-card

SEB-cards are handed over to the Subscriber at a SEB Customer Service Point. The Subscriber receives the SEB-card which contains certificates in suspended state. The SEB-card along with a security envelope containing the activation codes of the certificates (PIN-code envelope) is handed over to the Subscriber by a SEB Customer Service Point employee. The Subscriber signs the SEB-card receipt confirming thereby having been informed of the Terms and Conditions of SEB-card [11] and receiving the PIN code envelope uncompromised and intact.

In order to terminate the suspension of SEB-card certificates the Subscriber must either:

- use the SK web application and digitally sign the termination of suspension application or;
- present the termination of suspension application to SEB Customer Service Point who processes the application for the Subscriber.

The SEB Customer Service Point employee processing the termination of suspension must be different from the one who handed over the SEB-card.

Acceptance of and signing the Terms and Conditions of SEB-card [11] as well as confirmation that the SEB-card has been handed over to the Subscriber are deemed Certificate acceptance.

Upon registration of the submitted confirmations at the SEB Customer Service Point the identity document used for the verification of the applicant’s identity must be noted down.

4.4.1.2 Qualified Smart-ID

Upon submitting an application for Q Smart-ID, the Subscriber confirms familiarisation and agreement to the Terms and Conditions of Q Smart-ID [14]. Corresponding confirmation is deemed Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

4.4.2.1 SEB-card

Certificates are not published by SK. Certificate validity can be checked through OCSP service.

4.4.2.2 Qualified Smart-ID

Certificates are published in Smart-ID System by SK. Certificate validity can be checked through OCSP service.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

4.4.3.1 SEB-card

SK delivers Certificates issued for SEB-cards immediately to Trüb Baltic AS for loading to the cards.

4.4.3.2 Qualified Smart-ID

The Certificates are automatically published to the Smart-ID System by SK.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

The Subscriber is required to use the Private Key and Certificate lawfully and in accordance with:

- the CP for SEB-card [6] and the CP for Q Smart-ID [2];
- this CPS;
- the Terms and Conditions of SEB-card [11]
- and the Terms and Conditions of Q Smart-ID [14].

4.5.2. Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber’s Public Key and Certificate lawfully and in accordance with:

- the CP for SEB-card [6] and the CP for Q Smart-ID [2];
- this CPS;
- the Terms and Conditions of SEB-card [11]
- and the Terms and Conditions of Q Smart-ID [14].

4.6. Certificate Renewal

Renewal of Certificates is not allowed.

4.7. Certificate Re-Key

Routine Re-Key initiated by the Subscriber is considered to be a new application and processed accordingly. Refer to clauses 3.2 and 4.1 to 4.4 of this CPS.

4.7.1. Circumstances for Certificate Re-Key

4.7.1.1 SEB-card

Certificate re-key is allowed to:

- fix production errors that are discovered during quality checks.

4.7.1.2 Qualified Smart-ID

There are no circumstances defined for which the re-keying procedure is different from an initial application.

4.7.2. Who May Request Certification of a New Public Key

4.7.2.1 SEB-card

Certificate re-key process to fix production errors of SEB-card can only be initiated by Trüb Baltic AS.

SK accepts only Certificate requests coming from Trüb Baltic AS for which there is a previous authorization by SEB.

4.7.2.2 Qualified Smart-ID

Not applicable.

4.7.3. Processing Certificate Re-Keying Requests

4.7.3.1. SEB-card

If Trüb Baltic AS has discovered production errors during quality checks, Trüb Baltic AS submits a new CSR to SK.

If the repeated request has no changed data in it, the already issued certificate is retransmitted. Otherwise all the erroneous or unusable Cert ificates to be replaced are revoked.

The rest of the process is similar to initial issuance.

4.7.3.2 Qualified Smart-ID

Not applicable.

4.7.4. Notification of New Certificate Issuance to Subscriber

4.7.4.1 SEB-card

The Subscriber notification is similar to initial notification pursuant to clause 4.3.2.1 of this CPS.

4.7.4.2 Qualified Smart-ID

Not applicable.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

If the Certificate re-key is performed the Subscriber confirms that he/she has read and agrees to the Terms and Conditions of SEB-card [11] and the Terms and Conditions of Q Smart-ID [14] as stated in clauses 4.4.1.1 and 4.4.1.2 of this CPS.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Refer to clause 4.4.2 of this CPS.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Refer to clause 4.4.3 of this CPS.

4.8. Certificate Modification

See clause 4.7 of this CPS.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1 of the CP for SEB-card [6] and the CP for Q Smart-ID [2].

4.9.2. Who Can Request Revocation

4.9.2.1 SEB-card

Refer to clause 4.9.2 of the CP for SEB-card [6].

SEB revokes certificates of SEB-cards immediately after Subscriber has lost the rights to use SEB-card.

4.9.2.2 Qualified Smart-ID

Subscriber can request revocation of the Subscriber's Certificates any time.

4.9.3. Procedure for Revocation Request

4.9.3.1 SEB-card

The applications for revoking certificates can be submitted at SEB Customer Service Points or by sending a digitally signed application to:

- personal@seb.ee (in case where SEB-card is issued in AS SEB Pank);
  employee_cards@seb.lv (in case where SEB-card is issued in AS SEB Banka);
- Personalo_departamentas@seb.lt (in case where SEB-card is issued in AB SEB bankas).

The identity of the applicant or the validity of the signature is verified in accordance to current legislation. The application for revocation of certificates must include the following information:

- The first and last name of the owner and applicant (if different);
- Personal identification number of the owner and applicant (if different); Country that has issued the personal identification number;
- Grounds for revocation.

Upon registration of the submitted application at the SEB Customer Service Point the identity document used for the verification of the applicant's identity must be noted down.

The person filing an application for revocation is identified and the legality to request revocation is established by SK.

After SK receives an application for revocation, the procedure for processing the request is the following:

- the application for revocation is registered in SK's information system;
- the compliance of the application for revocation with the CP for SEB-card [6] is verified in SK's information system;
- OCSP no longer responds with "GOOD";
- the Certificate is marked as revoked in the certificate database;
- a new CRL is published according to clause 4.9.7 of this CPS;
- the documentation on which the application for revocation was based is archived;
- the Subscriber is notified of revocation of the Certificate.

The revocation of the Certificate is recorded in the certificate database of SK. The Subscriber has a possibility to ascertain on the basis of CRL or OCSP that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

4.9.3.2 Qualified Smart-ID

The revocation request is registered by the Help Line operator, who suspends the Q Smart-ID service.

Revocation request submitted via the Help Line is recorded.

The Help Line operator directs the Subscriber to self-service web portal, where the Subscriber is authenticated using Verified Electronic Authentication. The Subscriber has to confirm the application there.

The self-service web portal sends the request for revocation to SK.

If the Subscriber does not have the possibility to submit a request for revocation through self-service web portal, the Subscriber can submit a signed application for revocation to the Customer Service Point.

In case of a signed application, the identity of the person is verified based on the copy of the identity document by an employee of the Customer Service Point. After SK has received an application for revocation of the Certificate, the procedure for processing the request is the following:

- The revocation application is registered by an employee of the Customer Service Point;
- The person filing an application for revocation is verified;
- The compliance of the application for revocation with the CP for Q Smart-ID [2] is verified in SK's information system;
- The documentation on which the application for revocation was based is archived;
- The Subscriber is notified of revocation of the Certificates.

The Certificate is revoked immediately after the application's legality has been verified, but no later than 12 hours after an application for revocation has been submitted. The revocation of the Certificate is recorded in the certificate database of SK no later than 24 hours after an application has been submitted. The Subscriber has a possibility to verify from the Smart-ID System that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

4.9.4. Revocation Request Grace Period

4.9.4.1 SEB-card

The Subscriber is required to request revocation immediately after detecting the loss or theft of the SEB-card or it becoming unusable due to another reason.

4.9.4.2 Qualified Smart-ID

The Subscriber is required to request revocation immediately after verifying the loss or theft of the device.

4.9.5. Time Within Which CA Must Process the Revocation Request

4.9.5.1 SEB-card

SK processes an application for revocation immediately after it has verified the correctness and completeness of the corresponding application as well as applicant's authority to request revocation.

4.9.5.2 Qualified Smart-ID

SK is immediately obliged to process an application for revocation but no later than 6 hours after an application for revocation has been submitted.

4.9.6. Revocation Checking Requirements for Relying Parties

The mechanisms available to a Relying Party in order to check the status of certificates on which it wishes to rely have been established in the Terms and Conditions of SEB-card [11] and the Terms and Conditions of Q Smart-ID [14].

4.9.7. CRL Issuance Frequency

The value of the nextUpdate field of CRL is set to 12 hours after issuance of CRL.

CRL for EID-SK 2016 is not issued.

4.9.8. Maximum Latency for CRLs

SK monitors of the expiry time of the CRL that is published on SK's website. If a new CRL is not published 120 minutes before expiry of the previous one, an alarm is raised.

4.9.9. On-Line Revocation/Status Checking Availability

An OCSP service is free of charge and publicly accessible.

An OCSP service serves as a primary source for the Certificate status information.

4.9.10. On-Line Revocation Checking Requirements

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been established in the Terms and Conditions of SEB-card [11] and the Terms and Conditions of Q Smart-ID [14].

4.9.11. Other Forms of Revocation Advertisements Available

SK offers an OCSP service with better SLA under agreement and price list.

4.9.12. Special Requirements Related to Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Suspension is allowed only for SEB-card Certificates, circumstances of suspension are listed in clause 4.9.13 of the CP for SEB-card [6].

4.9.14. Who Can Request Suspension

4.9.14.1 SEB-card

Anyone can request Certificate suspension.

4.9.14.2 Qualified Smart-ID

Not applicable.

4.9.15. Procedure for Suspension Request

4.9.15.1 SEB-card

The Subscriber can request Certificate suspension via phone 24 hours a day, 7 days a week.

The person requesting suspension and the legality to request suspension is verified by using professional skills of the operator.

Alternatively, the person files a signed application for suspension to an employee of the SEB Customer Service Point or SK. The person filing an application for suspension is identified and the legality to request suspension is verified by using professional skills of an employee of the SEB Customer Service Point or SK.

After SK has received a request for suspension of the Certificate, the procedure for processing the request is the following:

- the compliance of the application for suspension of the Certificate with the CP for SEB-card [6] is verified in SK's information system; the application for suspension is registered in SK's information system;
- the Certificate is marked as suspended in the certificate database;
- OCSP no longer responds with "GOOD";
- a new CRL is published in accordance with clause 4.9.7 of this CPS;
- the documentation on which the application for suspension was based is archived.

The Subscriber is immediately notified of the successful Certificate suspension after completion of the suspension procedure. The Subscriber has a possibility to ascertain on the basis of OCSP or CRL that the Certificate has been suspended.

4.9.15.2 Qualified Smart-ID

Not applicable.

4.9.16. Limits on Suspension Period

4.9.16.1 SEB-card

There are no limits on the suspension period.

4.9.16.2 Qualified Smart-ID

Not applicable.

4.9.17. Circumstances for Termination of Suspension

4.9.17.1 SEB-card

Refer to clause 4.9.17 of the CP for SEB-card [6].

4.9.17.2 Qualified Smart-ID

Not applicable.

4.9.18. Who Can Request Termination of Suspension

4.9.18.1 SEB-card

Refer to clause 4.9.18 of the CP for SEB-card [6].

4.9.18.2 Qualified Smart-ID

Not applicable.

4.9.19. Procedure for Termination of Suspension

4.9.19.1 SEB-card

The procedure of termination of suspension is the following:

- termination of suspension request is registered by an employee of the SEB Customer Service Point or SK;
- the person filing an application for termination of suspension is identified by an employee of the SEB Customer Service Point or SK; the legality to request termination of suspension is verified by an employee of the SEB Customer Service Point or SK;
- the compliance of the application for termination of suspension of the Certificate with the CP for SEB-card [6] is verified in SK's information system;
- the fact of termination of suspension is registered in SK's information system;
- OCSP responds with "GOOD";
- the Certificate is marked as active in the certificate database;
- a new CRL is published in accordance with clause 4.9.7 of this CPS.

The Subscriber is immediately notified of the successful completion of procedure of termination of suspension of the Certificate. The Subscriber has a possibility to ascertain on the basis of OCSP or the next CRL that the suspension of the Certificate has been terminated.

4.9.19.2 Qualified Smart-ID

Not applicable.

4.10. Certificate Status Services

Refer to clause 4.10 of SK PS [4].

4.11. End of Subscription

The Subscriber may end a subscription for the Certificate by revoking the Certificate without replacing it.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

SK does not provide the Subscriber with key escrow and recovery services.

Storing the components of the split private key of Q Smart-ID Subscriber in the Smart-ID Server is not considered a key escrow service.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

Refer to clause 5.1 of SK PS [4].

5.2. Procedural Controls

Refer to clause 5.2 of SK PS [4].

5.3. Personnel Controls

Refer to clause 5.3 of SK PS [4].

5.4. Audit Logging Procedures

Refer to clause 5.4 of SK PS [4].

Audit log of events relation to preparation of QSCD is kept.

5.5. Records Archival

5.5.1. Types of Records Archived

Refer to clause 5.5.1 of SK PS [4].

All physical records from issuance process and from applications for suspension, termination of suspension and revocation are retained by RA-s and archived in accordance with relevant regulations.

5.5.2. Retention Period for Archive

Refer to clause 5.5.2 of SK PS [4].

5.5.3. Protection of Archive

Refer to clause 5.5.3 of SK PS [4].

5.5.4. Archive Backup Procedures

Refer to clause 5.5.4 of SK PS [4].

5.5.5. Requirements for Time-Stamping of Records

Refer to clause 5.5.5 of SK PS [4].

5.5.6. Archive Collection System (Internal or External)

Refer to clause 5.5.6 of SK PS [4].

RA-s may use external archive collection system for physical archive records.

5.5.7. Procedures to Obtain and Verify Archive Information

Refer to clause 5.5.7 of SK PS [4].

5.6. Key Changeover

Refer to clause 5.6 of SK PS [4].

5.7. Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [4].

5.8. CA or RA Termination

Refer to clause 5.8 of SK PS [4].

6. Technical Security Controls

6.1. Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [4].

6.1.1. Key Pair Generation

Refer to clause 6.1.1 of SK PS [4].

6.1.1.1 SEB-card

The Subscriber Private Keys is generated during personalisation in the chip of the SEB-card by Trüb Baltic AS. The generated keys can not be extracted or restored from the card. The Subscriber keys are protected by the activation PIN codes handed over and known only to the Subscriber.

6.1.1.2 Qualified Smart-ID

Qualified Smart-ID Key Pair Terminology

Q Smart-ID Key Pair is generated with multiple components for additional protection and cryptographic properties. The following terminology is used to describe the technical security controls:

1 'Public key' - is the public verification key in the public-key cryptography. This corresponds to the regular RSA public key. The .relation between the 'Public key' and a 'Subscriber's Identity' is attested by a Certificate. Public key has the following components: 'Application's share of the public key' and 'Server's share of the public key'.
2 'App's share of the public key' - is generated in the Smart-ID app, along with the generation of the 'App's share of the private key'.

3. 'Server's share of the public key' - is generated in the Smart-ID server, along with the generation of the 'Server's share of the private key'.

4 'Private key' - is the confidential component of the key pair in the public-key cryptography. 'Private key' is used for creating digital signatures. In the Smart-ID System, the value of 'Private key' itself is never generated and the 'Private key' exists only in the form of it's components. 'Private key' has the following components:

4.1. 'App's share of the private key', which is a regular RSA private key. It is further divided to the following components:

4.1.1. 'App's part of the private key'

4.1.2. 'Server's part of the private key'

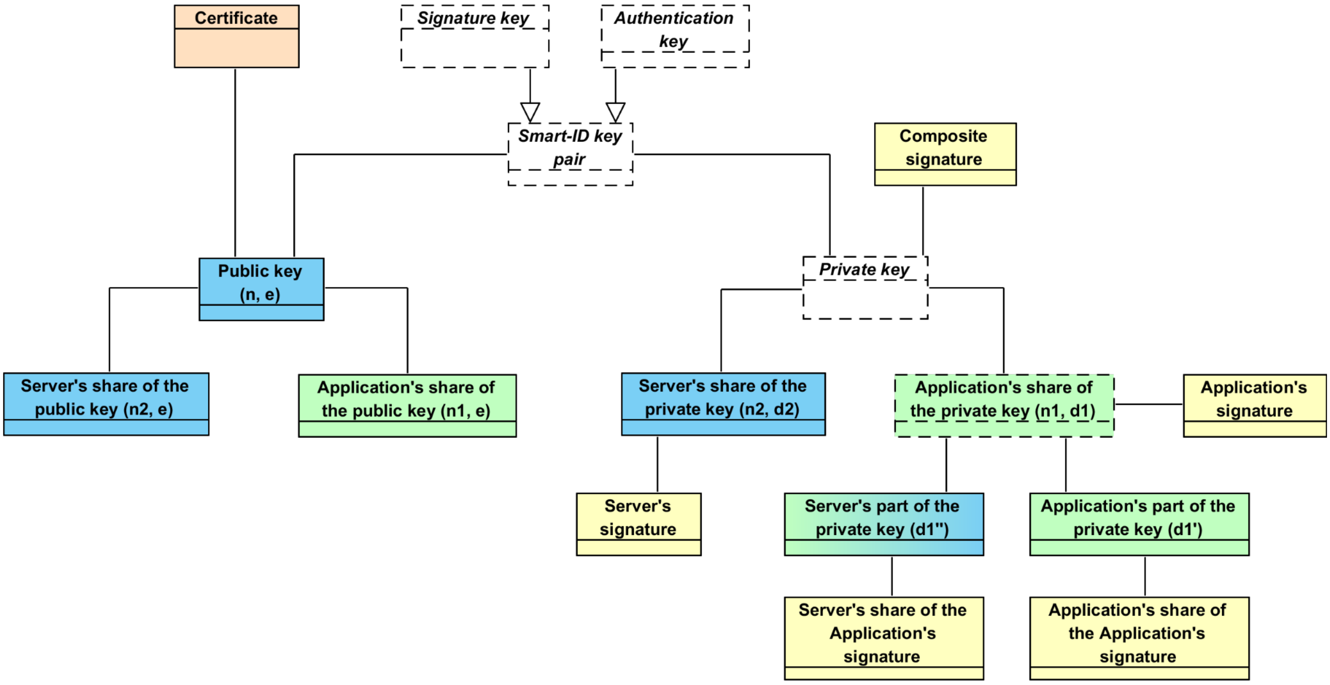
4.2. 'Server's share of the private key', which is a regular RSA private key..

5 'Application's share of the private key' - is the component of the private key that is generated in the Smart-ID app. The share is divided into two parts immediately after generation and the share itself is deleted.

6 'App's part of the private key' - is the component of the private key, which is generated in the Smart-ID app and stored in the Smart-ID app and is protected with the Subscriber's PIN-code.

7 'Server's part of the private key' - is the component of the private key, which is generated in the Smart-ID app and securely transmitted to the server. 'Server's part of the private key' is stored in the server's database and protected with Key-Wrapping-Key inside the HSM.

8 'Server's share of the private key' - is the component of the private key, which is generated in the HSM and stored inside the HSM.


Certificate
Signature key
Authentication key
Smart-ID key pair
Composite signature
Public key (n, e)
Private key
Server's share of the public key (n2, e)
Application's share of the public key (n1, e)
Server's share of the private key (n2, d2)
Application's share of the private key (n1, d1)
Application's signature
Server's signature
Server's part of the private key (d1")
Application's part of the private key (d1')
Server's share of the Application's signature
Application's share of the Application's signature

6.1.1.2.1 Smart-ID Key Pair Generation

Subscriber Key Pair is generated during the Smart-ID registration process in the Smart-ID app and in the Smart-ID server. The following components are generated.

Generation of 'App's share of the private key' and 'App's share of the public key'

'App's share of the private key' and 'App's share of the public key' is a 2048-bit RSA keypair. Smart-ID app generates the keypair according to FIPS 186-4 with the PRNG, which corresponds to NIST SP 900-90A. After dividing the 'App's share of the private key' to components, the private key is deleted.

Generation of 'App's part of the private key'

The 'App's part of the private key' is a 2048-bit random number. Smart-ID app generates the 'App's part of the private key' randomly with the PRNG, which corresponds to NIST SP 900-90A.

Generation of 'Server's part of the private key'

The 'Server's part of the private key' is a 2048-bit number, which is computed from the private exponent of the 'App's share of the private key' and 'App's part of the private key'. Smart-ID app computes the 'Server's part of the private key' and transmits the 'Server's part of the private key' securely to the Smart-ID server.

Generation of 'Server's share of the private key' and 'Server's share of the public key'

'Server's share of the private key' and 'Server's share of the public key' is a 2048-bit RSA keypair. Smart-ID server generates the keypair inside the Smart-ID HSM module.

Generation of Subscriber's 'Public key'

Subscriber's 'Public key' is a 4096-bit RSA public key. The public key is computed by the Smart-ID server from the 'App's share of the public key' and 'Server's share of the public key'. This way all the Smart-ID keypair components are tied together with the 'Public key'.

6.1.2. Private Key Delivery to Subscriber

6.1.2.1 SEB-card

The Subscriber Private Keys are delivered in the chip of the card. The confidentiality and non-usage of the generated Private Keys and PIN codes until issuance of the card before delivery to the Subscriber is warranted by respective parties involved in handling the cards.

6.1.2.2 Qualified Smart-ID

Subscriber's 'Private key' is composed of multiple components.

Delivery of 'App's part of the private key'

The 'App's part of the private key' is generated inside the Subscriber's mobile device and is never transmitted outside of this device.

Delivery of 'Server's part of the private key'

The 'Server's part of the private key' is generated inside the Subscriber's mobile device and is securely transmitted to the Smart-ID server. The transmission is handled in the following way:

1. The key-tranmission-keypair (KTK) is generated inside the Smart-ID HSM module. The KTK is 2048-bit RSA keypair.
2. The public key of the KTK is embedded in the binary distribution of the Smart-ID app.
3. The 'Server's part of the private key' is encoded and encrypted with the public key of the KTK (according to the RFC 7516) and transmitted to the Smrt-ID server inside the TLS channel, for additional confidentiality and authenticity.
4. The Smart-ID server uses the HSM to decrypt the 'Server's part of the private key' and stores it securely in the database, wrapped with another long-term key-wrap-keypair (KWK). The KWK is generated and stored inside the Smart-ID HSM module.

Delivery of 'Server's share of the private key'

The 'Server's share of the private key' is generated inside the Smart-ID HSM module and is never transmitted outside of the HSM module.

6.1.3. Public Key Delivery to Certificate Issuer

6.1.3.1 SEB-card

Trüb Baltic AS sends the Public Key to be certified to SK via a secure and private elecronic channel using a message signed by Trüb Baltic AS.

6.1.3.2 Qualified Smart-ID

Subscriber's 'Public key' is composed of multiple components.

Delivery of 'App's share of the public key' from Smart-ID app to Smart-ID server

The 'App's share of the public key' is generated in the Smart-ID app and then transmitted to the Smart-ID server during the Subscriber's registration process. The public key is transmitted over the TLS communication channel for confidentiality and authenticity.

Delivery of 'Server's share of the public key' from Smart-ID HSM to Smart-ID server

The 'Server's share of the public key' is generated inside the Smart-ID HSM module and then transmitted to Smart-ID server.

Delivery of Subscriber's 'Public key' from Smart-ID server to Certificate Issuer

The Subscriber's 'Public key' is computed inside the Smart-ID server and then transmitted to Certificate Issuer inside the PKCS#10 Certificate Signing Request (CSR). The CSR is signed by the Subscriber for authenticity. The transmission is protected by TLS communication channel for additional confidentiality and authenticity.

6.1.4. CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [4].

6.1.5. Key Sizes

6.1.5.1 SEB-card

Subscriber keys are 2047 or 2048 bits RSA keys.

6.1.5.2 Qualified Smart-ID

1. 'App's share of the private key' is a 2047 or 2048 bit RSA private key.
2. 'App's part of the private key' is a 2047 or 2048 bit number.

3. 'Server's part of the private key' is a 2047 or 2048 bit number.
4. 'Server's share of the private key' is a 2047 or 2048 bit RSA private key.
5. 'App's share of the public key' is a 2047 or 2048 bit RSA public key.
6. 'Server's share of the public key' is a 2047 or 2048 bit RSA public key.
7. 'Public key' is a 4094, 4095 or 4096 bit RSA public key.

6.1.6. Public Key Parameters Generation and Quality Checking

6.1.6.1 SEB-card

The quality of Public Keys is guaranteed by using secure random number generators built into the smartcard. User-generated keys are not accepted. Before issuing a Certificate, key is checked for duplicates and some basic analytic checks are applied (e.g. e > 1 for RSA). More thorough checks are run over database of issued Certificates regularly.

6.1.6.2 Qualified Smart-ID

Quality of public keys is quaranted by using secure random number generators inside the Smart-ID app and Smart-ID HSM module and following the guidelines in the FIPS 186-4. Before issuing a Certificate, key is checked for duplicates and some basic analytic checks are applied (e.g. e > 1 for RSA). More thorough checks are run over database of issued Certificates regularly.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to clause 6.1.7 of SK PS [4].

Key usage purposes are described in clause 7.1 of this CPS.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

6.2.1.1 SEB-card

Refer to clause 6.2.1 of SK PS [4].

The chips used to store Subscriber Private keys are QSCD according to eIDAS Regulation [9].

6.2.1.2 Qualified Smart-ID

Refer to clause 6.2.1 of SK PS [4].

Qualified Smart-ID app cryptographic library standards

The Smart-ID app for the Android and iOS platforms are corresponding to FIPS 186-4.

Qualified Smart-ID server cryptographic library standards

The Smart-ID server is using Smart-ID HSM module for the cryptographic operations. HSM module is corresponding to FIPS-140-2 Level 3.

6.2.2. Private Key (n out of m) Multi-Person Control

6.2.2.1 SEB-card

Refer to clause 6.2.2 of SK PS [4].

No Multi-Person control is applied to Subscriber Private keys.

6.2.2.2 Qualified Smart-ID

Multi-Person Control of 'App's part of the private key'

No Multi-Person control is applied to 'App's part of the private key'.

Multi-Person Control of 'Server's part of the private key'

The access to the KWK key, which protects the 'Server's part of the private key', is divided into two parts that are secured by different persons in Trusted Roles. For activation of the KWK key the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [4].

Multi-Person Control of 'Server's share of the private key'

The access to the 'Server's share of the private key', is divided into two parts that are secured by different persons in Trusted Roles. For activation of the key, the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [4].

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [4].

SK does not offer Key Escrow services to Subscribers.

6.2.4. Private Key Backup

6.2.4.1 SEB-card

Refer to clause 6.2.4 of SK PS [4].

The Subscriber Private Keys cannot be extracted or restored from the chip and are not backed up.

6.2.4.2 Qualified Smart-ID

Refer to clause 6.2.4 of SK PS [4].

In general, Smart-ID System doesn't provide the private key backup services. SK makes the following exceptions to the following components of the Subscriber's private key in order to support high availability of the Smart-ID System.

No backup of 'App's part of the private key'

The encrypted value of 'App's part of the private key' is stored inside the Smart-ID app private storage area. It is not backed up and not copied from the storage area.

In case Subscriber needs to recover from the malfunctioning mobile device or user error, Subscriber needs to complete the registration process again.

Backing up of encrypted value of 'Server's part of the private key'

The encrypted value of 'Server's part of the private key' is stored inside the Smart-ID database.

The Smart-ID database is regularly synchronised to another data center and regularly copied to the backup storage.

Backing up of KWK of 'Server's part of the private key'

The 'Server's part of the private key' is encrypted with KWK, which is stored inside the Smart-ID HSM module.

The HSM module is regularly syncronized to another data center and regularly backed up to backup storage.

Backing up 'Server's share of the private key'

The 'Server's share of the private key' is stored inside the Smart-ID HSM module.

The Smart-ID HSM module is regularly synchronised to another data center and regularly backed up to backup storage.

6.2.5. Private Key Archival

6.2.5.1 SEB-card

Refer to clause 6.2.5 of SK PS [4].

The Subscriber Private Keys cannot be extracted or restored from the chip and are not archived.

6.2.5.2 Qualified Smart-ID

Refer to clause 6.2.5 of SK PS [4].

Components of Subscriber's 'Private key' are not archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

6.2.6.1 SEB-card

Refer to clause 6.2.6 of SK PS [4].

The Subscriber Private Keys for SEB-card are generated inside the card.

6.2.6.2 Qualified Smart-ID

Refer to clause 6.2.6 of SK PS [4].

Private key transfer into or from the cryptographic module is not done, otherwise than described in the clause 6.1.2 of this CPS.

6.2.7. Private Key Storage on Cryptographic Module

6.2.7.1 SEB-card

Refer to clause 6.2.7 of SK PS [4].

Private keys of the Subscriber's are stored on the chip of the SEB-card.

6.2.7.2 Qualified Smart-ID

Refer to clause 6.2.7 of SK PS [4].

Storage of 'App's part of the private key'

'App's part of the private key' is a random integer number. For storage, it is encrypted with the 128-bit AES key. The encrypted random number is then stored on the private area of the Smart-ID app on the mobile device storage.

The AES key is generated from the Subscriber's PIN code with the PBKDF2 function (according to RFC 2989). The AES key is never stored by the Smart-ID app.

The AES encryption algorithm is used in the CBC mode and without any padding.

Storage of 'Server's part of the private key'

'Server's part of the private key' is a random integer number. For storage in the Smart-ID database, it is encrypted with the 128-bit key-wrapping-key (KWK).

The KWK is a 128-bit AES key, which is generated inside the Smart-ID HSM module.

Storage of 'Server's share of the private key'

'Server's share of the private key' is a RSA private key. It is generated inside the Smart-ID HSM module and stored inside the HSM module.

6.2.8. Method of Activating Private Key

6.2.8.1 SEB-card

Refer to clause 6.2.8 of SK PS [4].

The Subscriber Private Keys are protected by PIN codes. The following rules apply:

- There is a separate PIN for each Private Key;
- The Subscriber must enter the activation code of the Authentication Certificate (PIN1) at least once after SEB-card has been inserted into the card reader device;
- The Subscriber must enter the activation code of the Qualified Electronic Signature Certificate (PIN2) before every single operation done with the corresponding Private Key;
- The usage of all Private Keys protected by a single PIN will be blocked after 3 consecutive incorrect tries;
- PIN can be unblocked using a PUK code;
- The usage of PUK code will be blocked after 3 consecutive incorrect tries;
- User can change the PIN and PUK codes.

The length of the activation codes is limited to:

- 4-12 numbers for the Authentication Key (PIN1);
- 5-12 numbers for the Signature Key (PIN2);
- 8-12 numbers for the The Unlock (PUK) code.

6.2.8.2 Qualified Smat-ID

Refer to clause 6.2.8 of SK PS [4].

In order to give signatures with Subscriber's 'Private Key', all components must be activated.

Activating 'App's part of the private key'

'App's part of the private key' is protected by Subscriber's PIN code and Subscriber needs to enter the PIN code to the Smart-ID app for each transaction. The clear-text PIN code is never stored by the Smart-ID app.

Subscriber's PIN code is chosen by the Subscriber during the registration process of Smart-ID.

The following rules apply:

1. PIN1 code to protect the authentication keypair have to be 4--12 numbers.
2. PIN2 code to protect the signature keypair have to be 5--12 numbers.
3. In case the Subscriber enters the wrong PIN-code 3 times in a row, the keypair is locked from usage for next three hours.
4. In case the Subscriber enters the wrong PIN-code 6 times in a row, the keypair is locked from usage for next 24 hours.
5. In case the Subscriber enters the wrong PIN-code 9 times in a row, the keypair is blocked and the certificate is revoked.

Activating 'Server's part of the private key'

'Server's part of the private key' is protected by KWK stored inside the Smart-ID HSM module. To activate the KWK, theoperator needs to enter the operator keycard into the HSM and enter the operator password to the HSM.

Activating 'Server's share of the private key'

'Server's share of the private key' is RSA private key, which is generated and stored inside the Smart-ID HSM module. To activate the key, the operator needs to enter the operator keycard into the HSM and enter the operator password to the HSM.

6.2.9. Method of Deactivating Private Key

6.2.9.1 SEB-card

Refer to clause 6.2.9 of SK PS [4].

The Private Key is deactivated by disconnecting power or resetting the card.

The Subscriber can deactivate a Private Key by entering all the PIN and PUK codes incorrectly 3 consecutive times.

6.2.9.2 Qualified Smart-ID

Refer to clause 6.2.9 of SK PS [4].

Deactivation of any component of the Subscriber's 'Private Key' also means that the Subscriber cannot give signatures anymore and needs to activate that component again.

Deactivating 'App's part of the private key'

The user entered PIN-code is only used for single transaction. The PIN and derived AES key is deleted from the Smart-ID app memory after the transaction is completed or when the Smart-ID server responds with 'Wrong PIN' error message.

Deactivating 'Server's part of the private key'

The 'Server's part of the private key' is only decrypted for single a transaction by the server and the clear-text value is immediately deleted from the Smart-ID server memory after the transaction is completed or when the Smart-ID server responds with 'Wrong PIN' error message.

Deactivating 'Server's share of the private key'

'Server's share of the private key' is stored inside the Smart-ID HSM module. Access to the keys is lost after the Smart-ID HSM or Smart-ID server is rebooted or disconnected from power.

6.2.10. Method of Destroying Private Key

6.2.10.1 SEB-card

Refer to clause 6.2.9 of SK PS [4].

The Subscriber Private Keys can be destroyed by physically destroying or damaging the chip.

6.2.10.2 Qualified Smart-ID

Refer to clause 6.2.10 of SK PS [4].

Destroying of any component of the Subscriber's 'Private key' also means that the Subscriber cannot give signatures anymore and needs to complete the registration process again.

Destroying 'App's part of the private key'

Subscriber can destroy the 'App's part of the private key' from the Smart-ID app during the account closing (for example, by closing the account in app or in the self-service portal, by uninstalling the app, by destroying the mobile device, etc).

Destroying 'Server's part of the private key'

'Server's part of the private key' is deleted in the Smart-ID server during the account closing (for example, by closing the account in app or in the self-service portal, after multiple wrong PIN codes entered, detection of cloned device, etc).

Destroying 'Server's share of the private key'

'Server's share of the private key' is deleted in the Smart-ID HSM module during the account closing (for example, by closing the account in app or in the self-service portal, after multiple wrong PIN codes entered, detection of cloned device, etc).

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS.

SEB-card is QSCD.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to clause 6.3.1 of SK PS [4].

All the Subscriber Public Keys are kept in database of SK and may be archived after expiration of the CA that has issued the certificates.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Refer to clause 6.3.2 of SK PS [4].

For Subscriber Certificates, the validity period is defined in clause 7.1 of this CPS.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

6.4.1.1 SEB-card

Refer to clause 6.4.1 of SK PS [4].

Activation codes are printed in one copy by Trüb Baltic AS straight to the security envelope which is handed over to the Subscriber unopened. Activation codes are protected in such way that it is impossible to read them without breaking security element. The Subscriber has prerogative to refuse from accepting of activation codes with altered security element.

6.4.1.2 Qualified Smart-ID

Refer to clause 6.4.1 of SK PS [4].

Smart-ID Application generates random activation codes and provides the Subscriber option to choose his own activation codes as well.

Activation data is used as the input seed to the encryption key derivation function (PBKDF2) and the resulting key is used to encrypt the locally stored 'App's part of the private key'. The activation codes themselves are never stored in the Smart-ID Application nor in the Smart-ID Service Provider.

6.4.2. Activation Data Protection

6.4.2.1 SEB-card

Refer to clause 6.4.2 of SK PS [4] and 6.4.1.1 of this CPS.

6.4.2.2 Qualified Smart-ID

Refer to clause 6.4.2 of SK PS [4].

Smart-ID Application generates random activation codes and displays them once to the Subscriber. After that, activation codes themselves are never stored in the Smart-ID Application nor in the Smart-ID Service Provider.

Subscriber has to memorise the activation codes and never share them with anyone.

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Refer to clause 6.5.1 of SK PS [4].

Subscriber is responsible for applying reasonable protections on her device.

6.5.2. Computer Security Rating

Refer to clause 6.5.2 of SK PS [4].

Subscriber is responsible for applying reasonable protections on her device.

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [4].

Subscriber is responsible for applying reasonable protections on her device.

6.7. Network Security Controls

6.7.1 SEB-card

Refer to clause 6.7 of SK PS [4].

Subscriber is responsible for applying reasonable protections on her device.

6.7.2 Qualified Smart-ID

Refer to clause 6.7 of SK PS [4].

Smart-ID app and Smart-ID server communicates with each other over the TLS channel. App implements the certificate pinning to verify the authenticity of channel endpoint. Server implements the app authentication to verify the authenticity of channel endpoint.

Server enforces known good encryption cipher-suites on the TLS channel.

Subscriber is responsible for applying reasonable protections on her device.

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [4].

Not applicable to Subscribers.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

Certificate profile is described in the Certificate Profile for SEB-card [5] and the Certificate Profile for Smart-ID [13], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

7.2. CRL Profile

The CRL profile is described in the Certificate Profile for SEB-card [5], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

The CRL profile for Q Smart-ID Certificates is not issued.

7.3. OCSP Profile

The OCSP profile is described in the Certificate Profile for SEB-card [5] and the Certificate Profile for Smart-ID [13], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

8. Compliance Audit and Other Assessments

Refer to chapter 8 of SK PS [4].

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

9.1.1 SEB-card

The fee for the certificate issuance is considered business secret of SK and SEB.

Certificate renewal is not performed.

9.1.2 Qualified Smart-ID

Certificate issuance for the Subscriber is free of charge.

Certificate renewal is not performed.

9.1.2. Certificate Access Fees

Valid and activated Certificates are available via OCSP service.

SEB-card Certificates are accessible directly on the SEB-card without any fees.

There are no public records about the Certificates.

9.1.3. Revocation or Status Information Access Fees

Revocation of the Certificate of SEB-card is free of charge.

A valid CRL is free of charge and accessible on SK's website https://sk.ee/en/repository/CRL/.

An OCSP service for online verification is free of charge and publicly accessible.

In case of other manners of publication information on certificate status, SK may fix a fee in a price list or require corresponding agreement.

9.1.4. Fees for Other Services

Fees for other services are specified in SK's price list or in the Subscriber's or Relying Party's agreement.

Fees for termination of suspension of the Certificates of the SEB-card and issuance of replacement PIN envelopes are specified in SEB Customer Service Point agreement.

9.1.5. Refund Policy

Refer to clause 9.1.5 of SK PS [4].

Financial settlements are considered business secret of SEB and SK.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Refer to clause 9.2.1 of SK PS [4].

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of SK PS [4].

9.3. Confidentiality of Business Information

Refer to clause 9.3 of SK PS [4].

9.4. Privacy of Personal Information

Refer to clause 9.4 of SK PS [4].

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CPS.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

9.6.1.1 SEB-card

Refer to clause 9.6.1 of SK PS [4].

SK ensures that:

- the supply of the certification service is in accordance with this CPS and the CP for SEB-card [6]; it keeps account of the certificates issued by it and of their validity;
- it accepts applications for suspension of SEB-card Certificates;
- it provides the possibility to check the validity of certificates 24 hours a day;
- the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
- the certification keys used in the supply of the certification service are activated on the basis of shared control;
- it provides security with its internal security procedures.

9.6.1.2 Qualified Smart-ID

Refer to clause 9.6.1 of SK PS [4].

SK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- the supply of the certification service is in accordance with this CPS and the CP for Q Smart-ID [2]; it keeps account of the certificates issued by it and of their validity;
- it provides the possibility to check the validity of certificates 24 hours a day;
- the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK; the certification keys used in the supply of the certification service are activated on the basis of shared control; it provides security with its internal security procedures.

9.6.2. RA Representations and Warranties

9.6.2.1. SEB-card

9.6.2.1.1 SEB Customer Service Point

Refer to clause 9.6.2 of SK PS [4].

SEB Customer Service Point ensures that:

- it issues SEB-card to Subscribers;
- it accepts Subscriber applications for the SEB-card certificate creations, suspensions, terminations of suspension and revocations; it checks the correctness and completeness of the listed applications;
- it identifies and verifies the Subscriber submitting any of the listed applications;
- it keeps records to prove legitimacy of the Subscriber's actions;
- it provides security with its internal security procedures.

SEB Customer Service Point forwards true and complete data to SK.

SEB Customer Service Point immediately notifies SK and Trüb Baltic AS about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

9.6.2.2 Qualified Smart-ID

9.6.2.2.1 Smart-ID Provider

Smart-ID Provider ensures that:

- it accepts Subscriber applications for issuance of Smart-ID Certificates;

- provides self-service web portal in accordance with the technical requirements set in applicable agreements.

9.6.2.2.2 Customer Service Point

Refer to clause 9.6.2 of SK PS [4].

The Customer Service Point ensures that:

- it accepts applications for the Certificate revocation;
- it checks the correctness and completeness of the revocation applications;
- it identifies and verifies the Subscriber submitting application for revocation;
- it keeps records to prove legitimacy of the Subscriber's actions;
- it provides security with its internal security procedures.

9.6.2.2.3 Help Line

Refer to clause 9.6.2 of SK PS [4].

The Help Line ensures that:

- it accepts requests for revocation of Certificates of Q Smart-ID from Subscribers;
- it provides security with its internal security procedures.

The Help Line takes calls from Subscribers and other parties 24 hours a day 7 days a week.

The Help Line immediately notifies SK about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

9.6.3. Subscriber Representations and Warranties

9.6.3.1 SEB-card

Refer to clause 9.6.3 of SK PS [4].

The Subscriber ensures that:

- he/she adheres to the requirements provided by SK in this CPS; he/she
- presents true and correct information to SEB;
- in case of a change in his/her personal details, he/she immediately notifies SEB of the correct details;
- he/she uses his/her private keys and corresponding certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her private key in accordance with this CPS; he/she immediately informs SK of a possibility of unauthorised use of his/her private key and suspends or revokes his/her certificates; he/she immediately suspends or revokes his/her certificates if his/her private key has gone out of his/her possession; he/she is aware that Electronic Signatures given on the basis of expired, revoked or suspended certificates are invalid.

The Subscriber is not responsible for the acts performed during the suspension of certificates.

In case the Subscriber terminates suspension of certificates, the Subscriber is solely and fully responsible for any consequences of Authentication and Electronic Signature using the certificates during the time when the certificates were suspended.

If the Subscriber has a suspicion that the SEB-card has gone out of control of the Subscriber at the time of suspension of certificates, the Subscriber is obliged to revoke the certificates.

The Subscriber is solely responsible for the maintenance of his/her private key.

The Subscriber has to accept the Terms and Conditions of SEB-card [11].

9.6.3.2 Qualified Smart-ID

Refer to clause 9.6.3 of SK PS [4].

The Subscriber ensures that:

- he/she adheres to the requirements provided by SK in this CPS; he/she presents true and correct information to Smart-ID System;
- in case of a change in his/her personal details, he/she notifies Smart-ID Provider of the correct details during a reasonable time;
- he/she uses his/her private keys and corresponding certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her private key in accordance with this CPS;
- he/she immediately informs SK of a possibility of unauthorised use of his/her private key and revokes his/her certificates;
- he/she immediately revokes his/her certificates if his/her private key has gone out of his/her possession;

- he/she is aware that Electronic Signatures given on the basis of expired or revoked certificates are invalid.

The Subscriber is solely responsible for the maintenance of his/her private key.

The Subscriber has to accept the Terms and Conditions of Q Smart-ID [14].

9.6.4. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [4].

A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in this CPS, the CP for SEB-card [6] and the CP for Q Smart-ID [2].

If not enough evidence is enclosed to the Certificate or Electronic Signature with regard to the validity of the Certificate, a Relying Party verifies the validity of the Certificate on the basis of certificate validation services offered by SK at the time of using the Certificate or affixing a Qualified Electronic Signature.

A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CP for SEB-card [6] and the CP for Q Smart-ID [2].

A Relying Party uses CRL service on its own responsibility.

9.6.5. Representations and Warranties of Other Participants

9.6.5.1 SEB-card

9.6.5.1.1 Trüb Baltic AS

An employee of Trüb Baltic AS is not punished for an intentional crime.

Trüb Baltic AS provides security with its internal security procedures.

9.6.5.2 Qualified Smart-ID

9.6.5.2.1 Smart-ID Provider

Smart-ID Provider ensures that:

- it adheres to the key generation and storage procedures under its control and described in this CPS;
- it adheres to provisions of fees described in this CPS;
- it transfers the correct Certificate and correct Certificate status information.

9.7. Disclaimers of Warranties

Refer to clause 9.7 of SK PS [4].

9.8. Limitations of Liability

Refer to clause 9.8 of SK PS [4].

9.9. Indemnities

Indemnities between the Subscriber and SK are regulated in the Terms and Conditions of SEB-card [11] and the Terms and Conditions of Q Smart-ID [14].

9.10. Term and Termination

9.10.1. Term

Refer to clause 2.2.1 of this CPS.

9.10.2. Termination

Refer to clause 9.10.2 of SK PS [4].

9.10.3. Effect of Termination and Survival

SK communicates the conditions and effect of this CPS's termination via its public repository. The communication specifies which provisions survive termination.

At a minimum, all responsibilities related to protecting personal and confidential information, also maintenance of SK archives for determined period and logs survive termination. All Subscriber agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

Termination of this CPS cannot be done before termination actions described in clause 5.8 of this CPS.

9.11. Individual Notices and Communications with Participants

The Subscriber is granted a right to get familiarized with the Terms and Conditions of SEB-card [11] and the Terms and Conditions of Q Smart-ID [14], before agreeing to and signing it.

The Subscriber's individual notices are communicated via the Subscriber's email address contained in the Certificate which the Subscriber provided during submitting an application for the SEB-card.

The Subscriber's individual notices are communicated via the Subscriber's email address or mobile phone number contained in registration form for Q Smart-ID account.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to clause 1.5.4 of this CPS.

9.12.2. Notification Mechanism and Period

Refer to clause 2.2.1 of this CPS.

9.12.3. Circumstances Under Which OID Must be Changed

Not applicable.

9.13. Dispute Resolution Provisions

Refer to clause 9.13 of SK PS [4].

The Subscriber or other party can submit their claim or complaint at the email address info@sk.ee.

9.14. Governing Law

This CPS is governed by the jurisdictions of the European Union and Estonia.

9.15. Compliance with Applicable Law

Refer to clause 9.15 of SK PS [4].

Additionally, SK ensures compliance with the Personal Data Protection Act [12].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

SK contractually obligates each RA to comply with this CPS and applicable industry guidelines. SK also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party prevails, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of SK. Unless specified otherwise in a contract with a party, SK does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS remains valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

SK may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. SK’s failure to enforce a provision of this CPS does not waive SK’s right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by SK.

9.16.5. Force Majeure

Refer to clause 9.16.5 of SK PS [4].

9.17. Other Provisions

Not applicable.

10. References

1. AS Sertifitseerimiskeskus - Certification Practice Statement, published: https://sk.ee/en/repository/CPS/;
2. AS Sertifitseerimiskeskus – Certificate Policy for Qualified Smart-ID, published: https://sk.ee/en/repository/CP/;
3. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
4. AS Sertifitseerimiskeskus Trust Services Practice Statement, published: https://sk.ee/en/repository/sk-ps/;
5. Certificate, CRL and OCSP Profile for SEB-cards, published: https://sk.ee/en/repository/profiles/;
6. AS Sertifitseerimiskeskus – Certificate Policy for the SEB card, published: https://sk.ee/en/repository/CP/;
7. ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;
8. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
9. 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;
10. ISO/IEC 7816, Parts 1-4, published: http://iso.org;
11. Terms and Conditions for Use of Certificates of SEB-card, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
12. Personal Data Protection Act, RT I 2007, 24, 127, published: https://www.riigiteataja.ee/en/eli/ee/507032016001/consolide/current;
13. Certificate and OCSP Profile for Smart-ID, published: https://sk.ee/en/repository/profiles/;
14. Terms and Conditions for Use of Certificates of Qualified Smart-ID, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/.