AS Sertifitseerimiskeskus – Certificate Policy for the SEB card

Version 3.0

OID: 1.3.6.1.4.1.10015.13.1

Effective since 01.01.2017

Version History		
Date	**Version**	**Changes**
01.01.2017	3.0	Approved version - Redesigned the Certificate Policy in accordance with the IETF RFC 3647 [1] and eIDAS [2].
26.02.2015	2.0	Editorial corrections and improvements to document formatting. Updated requirements to issue SEB-card also in Latvian and Lithuanian SEB branches. Chapter 2.4.2 - updated publication frequency of Certificate Revocation List. Chapter 6.1.2.2 - specified the Protection of Client's Private Key and Activation Codes during Personalization Period. Chapter 9 - updated references to the related legislations.
21.09.2012	1.0	Version 1.0

1. Introduction

1.1. Overview

This document, named "AS Sertifitseerimiskeskus – Certificate Policy for the SEB card" (hereinafter referred to as CP), defines procedural and operational requirements that Sertifitseerimiskeskus (hereinafter referred to as SK) adheres to and requires entities to adhere to when issuing and managing the Certificates for employee cards issued to natural persons (hereinafter referred as SEB card) issued by AS SEB Pank, AS SEB Banka and AB SEB bankas (hereinafter referred together as SEB). These Certificates facilitate electronic signatures and electronic identification of natural persons. The certificates always come in pairs: each SEB card contains one Authentication certificate and one Qualified Electronic Signature Certificate and their corresponding Private keys. Each Private Key is protected by separate activation data (PIN code) and each SEB card has a single Unlock (PUK code). A single person can have only one SEB card with valid Certificates at any point of time. The SEB cards are physically shaped in ID-1 format, comply to the ISO/IEC 7816 [3] and ID Card Documentation [4].

Issuing and managing Certificates for the SEB card is based on Regulation (EU) N° 910/2014 [2] which establishes a legal framework for electronic signatures.

> This document describes only restrictions to the Policy for EU qualified Certificates issued to natural persons where the Private Key and the related Certificate reside on a QSCD (QCP-n-qscd) from ETSI EN 319 411-2 [5] and Normalised Certificate Policy requiring a Secure Cryptographic Device (NCP+) from ETSI EN 319 411-1 [6].
>
> **The semantics of “no stipulation” in this document is that no additional restrictions are set and relevant provisions from QCP-n-qscd and NCP+ are applied directly.**

Issuing and managing Qualified Electronic Signature Certificates for the SEB card is based on the requirements of the Policy QCP-n-qscd: Certificate Policy for EU qualified Certificates issued to natural persons with Private Key related to the certified Public Key in a QSCD.

Issuing and managing Authentication Certificates for the SEB card is based on the requirements of the Policy NCP+: Normalised Certificate Policy requiring a Secure Cryptographic Device.

The Certification Service for Qualified Electronic Signature Certificates for the SEB card described in this CP SHALL be qualified trust service according to the Trusted List of Estonia.

Data structures and communication protocols in use SHALL be as described in ID Card Documentation [4] where applicable.

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

- QCP-n-qscd,
- NCP+,
- this CP,
- CPS.

This CP is a complete redesign of the previous AS Sertifitseerimiskeskus - Certification Practice Statement [7] and SEB-card Certification Policy [8]. Redesign of the above mentioned documents in accordance with IETF RFC 3647 [1] and enforcement of this CP does not substantially change provision of the corresponding Certification Services.

To preserve IETF RFC 3647 [1] outline, this CP is divided into nine parts, section headings that do not apply, are designated as **"Not applicable"**. Each top-level chapter includes references to the relevant sections in ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

In this CP modal verbs in capital letters are to be interpreted as described in Clause 3.2 of the ETSI Drafting Rules [9] (Verbal forms for the expression of provisions).

Terms and acronyms listed in Clause 1.6 of this CP, are written starting with a capital letter in this CP.

1.2. Document Name and Identification

Refer to Clause 5.3 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

This document is named “AS Sertifitseerimiskeskus – Certificate Policy for the SEB card".

This CP is identified by 1.3.6.1.4.1.10015.13.1

OID is composed according to the contents of the following table.

Parameter	OID reference
Internet attribute	1.3.6.1

Private entity attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification Service attribute	13.1

Qualified Electronic Signature Certificate for the SEB card issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-2 [5] clause 5.3 c) for QCP-n-qscd: 0.4.0.194112.1.2

  Itu-t(0) identified-Organisation(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)
- This CP.

Authentication Certificates for SEB card issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [6] clause 5.3 b) for NCP+: 0.4.0.2042.1.2

  itu-t(0) identified-Organisation(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
- This CP.

1.3. PKI Participants

Refer to Clause 5.4 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

1.3.1. Certification Authorities

No stipulation.

1.3.2. Registration Authorities

In the role of RA acts SEB.

1.3.3. Subscribers

Subscriber is the Subject of the Certificate issued under this CP.

Subscriber can be only a natural person appointed by SEB who SHALL have:

- Estonian personal code and valid Estonian personal identification document, residence permit card, digital identity document or the e-residence card or
- Latvian personal code or
- Lithuanian personal code.

1.3.4. Relying Parties

Relying Parties are legal or natural persons who are making decisions based on the Certificate.

1.3.5. Other Participants

Card Personaliser is the manufacturer of SEB card.

1.4. Certificate Usage

Refer to Clause 5.5 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Qualified Electronic Signature Certificate is intended for:

- creating Qualified Electronic Signatures compliant with eIDAS [2].

Authentication Certificate is intended for:

- Authentication,
- secure e-mail
- Smart Card logon to the workstation.

CA Private Keys SHALL NOT be used to sign other types of Certificates except for the following:

- Subscriber Certificates compliant with QCP-n-qscd or NCP+,
- OCSP response verification Certificates,
- Internal Certificates for technical needs.

1.4.2. Prohibited Certificate Uses

Subscriber Certificates issued under this CP SHALL NOT be used for any of the following purposes:

- unlawful activity (including cyber attacks and attempt to infringe the Certificate or the SEB card),
- issuance of new Certificates and information regarding Certificate validity,
- enabling other parties to use the Subscriber's Private Key,
- enabling the Certificate issued for electronic signing to be used in an automated way,
- using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

The Subscriber Authentication Certificate SHALL NOT be used to create Qualified Electronic Signatures compliant with eIDAS [2].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP is administered by SK.

AS Sertifitseerimiskeskus

Registry code 10747013

Pärnu Mnt 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

No stipulation.

1.5.4. CPS Approval Procedures

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

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

All amendments to this CP SHALL be coordinated with RA as well as the Card Personaliser.

All amendments SHALL be approved by the business development manager and amended CP SHALL be enfored by the CEO.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CP 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.
Card Personaliser	Manufacturer of SEB cards.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [10], 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 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.
Directory Service	Trust service related to publication of Certificate validity information.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
ID-1	Format which defines physical characteristics of identification cards according to the standard ISO/IEC 7816 [3].
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.
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.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
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 [2] Regulation.

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 [2] Regulation.
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.
SEB card	Employee card issued by SEB linked to Certificates facilitate electronic signatures and electronic identification of natural persons. These documents are not deemed identity documents in the legal sense.
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 the SEB card 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.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy. This document is a CP.
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [2] 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
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
SEB	AS SEB Pank, AS SEB Banka, AB SEB bankas. Legal bodies tasked with issuing SEB cards to natural persons.
SK	AS Sertifitseerimiskeskus, Certification Service provider
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement [11]

2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

2.1. Repositories

SK SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a

scheduled downtime that does not exceed 0,5% annually.

2.2. Publication of Certification Information

2.2.1. Publication and Notification Policies

This CP, the Certification Practice Statement [12], the Certificate Profile [10], as well as the Terms and Conditions [13] with the enforcement dates SHALL be published on SK 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

Information about service levels, fees and technical details laid out in mutual agreements between SK, RA and Card Personaliser MAY be left out of CPS.

The CPS MAY not cover internal procedures of the RA and Card Personaliser.

2.3. Time or Frequency of Publication

No stipulation.

2.4. Access Controls on Repositories

No stipulation.

3. Identification and Authentication

Refer to Clause 6.2 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

3.1. Naming

The Distinguished Name of the Subscriber SHALL comply with the conventions set in the Certificate Profile [10].

3.1.1. Type of Names

No stipulation.

3.1.2. Need for Names to be Meaningful

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

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

All the names in Certificates SHALL be encoded in UTF-8.

3.1.5. Uniqueness of Names

SK SHALL ensure that Certificates with matching Common Name (CN), SerialNumber and e-mail addresses in Subject Alternative Name (SAN) fields are not issued to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Private Keys SHALL be generated on the QSCD during personalisation by the Card Personaliser.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

Authentication SHALL be carried out by RA in accordance with procedures set in applicable agreements.

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information SHALL NOT be allowed in a Certificate.

3.2.5. Validation of Authority

Validation SHALL be carried out by RA in accordance with applicable agreements.

3.2.6. Criteria for Interoperation

No stipulation.

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 CP.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to Clause 3.2 of this CP.

3.4. Identification and Authentication for Revocation Request

No stipulation.

4. Certificate Life-Cycle Operational Requirements

Refer to Clause 6.3 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

SEB CAN submit SEB card application. SK SHALL accept CSRs only from the Card Personaliser after receiving corresponding signed SEB card application from SEB.

4.1.2. Enrolment Process and Responsibilities

SEB WILL request a new SEB card from Card Personaliser and sends corresponding signed SEB card application to SK.

It is the responsibility of a Card Personaliser to manufacture the card, imprint visual elements to it, fill out Personal Data File on the card, generate keypairs for Authentication and Qualified Electronic Signature and submit a pair of CSRs to SK.

SEB is responsible for submitting correct identification data (names, personal codes, dates, picture) to the Card Personaliser. Card Personaliser and SK SHALL rely upon the values provided by SEB.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber's identity WILL be validated by SEB as described in procedures set in applicable agreements.

SEB WILL send the SEB card application to Card Personaliser and corresponding signed SEB card application to SK.

SK SHALL accept CSRs only from the Card Personaliser after receiving corresponding signed SEB card application from SEB. SK and Card Personaliser SHALL rely upon identification data provided by SEB.

4.2.2. Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate for which there is no previous approval from SEB as required in clause 4.1.1 of this CP.

CA SHALL refuse to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable agreements. If the data contained in a CSR needs to be modified, the corresponding amendment SHALL be coordinated with SEB.

4.2.3. Time to Process Certificate Applications

In accordance with the applicable agreements.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

After Certificate Issuance OCSP service SHALL return response "REVOKED" and the Ceritifcate is listed in CRL as suspended until the SEB card is handed over to and accepted by the Subject.

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

No stipulation.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

For Certificate acceptance Subscriber SHALL sign the application for activation of Certificates.

In case activation in RA office employee of processing the activation SHALL be different from the one who handed over the SEB card.

4.4.2. Publication of the Certificate by the CA

OCSP SHALL start responding with "GOOD" and the Certificate is removed from CRL immediately after the Subscriber has accepted the Cer tificate.

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

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

No stipulation.

4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

4.6. Certificate Renewal

Not allowed.

4.7. Certificate Re-Key

Certificate re-key SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks.

During Certificate re-key, the Certificates to be replaced SHALL be revoked.

Certificate re-key MAY be done only upon initial application in the case of SEB card manufacturing errors before acceptance of the Certificates. In this case only the last Certificates SHALL be written to the card and remain valid. All the errorneous or unusable Certificates SHALL be revoked immediately.

4.7.1. Circumstances for Certificate Re-Key

This CP treats recurring SEB card application as initial application for SEB card. If the SEB applies recurring SEB card, this request SHALL be processed as an application for a new SEB card, and physical authentication SHALL be done.

Certificate re-key is allowed to

- replace an expired or broken SEB card;
- fix production errors that are discovered during quality checks.

Additional circumstances for Certificate Re-key SHALL be agreed upon with SEB and the CP and CPS SHALL be updated to reflect the changes.

4.7.2. Who May Request Certification of a New Public Key

Only the SEB CAN initiate the re-key process unless the need to replace the Certificate is discovered during quality checks before delivery of the SEB card to the Subscriber. SK SHALL NOT accept re-key requests from other parties except Card Personaliser.

4.7.3. Processing Certificate Re-Keying Requests

If the re-keying is to replace an expired or broken SEB card or to apply recurring SEB card, the process is similar to initial issuance.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

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

Refer to Clause 4.4.2 of this CP.

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

No stipulation.

4.8. Certificate Modification

Certificate modification SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks.

During Certificate modification, the Certificates to be replaced SHALL be revoked.

Certificate modification MAY be done only upon initial application in the case of SEB card manufacturing errors before acceptance of the Certificates. In this case only the last pair of Certificates SHALL be written to the SEB card and remain valid. All the errorneous or unusable Certificates SHALL be revoked immediately.

4.8.1. Circumstances for Certificate Modification

Certificate modification is allowed to

- change the data that is visually imprinted on SEB card and stored in the Personal Data File;
- fix production errors that are discovered during quality checks.

Additional circumstances for Certificate modification SHALL be agreed upon with SEB and the CP and CPS SHALL be updated to reflect the changes.

4.8.2. Who May Request Certificate Modification

SEB CAN initiate the modification process. In case the need to replace the Certificate is discovered during quality checks before the delivery of the SEB card to the Subscriber Certificate modification MAY be performed by the CA internally or requested by SEB and Card Personaliser.

SK SHALL NOT accept modification requests from other parties except for the Card Personaliser after received corresponding signed SEB card application from SEB.

4.8.3. Processing Certificate Modification Requests

In case of fixing production errors CA SHALL process Certificate modification requests and is not required to negotiate it with the Subscriber.

In case of changing the data that is visually imprinted on the SEB card and stored in the Personal Data File this request SHALL be processed as an application for a new SEB card, and physical authentication SHALL be done.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of the Modified Certificate by the CA

Refer to Clause 4.4.2 of this CP

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

No stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances for Certificate revocation SHALL be as laid down in Article 19 of the Estonian eIDAS supplement Act [14].

In addition Certificate revocation SHALL be done in case revocation of SEB card due to termination of the contract between Subscriber and SEB or is when the SEB card is damaged or needs replacement for some other reasons.

In addition Certificate suspension SHALL be done by CA in case of reasonable doubt that the Certificate contains inaccurate data or the certificate is not under the control of the Subscriber and may be used without the Subscriber's consent.

Revoked Certificate SHALL NOT be reinstated.

4.9.2. Who Can Request Revocation

Entities eligible to request Certificate revocation SHALL be as laid down in Article 19 of the Estonian eIDAS supplement Act [14].

In addition Subscriber and SEB CAN request Certificate revocation.

4.9.3. Procedure for Revocation Request

The procedure for revocation request SHALL be as laid down in Article 20 of the Estonian eIDAS supplement Act [14].

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time Within Which CA Must Process the Revocation Request

No stipulation.

4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency

No stipulation.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

Circumstances for Certificate suspension SHALL be as laid down in Article 17 of the Estonian eIDAS supplement Act [14].

In addition Certificate suspension SHALL be done upon the discovery of loss of SEB card or in case of reasonable doubt that the Certificate contains inaccurate data or the certificate is not under the control of the Subscriber and may be used without the Subscriber's consent.

4.9.14. Who Can Request Suspension

Anyone can request Certificate suspension.

4.9.15. Procedure for Suspension Request

It SHALL be possible to request Certificate suspension via phone 24 hours a day, 7 days a week. Certificate suspension SHALL leave a uniquely identifiable trace.

4.9.16. Limits on Suspension Period

No limits.

4.9.17. Circumstances for Termination of Suspension

Circumstances for Termination of Certificate suspension SHALL be as laid down in Article 18 of the Estonian eIDAS supplement Act [14].

4.9.18. Who Can Request Termination of Suspension

Entities who can request termination of Certificate suspension SHALL be as laid down in Article 18 of the Estonian eIDAS supplement Act [14].

In addition Subscriber CAN request termination of suspension.

4.9.19. Procedure for Termination of Suspension

The procedure for termination of Certificate suspension SHALL be as laid down in Article 18 of the Estonian eIDAS supplement Act [14].

4.10. Certificate Status Services

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

SK SHALL ensure that the Certificate Status Services are available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0,5% annually.

4.10.3. Operational Features

No stipulation.

4.11. End of Subscription

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

Not allowed.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

Refer to Clause 6.4 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

6. Technical Security Controls

Refer to Clause 6.5 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The Subscriber Certificate keys SHALL be generated using the QSCD by Card Personaliser.

6.1.2. Private Key Delivery to Subscriber

Certificate keys SHALL be delivered on a QSCD that SHALL be handed over to the SEB by the Card Personaliser.

SEB, in turn, SHALL deliver it unopened to the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

The Card Personaliser SHALL deliver the Public Key to the CA using a secure communication channel.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [10].

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

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

Allowed key usage flags SHALL be set as described in the Certificate Profile [10].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Private Key SHALL be generated on a QSCD.

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

No stipulation.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

No stipulation.

6.2.5. Private Key Archival

No stipulation.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation.

6.2.8. Method of Activating Private Key

The Subscriber SHALL be prompted to enter the PIN code of the Authentication Certificate at least once after the SEB card has been inserted into the card reader device.

The Subscriber SHALL be prompted to enter the PIN code of the Qualified Electronic Signature Certificate before every single operation done with the corresponding Private Key.

It SHALL be possible to create different PIN codes for different keys of the Subscriber.

The length of the PIN codes SHALL be at least:

- for the Authentication Key 4 numbers,
- for the signature Key 5 numbers,

The PUK code SHALL be at least 8 numbers.

6.2.9. Method of Deactivating Private Key

SEB card SHALL be permanently blocked after three failed attempts to enter the PUK code.

In case the PUK code is lost or the SEB card is permanently blocked the Client SHALL apply for a new SEB card.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Validity period of the Subscriber Certificate SHALL NOT exceed the validity period of the corresponding SEB card, for which it was issued.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Activation PIN codes SHALL be generated by the Card Personaliser and SHALL be included in a separate sealed envelope for delivery to the Subscriber. Copies of the PIN codes SHALL NOT be stored by the Card Personaliser.

6.4.2. Activation Data Protection

PIN codes SHALL be handed over personally to the Subscriber by the RA.

Copies of the PIN codes SHALL NOT be stored by the RA.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

No stipulation.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

No stipulation.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

No stipulation.

6.8. Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

7.1. Certificate Profile

The Certificate SHALL comply with the profile described in Certificate Profile [10].

7.2. CRL Profile

The CRL SHALL comply with the profile described in the Certificate Profile [10].

7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [10].

8. Compliance Audit and Other Assessments

Refer to Clause 6.7 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

9. Other Business and Legal Matters

Refer to Clause 6.8 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

No stipulation.

9.3.2. Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility to Protect Confidential Information

No stipulation.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation.

9.4.2. Information Treated as Private

No stipulation.

9.4.3. Information Not Deemed Private

No stipulation.

9.4.4. Responsibility to Protect Private Information

No stipulation.

9.4.5. Notice and Consent to Use Private Information

No stipulation.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CP.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

An employee of CA SHALL NOT be punished for an intentional crime.

9.6.2. RA Representations and Warranties

An employee of RA SHALL NOT be punished for an intentional crime.

9.6.3. Subscriber Representations and Warranties

No stipulation.

9.6.4. Relying Party Representations and Warranties

Relying Party SHALL verify the validity of the Certificate using validation services offered by SK prior to using the Certificate.

Relying Party SHALL consider the limitations stated in the Certificate and SHALL ensure that the transaction to be accepted corresponds to this CP.

9.6.5. Representations and Warranties of Other Participants

An employee of Card Personaliser SHALL NOT be punished for an intentional crime.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

Refer to Clause 2.2.1 Publication and Notification Policies of this CP.

9.10.2. Termination

This CP SHALL remain in force until it is replaced by the new version or when it is terminated due to the CA termination or when the service is terminated and all the Certificates therefore become invalid.

9.10.3. Effect of Termination and Survival

SK SHALL communicate the conditions and effect of termination of this CP.

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to Clause 1.5.4 of this CP.

9.12.2. Notification Mechanism and Period

Refer to Clause 1.5.4 of this CP.

9.12.3. Circumstances Under Which OID Must be Changed

OID SHALL change when the scope of this CP changes or when the new type of the Certificate occurs.

9.13. Dispute Resolution Provisions

No stipulation.

9.14. Governing Law

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

9.15. Compliance with Applicable Law

SK SHALL ensure compliance with the following requirements:

- eIDAS [2] - 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,

- Estonian eIDAS supplement Act [14],

- Personal Data Protection Act [15],

- related European Standards:

    - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [16],
    - EN 419 211 Protection profiles for secure signature creation device [17],
    - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [6],
    - ETSI EN 319 411-2 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 [5].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

No stipulation.

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

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. Other Provisions

Not allowed.

10. References

1. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt;
2. 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;
3. ISO/IEC 7816, Parts 1-4, published at http://iso.org;
4. ID Card documentation webpage: http://www.id.ee/index.php?id=35772;
5. 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;
6. 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;
7. AS Sertifitseerimiskeskus – Certification Practice Statement (CPS), published: https://sk.ee/en/repository/CPS/;
8. SEB-card Certification Policy, published: https://sk.ee/en/repository/CP/;
9. ETSI Drafting Rules (Verbal forms for the expression of provisions);
10. Certificate, CRL and OCSP Profile for SEB-cards published: https://sk.ee/en/repository/profiles/;

11 AS Sertifitseerimiskeskus Trust Services Practice Statement, published: https://sk.ee/en/repository/sk-ps/;
12 AS Sertifitseerimiskeskus - EID-SK Certification Practice Statement, published: https://sk.ee/en/repository/CPS/;
13 Terms and Conditions for Use of Certificates of SEB-card, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
14 Estonian eIDAS supplement Act (2016-05, draft);
15 Personal Data Protection Act, 06.01.2016, published: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current;
16 ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
17 ETSI EN 419 211 Protection profiles for secure signature creation device.