Document Information	
Name	SK ID Solutions AS - ESTEID2018 Certification Practice Statement
Version number	4.0
Version No. and date	Changes
10.04.2020 4.0	Clause 1.5.4 - added that SK performs annual review of this CPS;
17.01.2020 3.0	Clause 3.2.3.2 - specified that upon the issuance of Diplomatic-ID, MFA verifies the identity of the Subscriber via physical presence checks in accordance with the IDA [7].
01.05.2019 2.0	Added description on ESTEID service Clause 1.3.1 - replaced incorrect CA ESTEID2018 certificate with the correct one Clause 1.6.1 - corrected the definition of QSCD Clauses 4.7.1 and 4.7.2 - specified Certificate re-key process to replace broken ID-card, Digi-ID or Diplomatic-ID Clause 4.7.3 - specified that during Certificate re-key, only the last Certificates are written to the card or Digi-ID media and remain valid Added that revocation status information is in addition to OCSP service also provided via CRL service. Therefore, clauses 1.6, 4.9.3, 4.9.7, 4.9.8, 4.9.15, 4.9.19, 4.10.1, 7.2 and 9.1.3 have been amended accordingly As CRL is published 12 hours the latest after issuance of the previous CRL, it has been added in clause 4.9.9 that OCSP serves as a primary source for the Certificate status information and contains Certificate status information until the Certificate expires. In relation to the aforementioned, clause 9.6.4 has been amended to include the stipulation that Relying Party uses CRL service on its own responsibility Clause 4.9.1 - added circumstances for revocation Clause 6.1.1 - specified that the chip of the ID-card, Digi-ID or Diplomatic-ID onto the Subscriber Private Keys are loaded, is a QSCD Clause 6.1.2 - specified that the Subscriber Private Keys are delivered on the QSCD
01.11.2018 1.0	First public edition
Effective from date	10.04.2020

1. Introduction

SK ID Solutions AS 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.

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

- "SK ID Solutions AS Trust Services Practice Statement" [2] (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 [1] this CPS is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [1], section headings that do not apply have the statement **"Not applicable"**. References to SK PS [2] and the "Certificate and OCSP Profile for ID-1 Format Identity Documents Issued by the Republic of Estonia" [3] (hereinafter referred to as Certificate Profile) documents are included where applicable.

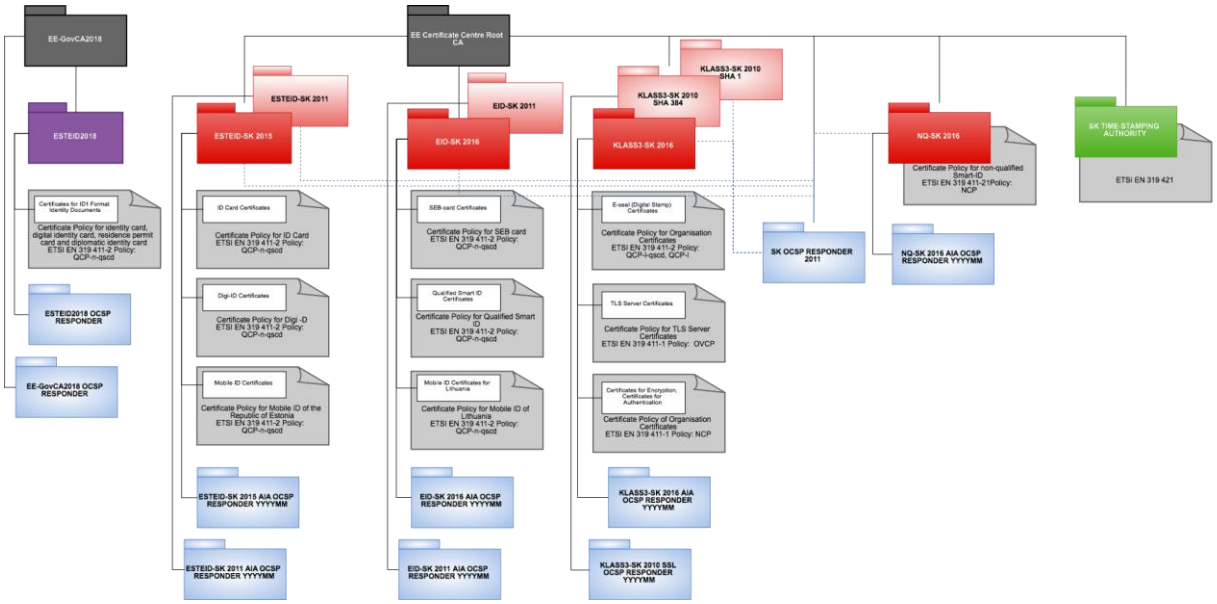
1.1. Overview

This CPS describes the practices used to comply with the "Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card [4] (hereinafter referred to as CP). This policy is compliant with ETSI EN 319 411-2 Policy: QCP-n-qscd [5] and ETSI EN 319 411-1 Policy: NCP+ [6].

SK always ensures compliance with the latest versions of the referred documents.

SK is currently using following certificate chains:

- EE Certification Centre Root CA chain, valid 2010-2030
- EE-GovCA2018 chain, valid 2018-2033



This CPS covers operation of ESTEID2018.

The certification service for Qualified Electronic Signature Certificate for the ID-card, Digi-ID and Diplomatic-ID 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 [5]
- NCP+ [6]
- CP [4]
- This CPS

1.2. Document Name and Identification

This document is called “SK ID Solutions AS – ESTEID2018 Certification Practice Statement.”

1.3. PKI Participants

1.3.1. Certification Authorities

SK operates as a Certificate Authority that issues Certificates for the ID-card, Digi-ID and Diplomatic-ID.

SK acts as a subcontractor of Idemia. There is a contract signed between Idemia and PBGB covering production, personalisation of the ID-card, Digi-ID and Diplomatic-ID as well as issuance and servicing of the Certificates.

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

The Certificates are issued by the intermediate CA ESTEID2018 that is identified by the following certificate:

Certificate: Data: Version: 3 (0x2) Serial Number: 75:47:fa:ac:14:74:4b:8b:5b:a3:66:d4:fe:66:55:ed Signature Algorithm: ecdsa-with-SHA512 Issuer: C=EE, O=SK ID Solutions AS/2.5.4.97=NTREE-10747013, CN=EE-GovCA2018 Validity Not Before: Sep 20 09:22:28 2018 GMT Not After : Sep 5 09:11:03 2033 GMT Subject: C=EE, O=SK ID Solutions AS/2.5.4.97=NTREE-10747013, CN=ESTEID2018 Subject Public Key Info: Public Key Algorithm: id-ecPublicKey Public-Key: (521 bit) pub: 04:01:c7:38:19:6f:ed:4a:d1:3d:83:f5:c8:78:4e: 6f:b4:40:fd:80:43:6e:d8:32:9d:25:4c:a9:87:71: 9c:5a:ca:1d:45:e1:ea:d1:64:82:1b:c7:b8:0d:64: d8:34:a8:9b:58:44:e6:4a:a1:07:95:6c:a4:37:a6: 6f:05:83:24:13:90:59:01:8e:23:fd:2d:dc:4b:5c: 70:b6:23:78:ce:c5:f7:13:8f:77:35:1b:65:a2:1b: a4:d4:47:a5:08:15:06:91:57:d3:1a:4b:4e:05:b6: ec:ca:48:32:15:3c:0c:70:56:16:97:80:68:d5:f7: 79:4a:43:e2:00:b9:72:f8:6c:2b:44:45:12 ASN1 OID: secp521r1 X509v3 extensions: X509v3 Authority Key Identifier: keyid:7E:29:56:E7:34:92:78:4E:77:E1:6F:2E:33:2A:98:71:C1:FD:34:9F X509v3 Subject Key Identifier: D9:AC:70:DB:5F:7E:BE:94:F8:A0:E4:BE:47:A2:D0:34:AD:9A:2A:12 X509v3 Key Usage: critical Certificate Sign, CRL Sign X509v3 Basic Constraints: critical CA:TRUE, pathlen:0 X509v3 Certificate Policies: Policy: 0.4.0.2042.1.2 Policy: 0.4.0.194112.1.2 Policy: 1.3.6.1.4.1.51361.1.1.1 CPS: https://www.sk.ee/CPS Policy: 1.3.6.1.4.1.51361.1.1.2 Policy: 1.3.6.1.4.1.51455.1.1.1 Policy: 1.3.6.1.4.1.51361.1.1.5 Policy: 1.3.6.1.4.1.51361.1.1.6 Policy: 1.3.6.1.4.1.51361.1.1.7 Policy: 1.3.6.1.4.1.51361.1.1.3 Policy: 1.3.6.1.4.1.51361.1.1.4 Policy: 1.3.6.1.4.1.51361.1.1.8 Policy: 1.3.6.1.4.1.51361.1.1.9 Policy: 1.3.6.1.4.1.51361.1.1.10 Policy: 1.3.6.1.4.1.51361.1.1.11 Policy: 1.3.6.1.4.1.51361.1.1.12 Policy: 1.3.6.1.4.1.51361.1.1.13 Policy: 1.3.6.1.4.1.51361.1.1.14 Policy: 1.3.6.1.4.1.51361.1.1.15 Policy: 1.3.6.1.4.1.51361.1.1.16 Policy: 1.3.6.1.4.1.51361.1.1.17 Policy: 1.3.6.1.4.1.51361.1.1.18 Policy: 1.3.6.1.4.1.51361.1.1.19 Policy: 1.3.6.1.4.1.51361.1.1.20 Policy: 1.3.6.1.4.1.51455.1.1.2 Policy: 1.3.6.1.4.1.51455.1.1.3 Policy: 1.3.6.1.4.1.51455.1.1.4 Policy: 1.3.6.1.4.1.51455.1.1.5 Policy: 1.3.6.1.4.1.51455.1.1.6 X509v3 Extended Key Usage: critical OCSP Signing, TLS Web Client Authentication, E-mail Protection Authority Information Access: OCSP - URI:http://aia.sk.ee/ee-govca2018 CA Issuers - URI:http://c.sk.ee/EE-GovCA2018.der.crt qcStatements: 0 0.....F.. X509v3 CRL Distribution Points: Full Name: URI:http://c.sk.ee/EE-GovCA2018.crl Signature Algorithm: ecdsa-with-SHA512 30:81:88:02:42:00:de:b9:46:38:1d:cc:d4:6c:52:92:d3:4d: 87:67:cf:20:72:58:18:77:3b:47:aa:09:44:37:24:cc:b5:71: 3a:74:c0:51:9c:26:e0:52:68:41:08:00:34:98:94:87:6f:21: 49:f1:6f:62:90:b8:92:ca:ea:e6:90:93:34:84:31:3d:2a:02: 42:01:23:aa:03:8d:39:21:ae:67:2a:34:c9:3c:db:07:42:53: 22:ec:a6:6c:21:c4:c7:3a:80:5c:73:1f:b9:e0:df:19:5f:53: 20:06:8c:c9:99:3e:7d:ad:96:3f:db:f3:9e:13:5e:b7:04:0c: 03:d1:47:54:40:09:cc:3c:fe:be:5b:75:5d

1.3.2. Registration Authorities

1.3.2.1. ID-card and Digi-ID

The RA-s are laid down in Chapter 3 of the IDA [7].

PBGB and MFA can appear in multiple roles throughout the process. Throughout the rest of this CPS a following distinction is made based on the role:

- Both institutions are referred to as RA when they are performing technical actions such as face to face authentication or delivery of the ID-card or Digi-ID
- They are referred together as PBGB when they are representing Republic of Estonia in the role of Document Issuer according to IDA [7], e.g. during initial identification of persons or making decisions about their eligibility to apply for an ID-card or Digi-ID

PBGB may be contacted at:

Pärnu Ave 139, 15060 Tallinn

Information: +372 612 3000

Fax: +372 612 3009

E-mail: info@politsei.ee

https://www.politsei.ee/en/

MFA can be contacted through its embassies and representations that can be checked at MFA website: http://www.vm.ee/en/embassies-and-representations.

1.3.2.1.1 PBGB Customer Service Point

Accepting applications and issuance of ID-card and Digi-ID is carried out in PBGB offices and embassies of the Republic of Estonia (hereinafter referred to as PBGB Customer Service Point).

Servicing Certificates of ID-card and Digi-ID (suspensions, terminations of suspension, revocations and designations of the replacement of PIN envelopes) is carried out in PBGB Customer Service Points.

The list and operating hours of PBGB Customer Service Points can be checked on the following websites:

- https://www2.politsei.ee/en/kontakt/kmb/
- http://www.vm.ee/en/country-representations/estonian-representations
- https://www.skidsolutions.eu/en/kontakt/customerservice/

1.3.2.2. Diplomatic-ID

In accordance with Chapter 5^3 of the IDA [7], MFA operates as an RA.

MFA can appear in multiple roles throughout the process. Throughout the rest of this CPS a following distinction is made based on the role:

- It is referred to as RA when it is performing technical actions such as face to face authentication or delivery of the Diplomatic-ID
- It is referred to as MFA when it is representing Republic of Estonia in the role of Document Issuer according to IDA [7], e.g. during initial identification of persons or making decisions about their eligibility to apply for an Diplomatic-ID

1.3.2.2.1 MFA Customer Service Point

Accepting applications and issuance of Diplomatic-ID is carried out at MFA and foreign representations of the Republic of Estonia (hereinafter referred to as MFA Customer Service Point).

Servicing Certificates of Diplomatic-ID (suspensions, terminations of suspension, revocations and designations of the replacement of PIN envelopes) is carried out in MFA Customer Service Points.

The list and operating hours of MFA Customer Service Points can be checked on the following websites:

- http://www.vm.ee/en/country-representations/estonian-representations

- https://www.skidsolutions.eu/en/kontakt/customerservice/

1.3.2.3. Help Line

The Help Line accepts applications for suspension of the Certificates from Subscribers and other parties.

Information on the Help Line and its contact details is available on SK's website https://www.skidsolutions.eu/en/kontakt/support/.

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

User support for solving problems related to ID-card and Digi-ID usage can also be requested at (+ 372) 666 8888.

1.3.3. Subscribers

Refer to clause 1.3. of the CP [4].

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. Card Manufacturer

Idemia operates as a Card Manufacturer.

Idemia:

- Accepts ID-card, Digi-ID and Diplomatic-ID orders
- Produces ID-card, Digi-ID and Diplomatic-ID blanks
- Personalises ID-card based on the orders sent by PBGB
- Personalises Diplomatic-ID based on the orders sent by MFA
- Generates the keys on the card for ID-card, and Diplomatic-ID and requests the corresponding Certificates
- Loads the Certificates to ID-card and Diplomatic-ID
- Delivers personalised ID-card to PBGB
- Delivers personalised Diplomatic-ID to MFA
- Delivers Digi-ID blanks to PBGB
- Provides technical environment for personalisation of Digi-ID in RA office
- Produces replacement PIN-envelopes for ID-card, Digi-ID and Diplomatic-ID

Idemia may be contacted at:

Karl Papello Building

Valukoja 7, Lasnamäe

11415 Tallinn

Information: +372 605 9800

Homepage: www.hansab.ee

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Refer to clause 1.4 of the CP [4].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS is administered by SK.

SK ID Solutions AS

Registry code 10747013

Pärnu Ave 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@skidsolutions.eu

https://www.skidsolutions.eu/en/

1.5.2. Contact Person

Business Development Manager

Email: info@skidsolutions.eu

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 [4] 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 publication, is published electronically on SK website.

All amendments to this CPS regarding ID-card and/or Digi-ID are coordinated with PBGB as well as Idemia.

All amendments to this CPS regarding Diplomatic-ID are coordinated with MFA and Idemia.

SK performs annual review of this CPS to ensure compliance of the present document and services provided based on this CPS with the applicable requirements.

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
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [3], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of the trust service provider's structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature. SK ID Solutions AS issues Certificates under this CPS.
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. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.

Term	Definition
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Digi-ID	Digital identity card for Estonian resident and digital identity card for e-resident. Within the meaning of this CPS, the term "Digi-ID" encompasses the previously listed identity documents unless stated otherwise.
Diplomatic-ID	Diplomatic identity card
Directory Service	Trust service related to publication of Certificate validity information.
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.
ID-card	Identity card for Estonian citizen, identity card for European Union citizen, residence permit card for long-term resident and residence permit card for temporary residence citizen. Within the meaning of this CPS, the term "ID-card" encompasses all the previously listed identity documents unless stated otherwise.
Idemia	Contractor of the PBGB who manufactures and personalises identity cards, resident permit cards and e-resident's digital identity cards as ordered by the PBGB, diplomatic identity cards as ordered by the MFA, and manufactures blank digital identity cards and provides the technical environment for the personalisation of digital identity cards in the RA offices.
ID-1	Format which defines physical characteristics of identification cards according to the standard ISO/IEC 7816 [9].
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 ID-card, Digi-ID and Diplomatic-id 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.

Term	Definition
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 eIDAS Regulation [8].
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 [8].
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.
Residence permit card	A residence card issued from year 2011 to natural persons entitled by IDA [7], is a mandatory identity document of an alien who is residing permanently in Estonia on the basis of a valid residence permit or right of residence. In this CPS is referred to as ID-card. Estonian residence permit is not the same as EU residence permit.
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.
SK Trust Services Practice Statement	A statement of practices that SK employs in providing Trust Services.
Subscriber	A natural person to whom the Certificates of ID-card, Digi-ID or Diplomatic-ID are issued as a public service if he/she has a statutory right and has requested it. Within the meaning of this CPS, the term "Subscriber" also encompasses a natural person's representative. Validation of authority of the natural person's representative is verified in accordance with clause 3.2.5 of this CPS.
Subject	In this document, the Subject is the same as the Subscriber.

Term	Definition
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 [10] upon submitting an application for the ID-card, Digi-ID or Diplomatic-ID.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014 [8] 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
IDA	Identity Documents Act [7]
MFA	Ministry of Foreign Affairs
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [6]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [5]
RA	Registration Authority
SK	SK ID Solutions AS

2. Publication and Repository Responsibilities

2.1. Repositories

Refer to clause 2.1 of SK PS [2].

2.2. Publication of Certification Information

Refer to clause 2.2 of SK PS [2].

2.2.1. Publication and Notification Policies

The CP [4] is published on website www.id.ee no less than 30 days prior to taking effect.

This CPS is published on SK's website: https://www.skidsolutions.eu/en/repository/CPS/.

This CPS and referred documents - the Certificate Profile [3] and the "Terms and Conditions for Use of Certificates for ID-1 Format Identity Documents of the Republic of Estonia" [10] (hereinafter referred to as Terms and Conditions) 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.

SK provides the capability to allow third parties to check and test Certificates it issues.

Test Certificates clearly indicate that they are for testing purposes.

2.2.2. Items not Published in the Certification Practice Statement

Refer to clause 2.2.2 of the CP [4].

Refer to clause 9.3.1 of SK PS [2].

2.3. Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.3.1. Directory Service

Refer to clause 2.3.3 of SK PS [2].

2.4. Access Controls on Repositories

Refer to clause 2.4 of SK PS [2].

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 [3].

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 [3].

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Pursuant to IDA [7], international letters are encoded according to ICAO transcription rules where necessary.

Rules for interpreting various name forms are described in the Certificate Profile [3].

3.1.5. Uniqueness of Names

Subscriber's distinguished name is compiled according to the certificate profile described in the Certificate Profile [3]. 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.

3.1.6. 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

Private Key of the Subscriber is generated by Idemia during personalisation of ID-card or Diplomatic-ID on the QSCD, i.e. in the chip of ID-card or Diplomatic-ID.

In case of Digi-ID, PBGB generates the Subscriber's Private Key during personalisation of Digi-ID on the QSCD, ie. in the chip of Digi-ID.

The cards are treated in a secure and traceable manner prior to handing over to the Subscriber.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

3.2.3.1. ID-card and Digi-ID

PBGB verifies the identity of the Subscriber upon the issuance of ID-card or Digi-ID in accordance with the IDA [7].

PBGB submits identification data to Idemia. Idemia forwards the data for the Certificate to SK.

Idemia and SK rely on the identification data provided by PBGB.

3.2.3.2. Diplomatic-ID

MFA verifies the identity of the Subscriber upon the issuance of Diplomatic-ID via physical presence checks in accordance with the IDA [7].

MFA submits identification data to Idemia. Idemia forwards the data for the Certificate to SK.

Idemia and SK rely on the identification data provided by MFA.

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

The right of representation of the Subscriber's representative is checked in accordance with the IDA [7].

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 3.2.3 of this CPS.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to clause 3.2.3 of this CPS.

3.4. Identification and Authentication for Revocation Request

Refer to clauses 4.9.3.1 and 4.9.3.2 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. ID-card and Digi-ID

The Subscriber submits an application for ID-card or Digi-ID to PBGB.

PBGB verifies the eligibility for the Subscriber to request ID-card or Digi-ID in accordance with the IDA [7].

PBGB is communicating with SK only through Idemia. SK accepts Certificate requests only from Idemia.

4.1.1.2. Diplomatic-ID

Foreign representation or international organisation submits an application for Diplomatic-ID to MFA.

MFA verifies the eligibility for the Subscriber to request Diplomatic-ID in accordance with the IDA [7].

MFA is communicating with SK only through Idemia. SK accepts Certificate requests only from Idemia.

4.1.2. Enrolment Process and Responsibilities

4.1.2.1. ID-card

The Subscriber fills and signs the application for ID-card at PBGB Customer Service Point. Upon signing the application for ID-card, the Subscriber confirms correctness of the information presented to PBGB and that he/she has read and agrees with the Terms and Conditions [10].

PBGB verifies the eligibility for the Subscriber to request ID-card in accordance with the IDA [7]. In case of positive decision, PBGB cryptographically signs data set containing the Subscriber's identification data and forms the order for a new card. PBGB forwards the data set and the order for the card over data exchange layer X-Road to Idemia. Idemia checks the data in the data set and notifies PBGB of accepting the order for a new card.

Idemia manufactures the card, imprints visual elements to it, fills out Personal Data File on the card and generates keypairs for the Authentication and Qualified Electronic Signature Certificate. Idemia encrypts Public Keys originating from the chip of the card with a dedicated transport key and forwards the request for the Certificates and data set previously signed by PBGB over a secure communication channel to SK. After receiving the request for the Certificates, SK decrypts Public Keys originating from the chip of the card with the dedicated transport key used by Idemia for encryption and cryptographically verifies PGBG's signature for the data set.

Idemia and SK rely on the identification data provided by PBGB.

SK checks the Subscriber's identification data in the Certificate request against the Subscriber's identification data in the data set. If there is a match, SK issues Certificates. Certificates are issued in suspended state.

SK forwards the Certificates to Idemia. Idemia loads the Certificates to the ID-card and delivers personalised, but unusable ID-card to PBGB.

4.1.2.2. Digi-ID

The Subscriber fills and signs the application for Digi-ID at PBGB Customer Service Point. Upon signing the application for Digi-ID, the Subscriber confirms correctness of the information presented to PBGB and that he/she has read and agrees with the Terms and Conditions [10].

PBGB verifies the eligibility for the Subscriber to request Digi-ID in accordance with the IDA [7]. PBGB verifies that Digi-ID is issued to the Subscriber who has been issued an ID-card or who is applying for an ID-card concurrently with Digi-ID.

In case of positive decision, PBGB cryptographically signs data set containing the Subscriber's identification data and forms the order for a new card. PBGB forwards the data set and the order for the card over data exchange layer X-Road to Idemia. Idemia checks the data in the data set and notifies PBGB of accepting the order for a new card.

Idemia manufactures the card and PBGB imprints visual elements to it, fills out Personal Data File on the card and generates keypairs for the Authentication and Qualified Electronic Signature Certificate. Idemia encrypts Public Keys originating from the chip of the card with a dedicated transport key and forwards the request for the Certificates and data set previously signed by PBGB over a secure communication channel to SK. After receiving the request for the Certificates, SK decrypts Public Keys originating from the chip of the card with the dedicated transport key used by Idemia for encryption and cryptographically verifies PGBG's signature for the data set.

Idemia and SK rely on the identification data provided by PBGB.

SK checks the Subscriber's identification data in the Certificate request against the Subscriber's identification data in the data set. If there is a match, SK issues Certificates. Certificates are issued in suspended state.

SK forwards the Certificates to Idemia. Idemia forwards the Certificates to PBGB and PBGB loads the Certificates to the Digi-ID.

4.1.2.3. Diplomatic-ID

Foreign representation or international organisation submits an application for Diplomatic-ID on behalf of the Subscriber to MFA Customer Service Point. Upon signing the application for Diplomatic-ID, the Subscriber confirms correctness of the information presented to MFA and that he/she has read and agrees with the Terms and Conditions [10].

MFA verifies the eligibility for the Subscriber to request Diplomatic-ID in accordance with the IDA [7]. In case of positive decision, MFA cryptographically signs data set containing the Subscriber's identification data and forms the order for a new card. MFA forwards the data set and the order for the card over data exchange layer X-Road to Idemia. Idemia checks the data in the data set and notifies MFA of accepting the order for a new card.

Idemia manufactures the card, imprints visual elements to it, fills out Personal Data File on the card and generates keypairs for the Authentication and Qualified Electronic Signature Certificate. Idemia encrypts Public Keys originating from the chip of the card with a dedicated transport key and forwards the request for the Certificates and data set previously signed by MFA over a secure communication channel to SK. After receiving the request for the Certificates, SK decrypts Public Keys originating from the chip of the card with the dedicated transport key used by Idemia for encryption and cryptographically verifies MFA's signature for the data set.

Idemia and SK rely on the identification data provided by MFA.

SK checks the Subscriber's identification data in the Certificate request against the Subscriber's identification data in the data set. If there is a match, SK issues Certificates. Certificates are issued in suspended state.

SK forwards the Certificates to Idemia. Idemia loads the Certificates to the Diplomatic-ID and delivers personalised, but unusable Diplomatic-ID to MFA.

4.1.3. Annual Control of QSCD

Refer to clause 4.1.3 of SK PS [2].

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. ID-card and Digi-ID

PBGB validates the Subscriber's identity as described in Chapters 3 and 5^2 of IDA [7].

PBGB forms the order for a new card and forwards it to Idemia.

PBGB sends the Certificate requests to SK via Idemia.

Idemia forwards the requests for the ID-card and Digi-ID Certificates to SK over secure communication channel.

SK accepts Certificate requests only from Idemia.

Idemia and SK rely on the identification data provided by PBGB.

4.2.1.2. Diplomatic-ID

MFA validates the Subscriber's identity as described in Chapter 5^3 of IDA [7].

MFA forms the order for a new card and forwards it to Idemia.

MFA sends the Certificate requests to SK via Idemia.

Idemia forwards the requests for the Certificates to SK over secure communication channel.

SK accepts Certificate requests only from Idemia.

Idemia and SK rely on the identification data provided by MFA.

4.2.2. Approval or Rejection of Certificate Applications

Refer to clause 4.2.2 of the CP [4].

The acceptance or rejection of an application for the ID-card and Digi-ID is decided by PBGB.

The acceptance or rejection for an application for the Diplomatic-ID is decided by MFA.

SK notifies Idemia of the refusal to issue a Certificate.

4.2.3. Time to Process Certificate Applications

Refer to clause 4.2.3 of the CP [4].

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

After verifying that the Subscriber's identification data in the Certificate request matches with the identification data in the data set, SK automatically issues the corresponding Certificates.

Certificates are loaded to the ID-card and Diplomatic-ID at Idemia or to the Digi-ID in PBGB.

All issued Certificates are in suspended state. Suspension is terminated only after the Subscriber has accepted the Certificates.

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

4.3.2.1. ID-card and Digi-ID

The Subscriber is notified by PBGB of the issuance of the ID-card or Digi-ID to which Certificates have been previously loaded. The ID-card and Digi-ID are issued to the Subscriber in PBGB Customer Service Point and secure PIN envelope containing PIN codes for ID-card or Digi-ID is handed over to the Subscriber.

4.3.2.2. Diplomatic-ID

The Subscriber is notified by MFA of the issuance of the Diplomatic-ID to which Certificates have been previously loaded. The Diplomatic-ID is issued to the Subscriber in MFA Customer Service Point and secure PIN envelope containing PIN codes for Diplomatic-ID is handed over to the Subscriber.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

4.4.1.1. ID-card and Digi-ID

During the issuance of the ID-card or Digi-ID, the Subscriber signs the file of the ID-card or Digi-ID issuance. Corresponding file includes confirmation that the ID-card or Digi-ID has been handed over to him/her.

The employee of PBGB Customer Service Point notifies SK that the ID-card or Digi-ID has been handed over to the Subscriber and SK terminates suspension of the Certificates.

SK notifies the employee of PBGB Customer Service Point about termination of suspension of the Certificates.

Signing the file of the ID-card or Digi-ID issuance as well as confirmation that the ID-card or Digi-ID has been handed over to the Subscriber are deemed Certificate acceptance.

4.4.1.2. Diplomatic-ID

During the issuance of the Diplomatic-ID, the Subscriber signs the file of the Diplomatic-ID issuance. Corresponding file includes confirmation that the Diplomatic-ID has been handed over to him/her.

The employee of MFA Customer Service Point notifies SK that the Diplomatic-ID has been handed over to the Subscriber and SK terminates suspension of the Certificates.

SK notifies the employee of MFA Customer Service Point about termination of suspension of the Certificates.

Signing the file of the Diplomatic-ID issuance as well as confirmation that the Diplomatic-ID has been handed over to the Subscriber are deemed Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

Certificates are published by SK in the Directory Service at ldaps://esteid.ldap.sk.ee immediately after the Subscriber has accepted it.

Suspended and revoked Certificates are deleted from the Directory Service.

In case of termination of suspension of Certificates, Certificates are re-published in the Directory Service.

Expired Certificates are deleted from the Directory Service on the next day following the expiration.

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

SK delivers issued Certificates immediately to Idemia for loading to the cards.

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 [4]
- This CPS
- The Terms and Conditions [10]

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 [4]
- This CPS
- The Terms and Conditions [10]

4.6. Certificate Renewal

Issuing replacement ID-card, Digi-ID or Diplomatic-ID after its expiration is considered re-keying due to the fact that the old Private Keys cannot be copied to the new QSCD.

4.7. Certificate Re-Key

If the Subscriber applies recurring ID-card, Digi-ID or Diplomatic-ID, this request is processed as an application for a new ID-card, Digi-ID or Diplomatic-ID.

During Certificate re-key, all the erroneous or unusable Certificates to be replaced are revoked.

Please note: Clause 4.7 of the CP [4] allows Certificate re-key to be performed remotely by stating that the Subscriber can also be digitally authenticated. Corresponding clause of this CPS does not follow referred requirement of the CP [4].

SK has coordinated respective non-conformance with the holder of the CP [4], i.e. PBGB.

4.7.1. Circumstances for Certificate Re-Key

Certificate re-key is allowed to:

- Replace an expired or broken ID-card, Digi-ID or Diplomatic-ID
- Fix production errors of ID-card, Digi-ID or Diplomatic-ID

If the Subscriber applies Certificate re-key to replace broken ID-card or Digi-ID, the Subscriber submits a warranty claim that is treated as a new application for ID-card or Digi-ID. In case of broken Diplomatic-ID, the Subscriber submits a new application for Diplomatic-ID to be replaced.

Certificate re-key to replace broken ID-card, Digi-ID or Diplomatic-ID or to fix production errors is performed based on initial application for ID-card, Digi-ID or Diplomatic-ID.

Please note: Clause 4.7.1 of the CP [4] allows Certificate re-key to be performed remotely by stating that the Subscriber can also be digitally authenticated. Corresponding clause of this CPS does not follow referred requirement of the CP [4].

Clause 4.7.3 of the CP [4] states that in case of replacement of broken ID-card, Digi-ID or Diplomatic-ID, the warranty claim is treated as the application for the Certificates and re-key is done upon initial Certificate application. This clause of the CPS is partially not compliant with respective clause of the CP [4] as in case of replacement of broken Diplomatic-ID, warranty claim is not submitted.

SK has coordinated respective non-conformances with the holder of the CP [4], i.e. PBGB.

4.7.2. Who May Request Certification of a New Public Key

Certificate re-key process to fix production errors of ID-card or Diplomatic-ID can only be initiated by Idemia.

Certificate re-key process to fix production errors of Digi-ID can only be initiated by PBGB.

Certificate re-key process to replace broken ID-card, Digi-ID or Diplomatic-ID can only be initiated by the Subscriber.

All the Certification requests are delivered to SK through Idemia.

Please note: Clause 4.7.2 of the CP [4] allows both the Subscriber and PBGB to request Certificate re-key to replace broken ID-card or Digi-ID. Additionally, clause 4.7.2 of the CP [4] allows the Subscriber and MFA to request Certificate re-key to replace broken Diplomatic-ID.

This clause of the CPS is partially not compliant with respective clause of the CP [4] as only the Subscriber initiates re-key process to replace broken ID-card, Digi-ID or Diplomatic-ID.

Clause 4.7.2 of the CP [4] states that SK shall not accept re-key requests from any other party than PBGB or the Card Manufacturer signed by either PBGB or MFA. This clause of the CPS is partially not compliant with respective clause of the CP [4] as SK receives certification requests only from the Card Manufacturer, i.e. Idemia.

SK has coordinated respective non-conformances with the holder of the CP [4], i.e. PBGB.

4.7.3. Processing Certificate Re-Keying Request

After Idemia has discovered ID-card or Diplomatic-ID production errors during quality checks, Idemia submits a new request for the Certificates to SK.

After PBGB has discovered Digi-ID production errors during quality checks, PBGB submits a new request for the Certificates to SK through Idemia.

If the repeated request has no changed data in it, the already issued Certificate is retransmitted. The rest of the process is similar to initial ID-card, Digi-ID or Diplomatic-ID issuance.

If the Certificate re-key is to replace an expired or broken ID-card, Digi-ID or Diplomatic-ID, the process is similar to initial issuance.

During Certificate re-key, only the last Certificates are written to the card or Digi-ID media and remain valid.

The validity period of the issued Certificates does not exceed the validity period of the underlying document.

SK immediately revokes the Certificates that have been replaced.

4.7.4. Notification of New Certificate Issuance to Subscriber

Refer to clause 4.3.2 of this CPS.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to clause 4.4.1 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

Not applicable.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1 of the CP [4].

In addition to the circumstances in clause 4.9.1 of the CP [4] and more precisely, SK has the right to revoke the Certificate if one or more of the following occurs:

- The Subscriber requests revocation via RA
- SK obtains evidence that the Subscriber has lost control over Private Keys or PIN codes
- SK obtains evidence that the Subscriber's original Certificate request was not authorised and the Subscriber does not retroactively grant authorisation
- SK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements
- SK obtains evidence that the Certificate was misused
- SK obtains evidence that the used cryptography is no longer ensuring the binding between the Subject and the Public Key
- SK is made aware that the Subscriber has violated one or more of their obligations under the Terms and Conditions [5]
- SK is made aware of a material change in the information contained in the Certificate
- SK is made aware that the Certificate was not issued in accordance with the CP [4] and/or CPS
- SK determines that any of the information appearing in the Certificate is inaccurate or misleading
- SK terminates provisioning of the Certification Service or SK is dissolved
- SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate
- Revocation is required by the CP [4]

- The technical content or format of the Certificate presents an unacceptable risk to Relying Parties
- If such an obligation is foreseen by the law or any legislation established on the basis thereof

Revoked Certificate is not reinstated.

Please note: Clause 4.9.1 of the CP [4] states that circumstances for Certificate revocation are as laid down in IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14]. This clause of the CPS is partially not compliant with respective clause of the CP [4] as it allows revocation to be performed on additional grounds (such as the Subscriber's original Certificate request was not authorised and the Subscriber does not retroactively grant authorisation, the Certificate was not issued in accordance with the CP [4] and/or CPS, the technical content or format of the Certificate presents an unacceptable risk to Relying Parties) not listed in the referred laws.

SK has coordinated respective non-conformance with the holder of the CP [4], i.e. PBGB.

4.9.2. Who Can Request Revocation

PBGB can present an application to revoke the Certificate of ID-card or Digi-ID in accordance with IDA [7].

MFA can present an application to revoke the Certificate of Diplomatic-ID in accordance with IDA [7].

The Subscriber or competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14] can submit an application for revocation of the Certificate.

Idemia can request revocation of the Certificate of ID-card or Diplomatic-ID, if ID-card or Diplomatic-ID fails at quality controls. If Digi-ID fails at quality controls, PBGB can request revocation of the Certificate via Idemia.

4.9.3. Procedure for Revocation Request

4.9.3.1. ID-card and Digi-ID

Certificate revocation is regulated by provisions and procedures of revocation of identity document in IDA [7].

The Subscriber submits a signed application for revocation through PBGB Customer Service Point to SK. The revocation request is registered by an employee of PBGB Customer Service Point.

An employee of PBGB Customer Service Point verifies the person filing an application for revocation in accordance with internal identity verification procedures and establishes the legality to request revocation.

An employee of the PBGB Customer Service Point forwards the request for revocation over secure communication channel to SK.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14], requests revocation of the Certificates, SK verifies the legality of the request and processes it according to the procedure listed below (except verifying the identity of the person requesting revocation).

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

- The compliance of the application for revocation with the CP [4] is verified
- The Certificate is marked as revoked in the certificate database
- The Certificate is immediately removed from the Directory Service and OCSP stops responding with status "GOOD"
- 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

After SK has received an application for revocation, SK processes it immediately.

If revocation is requested by competent authority, the Certificates are revoked given all the reasonable circumstances, no later than on the date indicated in the revocation request or 24 hours after receipt of the request.

The revocation of the Certificate is recorded in the certificate database of SK. The Subscriber has a possibility to verify from the Directory Service, the CRL or via OCSP that the Certificate has been revoked.

Idemia requests revocation of ID-card Certificates by sending revocation request to SK. In case of Digi-ID, PBGB sends revocation request to SK via Idemia. SK revokes the Certificates that have not yet been accepted by the Subscriber.

Revoked Certificate can not be reinstated.

4.9.3.2. Diplomatic-ID

Certificate revocation is regulated by provisions and procedures of revocation of identity document in IDA [7].

Foreign representation or international organisation submits an application for Diplomatic-ID to MFA Customer Service Point.

Alternatively, the Subscriber submits a signed application for revocation to MFA Customer Service Point.

The revocation request is registered by an employee of MFA Customer Service Point.

If the Subscriber requests revocation of the Certificates, MFA Customer Service Point verifies the person filing an application for revocation in accordance with internal identity verification procedures and establishes the legality to request revocation.

If revocation of the Certificates is requested by foreign representation or international organisation, an employee of the MFA Customer Service Point verifies the legality of the request.

An employee of the MFA Customer Service Point forwards the request for revocation over secure communication channel to SK.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14], requests revocation of the Certificates, SK verifies the legality of the request and processes it according to the procedure listed below (except verifying the identity of the person requesting revocation).

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

- The compliance of the application for revocation with the CP [4] is verified
- The Certificate is marked as revoked in the certificate database
- The Certificate is immediately removed from the Directory Service and OCSP stops responding with status "GOOD"
- 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

After SK has received an application for revocation, SK processes it immediately.

If revocation is requested by competent authority, the Certificates are revoked given all the reasonable circumstances, no later than on the date indicated in the revocation request or 24 hours after receipt of the request.

The revocation of the Certificate is recorded in the certificate database of SK. The Subscriber has a possibility to verify from the Directory Service, the CRL or via OCSP that the Certificate has been revoked.

Idemia requests revocation of Diplomatic-ID Certificates by sending revocation request to SK. SK revokes the Certificates that have not yet been accepted by the Subscriber.

Revoked Certificate can not be reinstated.

4.9.4. Revocation Request Grace Period

4.9.4.1. ID-card and Digi-ID

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

4.9.4.2. Diplomatic-ID

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

4.9.5. Time Within Which CA Must Process the Revocation Request

After PBGB, MFA or Idemia has forwarded an application for revocation to SK, SK immediately processes an application for revocation.

SK processes third party's 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.

4.9.6. 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 [10].

4.9.7. CRL Issuance Frequency

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

CRL is signed by ESTEID2018.

4.9.8. Maximum Latency for CRLs

SK monitors 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

OCSP service is free of charge and publicly accessible.

An OCSP service serves as a primary source for the Certificate status information and contains Certificate status information until the Certificate expires.

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 [10].

4.9.11. Other Forms of Revocation Advertisements Available

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

Revocation status information of the expired Certificate can be requested at the email address info@skidsolutions.eu

4.9.12. Special Requirements Related to Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Refer to clause 4.9.13 of the CP [4].

4.9.14. Who Can Request Suspension

Anyone can request Certificate suspension.

4.9.15. Procedure for Suspension Request

4.9.15.1. ID-card and Digi-ID

The suspension request is registered by the Help Line operator or suspension is registered by an employee of the PBGB Customer Service Point.

Suspension request submitted via the Help Line is recorded. The person requesting suspension and the legality to request suspension is verified by using professional skills of the Help Line operator.

Alternatively, the person files a signed application for suspension to an employee of the PBGB Customer Service Point. An employee of PBGB Customer Service Point verifies the person filing an application for suspension in accordance with internal identity verification procedures and establishes the legality to request suspension.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14] requests suspension of the Certificates, SK verifies the legality of the request and processes it according to the procedure listed below (except verifying the identity of the person requesting suspension).

An employee of the Help Line or the PBGB Customer Service Point forwards the request for suspension over secure communication channel to SK.

After SK has received a request for suspension of the Certificate of ID-card or Digi-ID, the procedure for processing the request is the following:

- The compliance of the application for suspension of the Certificate with the CP [4] is verified
- The application for suspension is registered in SK's information system
- The Certificate is suspended by SK
- The Certificate is marked as suspended in the certificate database and if suspension is requested by competent authority, the Certificate is tagged accordingly in SK's internal database to distinguish it later from other suspended Certificates
- The Certificate is immediately removed from the Directory Service and OCSP stops responding with status "GOOD"
- A new CRL is published according to clause 4.9.7 of this CPS
- The documentation on which the application for suspension was based is archived

After SK has received an application for suspension via the Help Line, SK processes it immediately.

If suspension is requested by competent authority, the Certificates are suspended given all the reasonable circumstances, no later than on the date indicated in the suspension request or 24 hours after receipt of the request.

If the Certificates have been suspended at the request of competent authority and suspension is later requested by the Subscriber, the Certificates are revoked. The Subscriber is informed by the Help Line operator about the situation. A request for revocation is sent to PBGB who processes it according to clause 4.9.3.1 of this CPS. Revocation does not happen immediately. The tag about special treatment is removed from the database.

In case the request for Certificate suspension was submitted via the Help Line, the Subscriber is immediately notified of the successful Certificate suspension after completion of the suspension procedure. The Subscriber has a possibility to verify on the basis of the Directory Service, the CRL or via OCSP that the Certificate has been suspended.

The Subscriber can apply for suspension of the Certificates via the Help Line 24 hours a day, 7 days a week.

4.9.15.2. Diplomatic-ID

The suspension request is registered by the Help Line operator or suspension is registered by an employee of the MFA Customer Service Point.

Suspension request submitted via the Help Line is recorded. The person requesting suspension and the legality to request suspension is verified by using professional skills of the Help Line operator.

Alternatively, the person files a signed application for suspension to an employee of the MFA Customer Service Point. An employee of MFA Customer Service Point verifies the person filing an application for suspension in accordance with internal identity verification procedures and establishes the legality to request suspension.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14] requests suspension of the Certificates, SK verifies the legality of the request and processes it according to the procedure listed below (except verifying the identity of the person requesting suspension).

An employee of the Help Line or the MFA Customer Service Point forwards the request for suspension over secure communication channel to SK.

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

- The compliance of the application for suspension of the Certificate with the CP [4] is verified
- The application for suspension is registered in SK's information system
- The Certificate is suspended by SK

- The Certificate is marked as suspended in the certificate database and if suspension is requested by competent authority, the Certificate is tagged accordingly in SK's internal database to distinguish it later from other suspended Certificates
- The Certificate is immediately removed from the Directory Service and OCSP stops responding with status "GOOD"
- A new CRL is published according to clause 4.9.7 of this CPS
- The documentation on which the application for suspension was based is archived

After SK has received an application for suspension via the Help Line, SK processes it immediately.

If suspension is requested by competent authority, the Certificates are suspended given all the reasonable circumstances, no later than on the date indicated in the suspension request or 24 hours after receipt of the request.

If the Certificates have been suspended at the request of competent authority and suspension is later requested by the Subscriber, the Certificates are revoked. The Subscriber is informed by the Help Line operator about the situation. A request for revocation is sent to MFA who processes it according to clause 4.9.3.1 of this CPS. Revocation does not happen immediately. The tag about special treatment is removed from the database.

In case the request for Certificate suspension was submitted via the Help Line, the Subscriber is immediately notified of the successful Certificate suspension after completion of the suspension procedure. The Subscriber has a possibility to verify on the basis of the Directory Service, the CRL or via OCSP that the Certificate has been suspended.

The Subscriber can apply for suspension of the Certificates via the Help Line 24 hours a day, 7 days a week.

4.9.16. Limits on Suspension Period

There are no limits on the suspension period.

4.9.17. Circumstances for Termination of Suspension

Refer to clause 4.9.17 of the CP [4].

4.9.18. Who Can Request Termination of Suspension

Refer to clause 4.9.18 of the CP [4].

4.9.19. Procedure for Termination of Suspension

4.9.19.1. ID-card and Digi-ID

The person files a signed application for termination of suspension to an employee of the PBGB Customer Service Point. The termination of suspension application is registered by an employee of the Customer Service Point of PBGB.

An employee of the PBGB Customer Service Point verifies the person filing an application for termination of suspension in accordance with internal identity verification procedures and establishes the legality to request termination of suspension.

An application for termination of suspension is forwarded to SK over secure communication channel by an employee of the PBGB Customer Service Point.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14] has requested suspension of the Certificates, they can request termination of suspension.

SK verifies legality of the request and that the Certificates noted in the request are tagged as suspended in SK's internal database. If SK has confirmed that the Certificates have been tagged accordingly, SK processes the request for termination of suspension as listed below (except verifying the identity of the person requesting termination of suspension).

After SK has received an application for termination of suspension of the Certificate of ID-card or Digi-ID, the procedure for processing the application is the following:

- The compliance of the application for termination of suspension of the Certificate with the CP [4] is verified
- If termination of suspension is requested by competent authority, SK verifies that competent authority requests termination of suspension for the Certificates it has previously requested to be suspended
- The application for termination of suspension is registered in SK's information system
- Suspension of the Certificate is terminated by SK
- After suspension of the Certificate is terminated, it is immediately published again in the Directory Service and OCSP starts responding with status "GOOD"
- A new CRL is published according to clause 4.9.7 of this CPS
- The documentation on which the application for termination of suspension was based is archived

After SK has received an application for termination of suspension, SK processes it immediately.

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 the Directory Service, the next CRL or via OCSP that suspension of the Certificate has been terminated. If the Subscriber requests termination of suspension that has been previously requested by competent authority, suspension is not terminated by SK.

If termination of suspension is requested by competent authority, suspension of the Certificate is terminated given all the reasonable circumstances, no later than on the date indicated in the request or 24 hours after receipt of the request.

4.9.19.2. Diplomatic-ID

The person files a signed application for termination of suspension to an employee of the MFA Customer Service Point. The termination of suspension application is registered by an employee of the Customer Service Point of MFA.

An employee of the MFA Customer Service Point verifies the person filing an application for termination of suspension in accordance with internal identity verification procedures and establishes the legality to request termination of suspension.

An application for termination of suspension is forwarded to SK over secure communication channel by an employee of the MFA Customer Service Point.

If competent authority within the meaning of IDA [7] and Electronic Identification and Trust Services for Electronic Transactions Act [14] has requested suspension of the Certificates, they can request termination of suspension.

SK verifies legality of the request and that the Certificates noted in the request are tagged as suspended in SK's internal database. If SK has confirmed that the Certificates have been tagged accordingly, SK processes the request for termination of suspension as listed below (except verifying the identity of the person requesting termination of suspension).

After SK has received an application for termination of suspension of the Certificate of Diplomatic-ID, the procedure for processing the application is the following:

- The compliance of the application for termination of suspension of the Certificate with the CP [4] is verified
- If termination of suspension is requested by competent authority, SK verifies that competent authority requests termination of suspension for the Certificates it has previously requested to be suspended
- The application for termination of suspension is registered in SK's information system
- Suspension of the Certificate is terminated by SK
- After suspension of the Certificate is terminated, it is immediately published again in the Directory Service and OCSP starts responding with status "GOOD"
- A new CRL is published according to clause 4.9.7 of this CPS
- The documentation on which the application for termination of suspension was based is archived

After SK has received an application for termination of suspension, SK processes it immediately.

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 the Directory Service, the next CRL or via OCSP that suspension of the Certificate has been terminated. If the Subscriber requests termination of suspension that has been previously requested by competent authority, suspension is not terminated by SK.

If termination of suspension is requested by competent authority, suspension of the Certificate is terminated given all the reasonable circumstances, no later than on the date indicated in the request or 24 hours after receipt of the request.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

SK offers CRL and OCSP services for checking certificate status. Service is accessible over HTTP protocol.

The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile [3].

4.10.2. Service Availability

SK ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.44% availability overall per year with a scheduled downtime that does not exceed 0.28% annually.

4.10.3. Operational Features

None.

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.

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 [2].

5.2. Procedural Controls

Refer to clause 5.2 of SK PS [2].

5.3. Personnel Controls

Refer to clause 5.3 of SK PS [2].

5.4. Audit Logging Procedures

Refer to clause 5.4 of SK PS [2].

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 [2].

All physical records about the replacement PIN envelope issuance, 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 [2].

5.5.3. Protection of Archive

Refer to clause 5.5.3 of SK PS [2].

5.5.4. Archive Backup Procedures

Refer to clause 5.5.4 of SK PS [2].

5.5.5. Requirements for Time-Stamping of Records

Refer to clause 5.5.5 of SK PS [2].

5.5.6. Archive Collection System (Internal or External)

Refer to clause 5.5.6 of SK PS [2].

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 [2].

5.6. Key Changeover

The Public Key of the CA does not change. The Public Key for the OCSP responder is sent inside the OCSP response, through which a change of key is known.

If necessary, details of a key changeover are considered each time. Common name of the CA always contains the number of the year which it was issued (e.g. ESTEID-SK 2011).

5.7. Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [2].

5.8. CA or RA Termination

Refer to clause 5.8 of SK PS [2].

6. Technical Security Controls

This CPS describes the Subscriber's key pair generation and management. Root CA's and intermediate CA's key pair generation and management is described in chapter 6 of SK PS [2].

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Refer to clause 6.1 of SK PS [2].

6.1.1.1. ID-card and Diplomatic-ID

The Subscriber Private Keys are generated during personalisation on the QSCD, i.e. in the chip of the ID-card or Diplomatic-ID by Idemia. 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. Digi-ID

The Subscriber Private Keys are generated during personalisation on the QSCD, i.e. in the chip of the Digi-ID in the RA office. 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.

6.1.2. Private Key Delivery to Subscriber

The Subscriber Private Keys are delivered on the QSCD, i.e. in the chip of the card.

Prior to the issuance of the card and delivery to the Subscriber, confidentiality and non-usage of the generated Private Keys and PIN codes is warranted by respective parties involved in handling the cards.

The confidentiality and non-usage of the generated Private Keys and PIN codes is also warranted by the suspended state of the ID-card, Digi-ID and Diplomatic-ID Certificates.

6.1.3. Public Key Delivery to Certificate Issuer

Idemia encrypts Public Keys originating from the chip of the card with a dedicated transport key and forwards the Public Keys to be certified over a secure communication channel to SK.

6.1.4. CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [2].

6.1.5. Key Sizes

Refer to the Certificate Profile [3].

6.1.6. Public Key Parameters Generation and Quality Checking

The quality of Public Keys is guaranteed by using secure random number generators built into the smartcard or HSM-s. User-generated keys are not accepted. Before issuing a Certificate, key is checked for duplicates and some basic analytic checks are applied. 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 [2].

Refer to the Certificate Profile [3].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Refer to clause 6.2.1 of SK PS [2].

The chips used to store Subscriber Private keys are QSCD according to eIDAS Regulation [8].

Keys are generated by a FIPS 140-2 (Level 3) certified device or higher certified security module.

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

Refer to clause 6.2.2 of SK PS [2].

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

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [2].

SK does not offer Key Escrow services to Subscribers.

6.2.4. Private Key Backup

Refer to clause 6.2.4 of SK PS [2].

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

6.2.5. Private Key Archival

Refer to clause 6.2.5 of SK PS [2].

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

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Refer to clause 6.2.6 of SK PS [2].

The Subscriber Private Keys are generated inside the card.

6.2.7. Private Key Storage on Cryptographic Module

Refer to clause 6.2.7 of SK PS [2].

Private Keys of the Subscriber are stored on the chip of the ID-card, Digi-ID or Diplomatic-ID.

6.2.8. Method of Activating Private Key

Refer to clause 6.2.8 of SK PS [2].

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

- There is a separate PIN for each Private Key corresponding to a Certificate with unique Distinguished Name (i.e. there are separate PIN-s for Authentication Key and Signature Key)
- The Subscriber must enter the activation code of the Authentication Certificate (PIN1) at least once after ID-card, Digi-ID or Diplomatic-ID 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 code is blocked after 3 consecutive incorrect tries
- PIN code can be unblocked using a PUK code
- The usage of PUK code is blocked after 3 consecutive incorrect tries
- The Subscriber can change the PIN and PUK codes

The length of the PIN codes is limited to:

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

If the PUK code of ID-card or Digi-ID is lost or blocked, the Subscriber can apply for replacement codes in PBGB Customer Service Point.

In case of Diplomatic-ID, the Subscriber can apply for replacement codes in MFA Customer Service Point.

6.2.9. Method of Deactivating Private Key

Refer to clause 6.2.9 of SK PS [2].

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

6.2.10. Method of Destroying Private Key

Refer to clause 6.2.9 of SK PS [2].

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

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS.

ID-cards, Digi-ID cards and Diplomatic-ID cards are QSCD according to eIDAS [8].

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to clause 6.3.1 of SK PS [2].

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 [2].

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

Refer to clause 6.4.1 of SK PS [2].

6.4.1.1. ID-card and Digi-ID

PIN codes are generated by Idemia in its system and after generation, printed on the security envelope. Idemia enters PIN codes on the card and associates the card with the envelope containing the referred PIN codes. Thereafter, PIN codes are deleted from Idemia's system.

Security envelope containing PIN codes is handed over to the Subscriber unopened. Copies of the codes are not stored by Idemia.

PIN 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 PIN codes with altered security element.

The replacement PIN envelopes are anonymous before issuance in the PBGB Customer Service Point. During issuance an employee of the PBGB Customer Service Point enters the number of

the envelope to the system and the card is programmed with the corresponding codes without exposing them to an employee of the PBGB Customer Service Point.

RA issues replacement PIN codes to the Subscriber when they need to be replaced or updated.

All PIN codes of a single ID-card or Digi-ID are replaced at once.

Prior to issuing replacement PIN codes RA performs Subscriber Authentication

6.4.1.2. Diplomatic-ID

PIN codes are generated by Idemia in its system and after generation, printed on the security envelope. Idemia enters PIN codes on the card and associates the card with the envelope containing the referred PIN codes. Thereafter, PIN codes are deleted from Idemia's system.

Security envelope containing PIN codes is handed over to the Subscriber unopened. Copies of the PIN codes are not stored by Idemia.

PIN 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 PIN codes with altered security element.

The replacement PIN envelopes are anonymous before issuance in the MFA Customer Service Point. During issuance an employee of the MFA Customer Service Point enters the number of the envelope to the system and the card is programmed with the corresponding codes without exposing them to an employee of the MFA Customer Service Point.

An employee of the MFA Customer Service Point issues replacement PIN codes to the Subscriber when they need to be replaced or updated.

All PIN codes of a single Diplomatic-ID are replaced at once.

Prior to issuing replacement PIN codes RA performs Subscriber Authentication.

6.4.2. Activation Data Protection

Refer to clause 6.4.2 of SK PS [2] and 6.4.1 of this CPS .

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 [2].

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 [2].

Subscriber is responsible for applying reasonable protections on her device.

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [2].

Subscriber is responsible for applying reasonable protections on her device.

6.7. Network Security Controls

Refer to clause 6.7 of SK PS [2].

Subscriber is responsible for applying reasonable protections on her device.

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [2].

Not applicable to Subscribers.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

Certificate profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/

7.2. CRL Profile

The CRL profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/

7.3. OCSP Profile

The OCSP profile is described in the Certificate Profile [3], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/

8. Compliance Audit and Other Assessments

Refer to chapter 8 of SK PS [2].

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

9.1.1.1. ID card and Digi-ID

The Subscriber pays fee for the review of an application for the issuance of the ID-card and Digi-ID according to the rate provided for in the State Fees Act [11]. Corresponding fee includes fee for the Certificate issuance.

The fee for the certificate issuance is considered business secret between SK and Idemia.

Certificate renewal is not performed.

9.1.1.2. Diplomatic-ID

The fee for the certificate issuance is considered business secret between SK and Idemia.

Certificate renewal is not performed.

9.1.2. Certificate Access Fees

Valid and activated Certificates are available via OCSP service and in the Directory Service.

The Directory Service is free of charge and accessible at ldaps://esteid.ldap.sk.ee.

9.1.3. Revocation or Status Information Access Fees

Revocation of the Certificate of the ID-card, Digi-ID and Diplomatic-ID is free of charge.

A valid CRL is free of charge and is accessible on SK's website https://www.skidsolutions.eu/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.

9.1.5. Refund Policy

The Subscriber is entitled to apply for the refund of the state fee for the review of an application for the issuance of the ID-card and Digi-ID in accordance with the State Fees Act [11].

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Refer to clause 9.2.1 of SK PS [2].

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 [2].

9.3. Confidentiality of Business Information

Refer to clause 9.3 of SK PS [2].

9.4. Privacy of Personal Information

Refer to clause 9.4 of SK PS [2].

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

Refer to clause 9.6.1 of SK PS [2].

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 [4]
- It keeps account of the certificates issued by it and of their validity
- It accepts applications for suspension of Certificates 24 hours a day
- 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

Due to ID-card, Digi-ID and Diplomatic-ID Certificates being used for Authentication and creating Qualified Electronic Signatures, usage of the Certificates imply legal capability of the Subscriber.

If the Subscriber has some sort of disability, Customer Service Point of PBGB and MFA as well as the Help Line assist with applying for and usage of the Certificates. Assistance to the Subscriber is also provided with suspension, termination of suspension and revocation of the Certificates.

9.6.2. RA Representations and Warranties

9.6.2.1. ID-card and Digi-ID

9.6.2.1.1 PBGB Customer Service Point

Refer to clause 9.6.2 of SK PS [2].

PBGB Customer Service Point ensures that:

- It notifies SK that ID-card or Digi-ID has been handed over to the Subscriber for SK to terminate suspension of the Certificates loaded thereon;
- It issues ID-card and Digi-ID to Subscribers;
- It accepts Subscriber applications for ID-card and Digi-ID Certificate creations, suspensions, terminations of suspension and revocations
- It accepts reasoned applications from the Subscriber for designation of replacement PIN codes
- It checks the correctness and completeness of the listed applications
- It identifies and verifies the Subscriber submitting any of the listed applications
- It provides security with its internal security procedures

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

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

If the Subscriber has some sort of disability, PBGB Customer Service Point provides all-around assistance to the Subscriber with applying for and servicing of the Certificates.

9.6.2.2. Diplomatic-ID

9.6.2.2.1 MFA Customer Service Point

Refer to clause 9.6.2 of SK PS [2].

MFA Customer Service Point ensures that:

- It notifies SK that Diplomatic-ID has been handed over to the Subscriber for SK to terminate suspension of the Certificates loaded thereon
- It issues Diplomatic-ID to Subscribers
- It accepts Subscriber applications for Diplomatic-ID Certificate creations, suspensions, terminations of suspension and revocations
- It accepts reasoned applications from the Subscriber for designation of replacement PIN codes
- It checks the correctness and completeness of the listed applications
- It identifies and verifies the Subscriber submitting any of the listed applications

- It provides security with its internal security procedures

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

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

If the Subscriber has some sort of disability, MFA Customer Service Point provides all-around assistance to the Subscriber with applying for and servicing of the Certificates.

9.6.2.3. Help Line

Refer to clause 9.6.2 of SK PS [2].

The Help Line ensures that:

- It accepts applications for the ID-card, Digi-ID and Diplomatic-ID Certificate suspensions
- 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.

If the Subscriber has some sort of disability, the Help Line provides all-around assistance to the Subscriber with applying for and servicing of the Certificates.

9.6.3. Subscriber Representations and Warranties

9.6.3.1. ID-card and Digi-iD

Refer to clause 9.6.3 of SK PS [2].

The Subscriber ensures that:

- He/she adheres to the requirements provided by SK in this CPS
- He/she presents true and correct information to PBGB while presenting an application for the ID-card and Digi-ID
- In case of a change in his/her personal details, he/she immediately notifies PBGB of the correct details in accordance with the established legislation
- He/she uses his/her Private Keys solely for creating Qualified Electronic Signatures
- He/she uses his/her Private Keys and corresponding Certificates solely on a secure cryptographic device handed over to him/her at PBGB Customer Service Point and 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 no longer uses his/her Private Key, in the case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised
- He/she is aware that Qualified Electronic Signatures given on the basis of expired, revoked or suspended Certificates are invalid

If the Subscriber has lost his/her ID-card or Digi-ID, the Subscriber has to suspend the Certificates immediately. There is an option to revoke the Certificates later.

The Subscriber is not responsible for the acts performed using suspended or revoked Certificates.

If the Subscriber finds his/her ID-card or Digi-ID and is certain that his/her Private Keys were not used during the suspension of the Certificates, the Subscriber may terminate suspension of the Certificates. In this case the Subscriber becomes solely and fully responsible for any consequences of Authentication and Qualified Electronic Signature using the Certificates during the time when the Certificates were suspended.

If the Subscriber is unable to verify if his/her Private Keys were used during the time when the ID-card or Digi-ID was lost, the Subscriber is obliged to revoke the Certificates.

The Subscriber is solely responsible for the maintenance of his/her Private Key.

The Subscriber is aware that SK publishes his/her valid Certificates during their validity period via LDAP directory service.

The Subscriber has to accept the Terms and Conditions [10].

9.6.3.2. Diplomatic-ID

Refer to clause 9.6.3 of SK PS [2].

The Subscriber ensures that:

- He/she adheres to the requirements provided by SK in this CPS
- He/she presents true and correct information to MFA while presenting an application for the Diplomatic-ID
- In case of a change in his/her personal details, he/she immediately notifies MFA of the correct details in accordance with the established legislation
- He/she uses his/her Private Keys solely for creating Qualified Electronic Signatures
- He/she uses his/her Private Keys and corresponding Certificates solely on a secure cryptographic device handed over to him/her at MFA Customer Service Point and 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 no longer uses his/her Private Key, in the case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised

- He/she is aware that Qualified Electronic Signatures given on the basis of expired, revoked or suspended Certificates are invalid

If the Subscriber has lost his/her Diplomatic-ID, the Subscriber has to suspend the Certificates immediately. There is an option to revoke the Certificates later.

The Subscriber is not responsible for the acts performed using suspended or revoked Certificates.

If the Subscriber finds his/her Diplomatic-ID and is certain that his/her Private Keys were not used during the suspension of the Certificates, the Subscriber may terminate suspension of the Certificates. In this case the Subscriber becomes solely and fully responsible for any consequences of Authentication and Qualified Electronic Signature using the Certificates during the time when the Certificates were suspended.

If the Subscriber is unable to verify if his/her Private Keys were used during the time when the Diplomatic-ID was lost, the Subscriber is obliged to revoke the Certificates.

The Subscriber is solely responsible for the maintenance of his/her Private Key.

The Subscriber is aware that SK publishes his/her valid Certificates during their validity period via LDAP directory service.

The Subscriber has to accept the Terms and Conditions [10].

9.6.4. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [2].

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 and the CP [4].

If not enough evidence is enclosed to the Certificate or Qualified 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 [4].

A Relying Party uses CRL service on its own responsibility.

9.6.5. Representations and Warranties of Other Participants

9.6.5.1. Idemia

An employee of Idemia is not punished for an intentional crime.

Idemia provides security with its internal security procedures.

9.7. Disclaimers of Warranties

Refer to clause 9.7 of SK PS [2].

9.8. Limitations of Liability

Refer to clause 9.8 of SK PS [2].

9.9. Indemnities

Indemnities between the Subscriber and SK are regulated in Terms and Conditions [10].

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 [2].

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 with a right to get familiarised with the Terms and Conditions [10], before agreeing to and signing it.

The Subscriber's individual notices are communicated via the Subscriber's email address in the certificate for Authentication.

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 [2].

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 [2].

Additionally, SK ensures compliance with the following requirements:

- IDA [7]
- State Fees Act [11]
- General Data Protection Regulation [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 [2].

9.17. Other Provisions

Not applicable.

10. References

1. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
2. SK ID Solutions AS Trust Services Practice Statement, published: https://www.skidsolutions.eu/en/repository/sk-ps/;
3. Certificate, CRL and OCSP Profile for ID-1 Format Identity Documents Issued by the Republic of Estonia, published: https://www.skidsolutions.eu/en/repository/profiles/;
4. Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card, published: https://www.id.ee/?lang=en&id=30500;
5. 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;
6. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
7. Identity Documents Act, RT I 1999, 25, 365, published: https://www.riigiteataja.ee/en/eli/ee/511042016001/consolide/current;
8. 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;
9. ISO/IEC 7816, Parts 1-4, published: http://iso.org;
10. Terms and Conditions for Use of Certificates for ID-1 Format Identity Documents of the Republic of Estonia, published: https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/;
11. State Fees Act, RT I, 30.12.2014, 1, published: https://www.riigiteataja.ee/en/eli/ee/511022015002/consolide/current;
12. General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
13. ID card documentation webpage: http://www.id.ee/index.php?id=35772;

14. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current.