SK ID Solutions AS - ESTEID-SK Certification Practice Statement

Version 3.0

1.November 2017

Version History		
Date	**Version**	**Changes**
01.11.2017	3.0	Clauses 4.9.15.1, 4.9.15.2 - added procedure for request of suspension by competent authority; Clause 4.9.15.2 - specified that if suspension is requested by the Subscriber, it applies to Certificate Pairs only; Clauses 4.9.19.1 and 4.9.19.2 - added procedure for request of termination of suspension by competent authority; Clause 4.9.19.2 - specified that if termination of suspension is requested by the Subscriber, it applies to Certificate pairs only.
24.10.2017	2.0	Due to change of SK's business name from AS Sertifitseerimiskeskus to SK ID Solutions AS, name of the CPS has been changed accordingly. Also, former business name has been replaced with the new one in clauses 1, 1.1, 1.2, 1.5.1 and 1.6.2 of this CPS; Clause 1 - removed paragraph which stated that the CPS is a complete redesign of the previous AS Sertifitseerimiskeskus - Certification Practice Statement, ESTEID Card Certification Policy and AS Sertifitseerimiskeskus - Certification Policy of the digital identity card in form of the Mobile-ID; Clause 1.1 - added that SK always ensures compliance with the latest versions of the applicable ETSI standards; updated the figure of certificate chain; Clauses 1.1, 1.3.1, 1.3.2.1, 1.3.2.2, 1.3.5.2 and 1.6.1 - lingual corrections; Clause 1.6.2 - added new acronyms and minor changes; Clause 3.1.1 - left out the value O = ESTEID (MOBIIL-ID E-RESIDENT) as Mobile ID is not issued for E-residents; Added the possibility for the Subscriber to apply for Mobile ID Certificates at PBGB. Therefore, clauses 3.2.3.2, 4.1.2.3 and 4.2.1.2 of this CPS have been amended accordingly; Amended the procedure of Certificate re-key for Mobile ID with the possibility for the Subscriber to sign an agreement with MO either with a Qualified Electronic Signature or handwritten signature. Therefore, clauses 4.7.3.2 and 9.6.2.2.4 of this CPS have been amended accordingly; Clauses 4.7.1.1, 4.7.2.1, 4.7.4.1 and 9.6.2.1.1 - replaced SHA-1 signatures with changeover to stronger cryptography; Clause 6.1.5 - added new key size of ECC algorithm; Clause 9.6.1.2 - added that SK is obligated to verify validity of the QSCD to be replaced and previously issued Certificates; Clause 9.6.3.2 - added that the Subscriber is obligated to confirm to MO that the QSCD to be replaced has been issued to him/her.
1.11.2016	1.0	First public edition.

1. Introduction
    - 1.1. Overview
    - 1.2. Document Name and Identification
    - 1.3. PKI Participants
        - 1.3.1. Certification Authorities
        - 1.3.2. Registration Authorities
            - 1.3.2.1. ID card and Digi-ID
            - 1.3.2.2. Mobile ID
            - 1.3.2.3. Help Line
        - 1.3.3. Subscribers
        - 1.3.4. Relying Parties
        - 1.3.5. Other Participants
            - 1.3.5.1. ID card and Digi-ID
            - 1.3.5.2. Mobile ID
    - 1.4. Certificate Usage
        - 1.4.1. Appropriate Certificate Uses
    - 1.5. Policy Administration
        - 1.5.1. Organization Administering the Document
        - 1.5.2. Contact Person
        - 1.5.3. Person Determining CPS Suitability for the Policy
        - 1.5.4. CPS Approval Procedures

- 1.6. Definitions and Acronyms
  - 1.6.1. Terminology
  - 1.6.2. Acronyms
- 2. Publication and Repository Responsibilities
  - 2.1. Repositories
  - 2.2. Publication of Certification Information
    - 2.2.1. Publication and Notification Policies
    - 2.2.2. Items not Published in the Certification Practice Statement
  - 2.3. Time or Frequency of Publication
    - 2.3.1. Directory Service
  - 2.4. Access Controls on Repositories
- 3. Identification and Authentication
  - 3.1. Naming
    - 3.1.1. Type of Names
    - 3.1.2. Need for Names to be Meaningful
    - 3.1.3. Anonymity or Pseudonymity of Subscribers
    - 3.1.4. Rules for Interpreting Various Name Forms
    - 3.1.5. Uniqueness of Names
    - 3.1.6. Recognition, Authentication, and Role of Trademarks
  - 3.2. Initial Identity Validation
    - 3.2.1. Method to Prove Possession of Private Key
      - 3.2.1.1. ID card and Digi-ID
      - 3.2.1.2. Mobile ID
    - 3.2.2. Authentication of Organization Identity
    - 3.2.3. Authentication of Individual Identity
      - 3.2.3.1. ID card and Digi-ID
      - 3.2.3.2. Mobile ID
    - 3.2.4. Non-Verified Subscriber Information
    - 3.2.5. Validation of Authority
    - 3.2.6. Criteria for Interoperation
  - 3.3. Identification and Authentication for Re-Key Requests
    - 3.3.1. Identification and Authentication for Routine Re-Key
      - 3.3.1.1. ID card and Digi-ID
      - 3.3.1.2. Mobile ID
    - 3.3.2. Identification and Authentication for Re-Key After Revocation
      - 3.3.2.1. ID card and Digi-ID
      - 3.3.2.2. Mobile ID
  - 3.4. Identification and Authentication for Revocation Request
- 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
      - 4.1.1.2. Mobile ID
    - 4.1.2. Enrolment Process and Responsibilities
      - 4.1.2.1. ID card
      - 4.1.2.2. Digi-ID
      - 4.1.2.3. Mobile ID
  - 4.2. Certificate Application Processing
    - 4.2.1. Performing Identification and Authentication Functions
      - 4.2.1.1. ID card and Digi-ID
      - 4.2.1.2. Mobile ID
    - 4.2.2. Approval or Rejection of Certificate Applications
      - 4.2.2.1. ID card
      - 4.2.2.2. Digi-ID
      - 4.2.2.3. Mobile ID
    - 4.2.3. Time to Process Certificate Applications
  - 4.3. Certificate Issuance
    - 4.3.1. CA Actions During Certificate Issuance
      - 4.3.1.1. ID card and Digi-ID
      - 4.3.1.2. Mobile ID
    - 4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate
      - 4.3.2.1. ID card and Digi-ID
      - 4.3.2.2. Mobile ID
  - 4.4. Certificate Acceptance
    - 4.4.1. Conduct Constituting Certificate Acceptance
      - 4.4.1.1. ID card and Digi-ID
      - 4.4.1.2. Mobile ID
    - 4.4.2. Publication of the Certificate by the CA
      - 4.4.2.1. ID card and Digi-ID
      - 4.4.2.2. Mobile ID
    - 4.4.3. Notification of Certificate Issuance by the CA to Other Entities
  - 4.5. Key Pair and Certificate Usage
    - 4.5.1. Subscriber Private Key and Certificate Usage
    - 4.5.2. Relying Party Public Key and Certificate Usage
  - 4.6. Certificate Renewal
  - 4.7. Certificate Re-Key
    - 4.7.1. Circumstances for Certificate Re-Key

4.7.1.1. ID card and Digi-ID
4.7.1.2. Mobile ID
4.7.2. Who May Request Certification of a New Public Key
4.7.2.1. ID card and Digi-ID
4.7.2.2. Mobile ID
4.7.3. Processing Certificate Re-Keying Requests
4.7.3.1. ID card and Digi-ID
4.7.3.2. Mobile-ID
4.7.4. Notification of New Certificate Issuance to Subscriber
4.7.4.1. ID card and Digi-ID
4.7.4.2. Mobile ID
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate
4.7.5.1. ID card and Digi-ID
4.7.5.2. Mobile ID
4.7.6. Publication of the Re-Keyed Certificate by the CA
4.7.7. Notification of Certificate Issuance by the CA to Other Entities
4.8. Certificate Modification
4.8.1. Circumstances for Certificate Modification
4.8.1.1. ID card and Digi-ID
4.8.1.2. Mobile ID
4.8.2. Who May Request Certificate Modification
4.8.2.1. ID card and Digi-ID
4.8.2.2. Mobile ID
4.8.3. Processing Certificate Modification Requests
4.8.3.1. ID card and Digi-ID
4.8.3.2. Mobile ID
4.8.4. Notification of New Certificate Issuance to Subscriber
4.8.5. Conduct Constituting Acceptance of Modified Certificate
4.8.6. Publication of the Modified Certificate by the CA
4.8.7. Notification of Certificate Issuance by the CA to Other Entities
4.9. Certificate Revocation and Suspension
4.9.1. Circumstances for Revocation
4.9.2. Who Can Request Revocation
4.9.2.1. ID card and Digi-ID
4.9.2.2. Mobile ID
4.9.3. Procedure for Revocation Request
4.9.3.1. ID card and Digi-ID
4.9.3.2. Mobile ID
4.9.4. Revocation Request Grace Period
4.9.4.1. ID card and Digi-ID
4.9.4.2. Mobile ID
4.9.5. Time Within Which CA Must Process the Revocation Request
4.9.6. Revocation Checking Requirements for Relying Parties
4.9.7. CRL Issuance Frequency
4.9.8. Maximum Latency for CRLs
4.9.9. On-Line Revocation/Status Checking Availability
4.9.10. On-Line Revocation Checking Requirements
4.9.11. Other Forms of Revocation Advertisements Available
4.9.12. Special Requirements Related to Key Compromise
4.9.13. Circumstances for Suspension
4.9.14. Who Can Request Suspension
4.9.15. Procedure for Suspension Request
4.9.15.1. ID card and Digi-ID
4.9.15.2. Mobile ID
4.9.16. Limits on Suspension Period
4.9.17. Circumstances for Termination of Suspension
4.9.18. Who Can Request Termination of Suspension
4.9.18.1. ID card and Digi-ID
4.9.18.2. Mobile ID
4.9.19. Procedure for Termination of Suspension
4.9.19.1. ID card and Digi-ID
4.9.19.2. Mobile ID
4.10. Certificate Status Services
4.10.1. Operational Characteristics
4.10.2. Service Availability
4.10.3. Operational Features
4.11. End of Subscription
4.12. Key Escrow and Recovery
4.12.1. Key Escrow and Recovery Policy and Practices
4.12.2. Session Key Encapsulation and Recovery Policy and Practices
5. Facility, Management, and Operational Controls
5.1. Physical Controls
5.2. Procedural Controls
5.3. Personnel Controls
5.4. Audit Logging Procedures
5.5. Records Archival
5.5.1. Types of Records Archived

5.5.2. Retention Period for Archive
5.5.3. Protection of Archive
5.5.4. Archive Backup Procedures
5.5.5. Requirements for Time-Stamping of Records
5.5.6. Archive Collection System (Internal or External)
5.5.7. Procedures to Obtain and Verify Archive Information
5.6. Key Changeover
5.7. Compromise and Disaster Recovery
5.8. CA or RA Termination
6. Technical Security Controls
6.1. Key Pair Generation and Installation
6.1.1. Key Pair Generation
6.1.1.1. ID Card
6.1.1.2. Digi-ID
6.1.1.3. Mobile ID
6.1.2. Private Key Delivery to Subscriber
6.1.3. Public Key Delivery to Certificate Issuer
6.1.3.1. ID Card
6.1.3.2. Digi-ID
6.1.3.3. Mobile ID
6.1.4. CA Public Key Delivery to Relying Parties
6.1.5. Key Sizes
6.1.6. Public Key Parameters Generation and Quality Checking
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)
6.2. Private Key Protection and Cryptographic Module Engineering Controls
6.2.1. Cryptographic Module Standards and Controls
6.2.1.1. ID card and Digi-ID
6.2.1.2. Mobile ID
6.2.2. Private Key (n out of m) Multi-Person Control
6.2.3. Private Key Escrow
6.2.4. Private Key Backup
6.2.5. Private Key Archival
6.2.6. Private Key Transfer Into or From a Cryptographic Module
6.2.7. Private Key Storage on Cryptographic Module
6.2.8. Method of Activating Private Key
6.2.9. Method of Deactivating Private Key
6.2.10. Method of Destroying Private Key
6.2.11. Cryptographic Module Rating
6.3. Other Aspects of Key Pair Management
6.3.1. Public Key Archival
6.3.2. Certificate Operational Periods and Key Pair Usage Periods
6.4. Activation Data
6.4.1. Activation Data Generation and Installation
6.4.1.1. ID card
6.4.1.2. Digi-ID
6.4.1.3. Mobile ID
6.4.2. Activation Data Protection
6.4.3. Other Aspects of Activation Data
6.5. Computer Security Controls
6.5.1. Specific Computer Security Technical Requirements
6.5.2. Computer Security Rating
6.6. Life Cycle Technical Controls
6.7. Network Security Controls
6.8. Time-Stamping
7. Certificate, CRL, and OCSP Profiles
7.1. Certificate Profile
7.2. CRL Profile
7.3. OCSP Profile
8. Compliance Audit and Other Assessments
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
9.1.1.2. Mobile ID
9.1.2. Certificate Access Fees
9.1.3. Revocation or Status Information Access Fees
9.1.4. Fees for Other Services
9.1.5. Refund Policy
9.2. Financial Responsibility
9.2.1. Insurance Coverage
9.2.2. Other Assets
9.2.3. Insurance or Warranty Coverage for End-Entities
9.3. Confidentiality of Business Information
9.4. Privacy of Personal Information
9.5. Intellectual Property rights
9.6. Representations and Warranties
9.6.1. CA Representations and Warranties

9.6.1.1. ID card and Digi-iD
9.6.1.2. Mobile ID
9.6.2. RA Representations and Warranties
9.6.2.1. ID card and Digi-ID
9.6.2.2. Mobile ID
9.6.3. Subscriber Representations and Warranties
9.6.3.1. ID card and Digi-iD
9.6.3.2. Mobile ID
9.6.4. Relying Party Representations and Warranties
9.6.5. Representations and Warranties of Other Participants
9.6.5.1. ID card and Digi-ID
9.6.5.2. Mobile ID
9.7. Disclaimers of Warranties
9.8. Limitations of Liability
9.9. Indemnities
9.10. Term and Termination
9.10.1. Term
9.10.2. Termination
9.10.3. Effect of Termination and Survival
9.11. Individual Notices and Communications with Participants
9.12. Amendments
9.12.1. Procedure for Amendment
9.12.2. Notification Mechanism and Period
9.12.3. Circumstances Under Which OID Must be Changed
9.13. Dispute Resolution Provisions
9.14. Governing Law
9.15. Compliance with Applicable Law
9.16. Miscellaneous Provisions
9.16.1. Entire Agreement
9.16.2. Assignment
9.16.3. Severability
9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)
9.16.5. Force Majeure
9.17. Other Provisions
10. References

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 Trust Services Practice Statement" [2] 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, CRL and OCSP Profile for the personal identification documents of the Republic of Estonia" [3] (hereinafter referred to as Certificate Profile) documents are included where applicable.

1.1. Overview

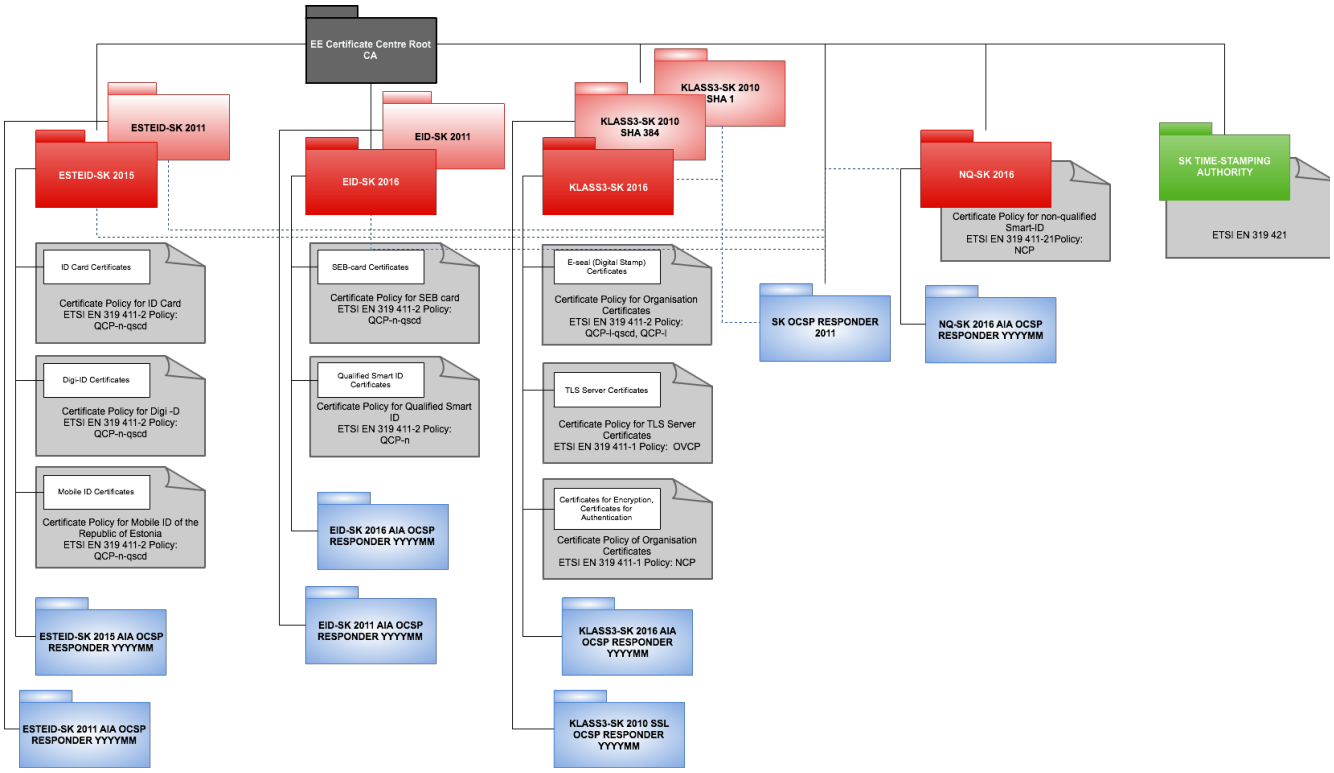
This CPS describes the practices used to comply with "SK ID Solutions AS - Certificate Policy for ID card" [4] (hereinafter referred to as CP), "SK ID Solutions AS - Certificate Policy for Digi-ID" [5] (hereinafter referred to as CP for Digi-ID) and "SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia" [6] (hereinafter referred to as CP for Mobile ID).

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

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

SK is currently using the following certificate chain:

EE Certification Centre Root CA chain, valid 2010-2030



This CPS covers operation of ESTEID-SK 2011 and ESTEID-SK 2015. The latter is the current issuing CA, whereas the older one is just serving status information for previously issued certificates.

The certification service for Qualified Electronic Signature Certificate for personal identification document as well as for the residence permit card (hereinafter referred together as ID card), the digital identity document as well as for the e-residence card (hereinafter together referred to as Digi-ID) and Mobile 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;
- NCP+;
- CP [4] or CP for Digi-ID [5] or CP for Mobile-ID [6];
- This CPS.

1.2. Document Name and Identification

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

1.3. PKI Participants

1.3.1. Certification Authorities

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

In case of ID card and Digi-ID, SK acts as a subcontractor of Trüb Baltic AS. There is a contract signed between Trüb Baltic AS and PBGB c overing production, personalisation of the ID card and Digi-ID as well as issuance and servicing of the Certificates.

In case of Mobile ID, SK provides the certification service under a contract signed between PBGB and SK.

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

The Certificates are issued by the intermediate CA-s ESTEID-SK 2011 and ESTEID-SK 2015 that are identified by the following certificates:

1) ESTEID-SK 2011

```
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number:
            29:52:93:aa:fd:8c:c6:d4:4d:83:30:a3:c2:64:51:0d
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification
Centre Root CA/emailAddress=pki@sk.ee
        Validity
            Not Before: Mar 18 10:14:59 2011 GMT
            Not After : Mar 18 10:14:59 2024 GMT
        Subject: C=EE, O=AS Sertifitseerimiskeskus, CN=ESTEID-SK
2011/emailAddress=pki@sk.ee
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b3:e9:7c:6c:66:1e:ab:fd:a5:dc:35:ed:e4:4a:
                    93:4c:3a:a9:90:a0:05:d4:a7:3c:dc:af:86:52:68:
                    66:61:ff:b2:47:22:2a:65:bc:d8:ba:b5:b5:bf:94:
                    ae:ec:02:24:6c:6f:ae:4a:cc:c5:91:38:46:ae:95:
                    de:ba:82:06:c3:3e:06:ba:91:4f:7b:0b:e0:17:1a:
                    ee:fe:0d:13:97:b2:d8:d4:3a:fe:95:96:b1:d9:54:
                    09:cb:98:83:a4:c9:ca:56:6b:18:cc:f8:47:d0:3d:
                    9b:83:c4:46:e4:c3:de:81:df:f7:c6:eb:d6:5b:a7:
                    7b:3d:cb:a5:84:87:05:39:63:d2:22:42:5f:18:4e:
                    41:a7:35:4c:62:75:06:ce:37:50:46:42:6f:87:54:
                    4b:20:4d:fd:b6:27:aa:fa:1b:71:6c:13:4e:eb:9c:
                    c3:6c:90:d0:b7:0e:3b:8b:48:25:0a:17:89:07:d2:
                    b5:46:54:af:41:76:20:9d:15:a6:63:1c:4c:a4:8f:
                    08:c8:1b:3a:a7:cb:1c:91:29:ee:18:6c:9e:81:f4:
                    00:66:f7:97:92:16:03:01:1e:d6:44:61:4f:aa:d1:
                    55:08:40:68:40:18:0b:ab:39:35:e3:5a:2d:53:b2:
                    c0:38:da:69:cb:19:06:44:23:91:97:31:7b:5a:6e:
                    9e:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.10015.100.1.1.1
                  User Notice:
                    Explicit Text:
                  CPS: https://www.sk.ee/CPS
            X509v3 Subject Key Identifier:

7B:6A:F2:55:50:5C:B8:D9:7A:08:87:41:AE:FA:A2:2B:3D:5B:57:76
            X509v3 Authority Key Identifier:

keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99
            X509v3 CRL Distribution Points:
                URI:http://www.sk.ee/repository/crls/eeccrca.crl
    Signature Algorithm: sha1WithRSAEncryption
        a0:b8:20:dd:c5:0b:68:15:0c:81:f4:e5:33:4c:80:5a:d0:38:
        21:92:9d:78:73:a0:97:25:44:ba:10:f3:50:42:39:74:d9:23:
        8a:a7:ec:de:f8:14:71:27:ac:0c:ba:b8:d1:bb:49:2e:6a:00:
        da:92:68:f2:0b:f1:da:7a:de:38:3f:2f:8a:a7:e2:25:9a:07:
```

```
9a:b9:18:62:4e:57:4e:d2:9d:31:d2:ee:05:2b:a8:28:46:0a:
59:d4:78:7c:62:65:b2:f5:dc:f9:0f:df:b2:e7:73:e4:ca:97:
54:8a:7e:0b:67:e4:56:c7:e5:ca:ab:86:f6:c0:fd:51:77:63:
39:62:9a:ef:8b:ec:45:68:85:6f:47:2b:16:7f:ff:3f:24:0e:
7e:a2:7a:23:c5:7d:97:53:3a:8b:ff:d1:e5:d5:2e:5c:6a:92:
5c:9b:52:e4:ba:2d:84:51:0e:2a:90:ba:98:01:29:00:53:c0:
d6:c2:f3:1d:14:1d:7d:34:1e:89:16:f9:d0:95:71:0b:ec:51:
bb:f8:c4:b8:51:ab:f3:2f:c9:3b:61:13:e4:5d:6e:4a:d5:d0:
```

```
        9b:b3:6d:f6:6f:00:37:e3:ef:99:c0:df:e6:40:cc:56:12:e5:
        9a:4c:3a:36:7d:a7:8a:d0:54:aa:73:41:39:25:ac:5d:26:ea:
        69:1d:70:4a
```

2) ESTEID-SK 2015

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:48:09:0b:87:9c:ef:21:56:72:ac:d3:de:6c:1b:5b
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification
Centre Root CA/emailAddress=pki@sk.ee
        Validity
            Not Before: Dec 17 12:38:43 2015 GMT
            Not After : Dec 17 23:59:59 2030 GMT
        Subject: C=EE, O=AS
Sertifitseerimiskeskus/2.5.4.97=NTREE-10747013, CN=ESTEID-SK 2015
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (4096 bit)
                Modulus (4096 bit):
                    00:d2:81:fa:d4:d0:f1:6d:d5:bd:93:c9:cb:03:5a:
                    86:68:be:01:ee:fc:9d:a1:dd:84:c2:9f:d2:4c:16:
                    41:df:01:2d:20:90:8b:76:4a:44:b1:2f:29:5d:f1:
                    62:46:ac:03:56:c8:06:19:bb:be:43:df:6d:ae:56:
                    f9:2c:8e:f2:8b:ba:c8:91:1a:2f:e4:d7:ed:05:d4:
                    8d:3d:25:39:ac:08:58:3d:08:6f:65:94:20:3b:04:
                    5a:1d:ae:44:cb:e0:5a:2c:91:e6:2e:a6:10:4b:d8:
                    50:bd:0b:02:63:2c:2c:fb:15:6f:34:55:29:2b:4a:
                    46:0f:ae:22:c9:ca:9d:32:e0:65:fe:75:aa:dd:f2:
                    ee:66:9a:70:06:1d:15:16:5b:66:e2:78:6b:ff:54:
                    b4:47:d4:d1:26:9a:85:50:66:c6:af:83:8a:fc:3c:
                    1e:6d:0e:4f:8e:17:52:e3:48:02:50:dc:26:0b:b7:
                    cf:43:8b:c8:1f:ec:7e:4c:29:36:68:6f:ae:dc:ca:
                    00:cf:42:2b:a5:55:aa:8b:0c:c6:fe:fc:6b:7a:e3:
                    cf:02:48:17:78:50:9e:61:fe:9f:5c:bb:06:cf:85:
                    a2:be:c6:45:6e:98:76:a4:c8:c4:2e:ee:ac:96:d9:
                    41:5d:f0:06:dd:f1:af:e3:7b:7d:d5:55:e2:73:2c:
                    d1:fd:e4:f9:76:c0:7e:cc:5b:16:d6:c1:d5:fb:53:
                    8d:3e:bf:aa:ce:00:f1:08:7d:9c:9a:ea:a8:64:d7:
                    c8:22:af:9b:ba:86:f7:78:0f:1e:7b:e5:e9:24:a2:
                    50:af:ed:6a:1a:b9:a1:82:08:ef:02:17:3b:9b:a7:
                    14:e3:1f:d0:7f:1c:11:62:12:15:36:12:5f:fa:c2:
                    95:4e:19:10:85:b2:7d:5f:1b:8a:93:77:35:f3:0c:
                    a6:c0:bd:66:a4:30:f4:3c:81:89:aa:5b:2c:31:e8:
                    ae:27:82:33:6a:01:5b:80:44:86:34:35:1d:e2:27:
                    26:d2:14:13:f0:29:90:79:49:b5:19:b5:9e:05:8b:
                    1e:a8:f8:4c:41:7f:7b:40:50:4b:5c:92:d5:cb:64:
                    82:ca:80:33:ec:1a:b5:a8:0e:37:fb:e1:1c:89:b3:
                    7e:c8:17:35:9d:0b:36:66:8a:bc:72:4f:4c:2b:46:
                    c2:c4:33:1e:52:44:14:cf:a5:5e:40:6a:7a:f4:89:
                    8e:42:bb:30:e3:aa:93:cf:49:ad:75:0a:cc:49:b9:
                    e4:5c:2b:8b:6a:7e:5d:3e:6d:bc:e0:9f:47:99:aa:
```

```
                    a2:62:2e:a3:e8:a2:dc:67:63:64:52:70:d0:15:eb:
                    01:56:53:04:9b:e7:c7:6b:68:91:ea:59:c0:15:86:
                    74:e9:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99
            X509v3 Subject Key Identifier:

B3:AB:88:BC:99:D5:62:A4:85:2A:08:CD:B4:1D:72:3B:83:72:47:51
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: 0.4.0.2042.1.2
                Policy: 0.4.0.194112.1.2
                Policy: 1.3.6.1.4.1.10015.1.1
                  CPS: https://www.sk.ee/CPS
                Policy: 1.3.6.1.4.1.10015.1.2
                Policy: 1.3.6.1.4.1.10015.1.3
                Policy: 1.3.6.1.4.1.10015.1.4
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Name Constraints:
                Excluded:
                  DNS:""
                  IP:0.0.0.0/0.0.0.0
                  IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0
            X509v3 Extended Key Usage:
                OCSP Signing, TLS Web Client Authentication, E-mail
Protection
            Authority Information Access:
                OCSP - URI:http://ocsp.sk.ee/CA
                CA Issuers -
URI:http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt
            X509v3 CRL Distribution Points:
                URI:http://www.sk.ee/repository/crls/eeccrca.crl
    Signature Algorithm: sha384WithRSAEncryption
        74:56:0c:62:37:3f:4d:2b:da:c3:a7:96:f2:c7:2a:4f:5e:13:
        b5:fd:dd:e4:fe:e1:ee:53:79:a4:2c:3a:91:39:cd:04:54:4e:
        db:21:c4:df:01:9f:1d:93:a1:0f:6b:82:2d:7c:ab:e3:30:5e:
        6d:9f:d2:6a:c6:6a:46:18:1b:46:e2:c7:b6:60:0d:0b:c2:30:
        3f:e4:b9:16:26:c0:b1:9d:7e:c4:d7:c2:1f:0a:b8:be:ae:48:
        71:7e:53:f6:53:b2:ce:aa:1b:b9:b1:08:71:bd:62:f7:9b:90:
        de:58:8f:fa:d8:46:f6:7d:fe:e2:7d:ae:27:81:cb:1c:38:c2:
        8e:db:d7:da:76:d8:f5:e4:02:45:cf:e7:2d:fe:a8:af:ce:7a:
        df:7c:96:ac:08:f7:b9:09:86:24:b6:cf:11:58:46:4f:9d:5d:
        b6:b3:9a:85:47:9e:8c:d8:2a:6b:19:69:25:2f:a1:83:4d:1f:
        5f:6d:a5:2e:c1:2d:db:20:8b:d2:a9:6e:f4:0b:6f:9c:b0:20:
        ca:bd:ba:dd:fe:6f:65:ef:ce:af:32:ce:61:cc:16:d2:c8:27:
```

```
a0:1f:bb:58:c9:a6:a0:fc:d8:15:00:15:cb:e2:e6:f8:67:3f:
c3:3b:6f:de:f8:47:5f:16:08:ea:60:35:0b:d7:0c:8f:b6:ff:
c6:48:35:e5
```

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 [9].

PBGB and Ministry of Foreign Affairs 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 [9], 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/

Ministry of Foreign Affairs can be contacted through its embassies and representations that can be checked at Ministry of Foreign Affairs 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 and/or service points of SEB Pank and Swedbank.

The exchange of Certificates of ID card and Digi-ID is carried out in PBGB Customer Service Points or using an application located in public data network.

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

- https://www.politsei.ee/en/kontakt/kmb/;
- http://www.vm.ee/en/country-representations/estonian-representations;
- https://sk.ee/en/kontakt/customerservice/.

1.3.2.1.2 SK Customer Service Point

Servicing Certificates of ID card and Digi-ID (suspensions, terminations of suspension, revocations and designations of replacement of PIN envelopes) is carried out in service points of SEB Pank and Swedbank (hereinafter referred to as SK Customer Service Point).

SK Customer Service Point acts as the representative of SK in the relations between SK and the Subscriber.

The relationship between SK Customer Service Point and SK is regulated by a bilateral agreement(s).

Information on SK Customer Service Points and their contact is available on the website of SK https://sk.ee/en/kontakt/customerservice/.

1.3.2.2. Mobile ID

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

- PBGB and MO are together referred to as RA when they are performing technical actions that are not specific to any particular organisation – e.g. Subscriber Authentication;
- PBGB and MO are explicitly referred to by their corresponding names, when they are performing actions specific to a particular type of organisation – e.g. issuing QSCD to the Subscriber or charging the state fee or PBGB when it is representing Republic of Estonia in the role of Document Issuer according to IDA [9], e.g. during initial identification of persons or making decisions about their eligibility to apply for Mobile 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/

The contact details of MO can be checked on the website of SK http://www.sk.ee.

For issuance of the QSCD there are contracts signed between SK and MO. SK has contractually delegated the responsibilities described in clause 1.3.2.2.1 to MO.

1.3.2.2.1 MO Customer Service Point

Issuance and servicing of QSCD-s, forwarding the request for Mobile ID Certificates in case of replacement of QSCD (Certificate re-key), servicing of Mobile ID Certificates and change of the mobile telephone number takes place in authorised MO Customer Service Points.

MO Customer Service Point accepts applications from Subscribers for revocation of Mobile ID Certificates. Before accepting an application for revocation, MO Customer Service Point verifies the Subscriber's identity according to its internal identification procedure.

The list and contact details of MO Customer Service Point can be checked on SK's website https://sk.ee/en/kontakt/customerservice/ and MO.

1.3.2.2.2 SK Customer Service Point

SK operates as a Customer Service Point.

SK Customer Service Point accepts electronically signed applications of suspension and termination of suspension of Mobile ID Certificates.

Contact information is available on the website of SK https://sk.ee/en/kontakt/.

1.3.2.3. Help Line

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

The Help Line accepts applications for suspension of Certificates of ID card and Digi-ID from Subscribers and other parties.

The Help Line also provides additional information and assists Subscribers regarding Mobile ID if necessary. The Help Line does not accept applications for suspension of Mobile ID Certificates.

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

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

1.3.3. Subscribers

Refer to clause 1.3. of the CP [4], CP for Digi-ID [8] and CP for Mobile-ID [9].

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. ID card and Digi-ID

Trüb Baltic AS:

- accepts ID card orders;
- produces ID card and Digi-ID blanks;
- personalises ID cards based on the orders sent by PBGB;
- generates the keys on the card for ID card and requests the corresponding Certificates;
- loads the Certificates to ID card;
- delivers personalised ID cards to PBGB;
- delivers Digi-ID blanks to PBGB;
- provides technical environment for personalisation of Digi-ID in RA office;
- produces replacement PIN-envelopes for ID card and Digi-ID.

Trüb Baltic AS may be contacted at:

Laki 5,

10621 Tallinn

Information: +372 658 11 30

E-mail: info@trueb.ee

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

1.3.5.2. Mobile ID

SCM:

- produces QSCD-s, generates key pairs and loads them on a QSCD.

MO:

- associates the Subscriber to specific QSCD and issues QSCD to the Subscriber.

Telecommunication Service Provider:

- operates software called Digidoc Service [15] that enables Mobile ID usage.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Refer to clause 1.4 of the CP [4], CP for Digi-ID [5] and CP for Mobile-ID [6].

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@sk.ee

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

1.5.2. Contact Person

Business Development Manager

Email: info@sk.ee

1.5.3. Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4. CPS Approval Procedures

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

In case the CP [4] and/or CP for Digi-ID [5] and/or CP for Mobile ID [6] are 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 Trüb Baltic AS.

All amendments to this CPS regarding Mobile ID are coordinated with PBGB and MO.

All amendments are approved by the business development manager and amended CPS is enfored 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 SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation [10].
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.
Directory Service	Trust service related to publication of Certificate validity information.
Digidoc Service	A SOAP-based web service with the help of which one can easily add identification, digital signature, signature identification and Mobile ID functionality to an e-service or application.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Digi-ID	Digital Identity Document.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
E-resident	A foreigner, for whom Estonia has created a digital identity and issued digital identification Document – an e-resident Digi-ID, on the basis of the identification credentials of their own country of citizenship.
E-resident Digi-ID	Digital identification document issued to a foreigner who has no right and need to apply for ID card or RP card.

ID card	An identification document which is a mandatory identity document of the Estonian citizens and aliens staying/residing permanently in Estonia.
ID-1	Format which defines physical characteristics of identification cards according to the standard ISO/IEC 7816 [11].
Integrity	A characteristic of an array: information has not been changed after the array was created.
Mobile ID	A digital identity in a mobile ID format, the Certificates of which enabling electronic identification and electronic signature are connected to the SIM-card of Mobile phone.
Object Identifier	An identifier used to uniquely name an object (OID).
Personal Data File	File on ID card and Digi-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.
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 [10].
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 [10]. In the context of Mobile ID, QSCD compliant SIM-card is a QSCD.
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 [9], 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 Mobile-ID are issued as a public service if he/she has a statutory right. 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.
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 [12] upon receipt of the Certificates.
Trüb Baltic AS	Manufacturer of ID cards. Additionally, Trüb Baltic AS prepares Digi-ID blanks in the factory and provides technical environment for personalisation in RA office.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [10] 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 [9]
MO	Mobile Operator
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [8]
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 [7]
RA	Registration Authority
SCM	SIM-card Manufacturer
SK	SK ID Solutions AS
SK PS	SK ID Solutions AS Trust Services Practice Statement [2]

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

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

This CPS and referred documents - the CP [4], CP for Digi-ID [5] and CP for Mobile-ID [6] and the Certificate Profile [3] as well as the "Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia" [12] (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.

2.2.2. Items not Published in the Certification Practice Statement

Refer to clause 2.2.2 of the CP [4], CP for Digi-ID [5] and CP for Mobile-ID [6].

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].

Value in the Organisation Name (O) indicates whether the Certificate is issued for the ID card, Digi-ID or Mobile-ID:

ID-card and RP-card O = ESTEID

Digi-ID: O = ESTEID (DIGI-ID)

Mobile-ID: O = ESTEID (MOBIIL-ID)

E-resident digi-ID: O = ESTEID (DIGI-ID E-RESIDENT)

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 [9], 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

3.2.1.1. ID card and Digi-ID

Private Key of the Subscriber is generated on the QSCD during personalisation in the chip of ID card or Digi-ID by Trüb Baltic AS and PBGB respectively.

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

3.2.1.2. Mobile ID

MO performs Subscriber Authentication and issues unpersonalised QSCD with pre-generated keys to the Subscriber. The Subscriber signs the corresponding application form and confirms the ownership of the issued QSCD.

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 [9].

PBGB submits identification data to Trüb Baltic AS. Trüb Baltic AS forwards the data for the Certificate to SK.

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

3.2.3.2. Mobile ID

Initial identity validation upon application for the issuance of QSCD is carried out by MO via physical presence checks.

If the Subscriber has lost his/her Mobile ID due to negligence and applies for a new Mobile ID, PBGB performs Subscriber Authentication via physical presence checks or by using electronic authentication means prior to requesting issuance of Mobile ID Certificates from SK. PBGB can perform electronic authentication only if the Subscriber has been issued a valid ID card or Digi-ID.

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 [9].

The Subscriber cannot apply for Mobile ID through a representative and Mobile ID cannot be issued to a representative.

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

3.3.1.1. ID card and Digi-ID

If the re-keying is done online using a designated application running in the Subscriber's computer, the Subscriber is authenticated using the valid Authentication Certificate of the ID card or Digi-ID that needs to be re-keyed.

If the re-keying is part of replacement of the physical card, identification and authentication procedures are similar to initial issuance as described in clause 3.2.3.1 of this CPS.

3.3.1.2. Mobile ID

In case of replacement of QSCD for valid Mobile ID (Certificate re-key) MO electronically verifies the Subscriber's identity and validates the Subscriber's electronic signature. MO can also perform Subscriber Authentication via physical presence.

3.3.2. Identification and Authentication for Re-Key After Revocation

3.3.2.1. ID card and Digi-ID

The Subscriber fills and signs the application for ID card or Digi-ID at PBGB Customer Service Point.

PBGB verifies the identity of the Subscriber in accordance with the IDA [9].

3.3.2.2. Mobile ID

In case the Certificates are revoked, the Subscriber has to apply for new Mobile ID and new Certificates.

Authentication of the Subscriber is carried out pursuant to clause 3.2.3.2 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 [9].

PBGB is communicating with SK only through Trüb Baltic AS. SK accepts CSRs only from Trüb Baltic AS.

4.1.1.2. Mobile ID

Certificate application can be submitted by the Subscriber via RA. SK accepts Certificate applications only from RA.

Mobile ID can be issued to the Subscriber who has a valid ID card or Digi-ID.

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 and confirms the correctness of the information. PBGB verifies the eligibility for the Subscriber to request ID card in accordance with the IDA [9].

In case of positive decision, PBGB forms the order for a new card and forwards it to Trüb Baltic AS. After receiving and accepting an application for a new card, Trüb Baltic AS manufactures the card, imprints visual elements to it, fills out Personal Data File on the card, generates keypairs for the Authentication and Qualified Electronic Signature. Trüb Baltic AS submits a pair of CSRs to SK.

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

The Certificates corresponding to the application are issued by SK upon automated authenticity and integrity verification of application data forwarded by PBGB.

SK is responsible for assigning the correct e-mail address in the eesti.ee domain to the certificate for Authentication. In case an e-mail address has already been assigned to the Subscriber, SK re-uses an assigned address. If the Subscriber has changed her name or has no previously assigned address, SK generates a new address according to clause 6.1 of the Certificate Profile [3].

SK forwards the Certificates to Trüb Baltic AS. Trüb Baltic AS loads the Certificates to the ID card and delivers personalised, but inactive and 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 and confirms the correctness of the information. PBGB verifies the eligibility for the Subscriber to request Digi-ID in accordance with the IDA [9]. 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 personalises a new Digi-ID, fills out Personal Data File, generates keypairs for Authentication and Qualified Electronic Signature and submits a pair of CSRs to Trüb Baltic AS. Trüb Baltic AS forwards the Certificate request to SK.

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

The Certificates corresponding to the application are issued by SK upon automated authenticity and integrity verification of application data forwarded by PBGB.

SK is responsible for assigning the correct e-mail address in the eesti.ee domain to the certificate for Authentication. In case an e-mail address has already been assigned to the Subscriber, SK re-uses an assigned address. If the Subscriber has changed her name or has no previously assigned address, SK generates a new address according to clause 6.1 of the Certificate Profile [3].

PBGB loads the Certificates to Digi-ID and personalises Digi-ID. SK forwards the inactive Certificates to Trüb Baltic AS.

4.1.2.3. Mobile ID

MO performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS. Upon successful Authentication, the Subscriber signs a Mobile ID agreement with MO and confirms the correctness of the information.

MO issues the QSCD to the Subscriber and forwards the information that associates the Subscriber with the Private Keys on the issued QSCD to SK.

The Subscriber submits an application for Mobile ID Certificates in web-based application submission environment of PBGB or via MO. Alter natively, the Subscriber submits an application for Mobile ID Certificates at PBGB and confirms the correctness of the information.

PBGB performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS and verifies the Subscriber's eligibility to request Mobile ID according to IDA [9]. In case of positive decision, PBGB forwards the application for the Certificates to SK.

The Certificates corresponding to the application are issued by SK upon automated authenticity and integrity verification of application data forwarded by RA.

SK is responsible for assigning the correct e-mail address in the eesti.ee domain to the certificate for Authentication. In case an e-mail address has already been assigned to the Subscriber, SK re-uses an assigned address. If the Subscriber has changed her name or has no previously assigned address, SK generates a new address according to clause 6.1 of the Certificate Profile [3].

SK relies on the identification data provided by PBGB.

If the Subscriber applies for a new Mobile ID, PBGB terminates valid Mobile ID and issues new Mobile ID to the Subscriber.

The Subscriber can apply for a new Mobile ID if the Subscriber has lost his/her Mobile ID due to negligence. The request for a new Mobile ID is processed pursuant to clause 3.2.3.2 of this CPS.

Certificates of the old Mobile ID are revoked.

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 Chapter 3 of IDA [9].

In case of ID card, PBGB forms the order for a new card and forwards it to Trüb Baltic AS.

In case of Digi-ID, PBGB sends the Certificate requests to SK via Trüb Baltic AS.

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

SK accepts CSRs only from Trüb Baltic AS.

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

4.2.1.2. Mobile ID

The Subscriber can apply for Certification in the following way:

- in case the Subscriber applies for a new Mobile ID, the Subscriber applies for Certification in web-based application submission environment of PBGB or via MO from PBGB or at PBGB. PBGB applies for Certification over data exchange layer X-Road at SK on

behalf of the Subscriber.

RA performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS.

Upon successful Authentication the Subscriber can apply for Certification by signing the corresponding request at RA.

SK accepts Certification applications only from RA. Certificate applications for Mobile ID contain explicit statement regarding the QSCD ownership by the Subscriber. RA validates QSCD ownership and ensures the validity of the Public Keys presented for Certification.

SK relies on identification information provided by RA.

4.2.2. Approval or Rejection of Certificate Applications

4.2.2.1. ID card

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

SK refuses to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable agreements. If the data contained in a CSR needs to be modified, SK coordinates corresponding amendment with PBGB.

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

4.2.2.2. Digi-ID

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

SK refuses to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable agreements. If the data contained in a CSR needs to be modified, SK coordinates corresponding amendment with PBGB.

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

4.2.2.3. Mobile ID

One decision is sufficient for issuing several Certificates to a single Subscriber as long as no more than one Mobile ID remains valid at any point of time. See clauses 4.7 and 4.8 of this CPS.

SK refuses to issue a Certificate if the Certificate request does not comply with the technical requirements set in applicable agreements. If the data contained in a Certificate request needs to be modified, SK coordinates corresponding amendment with RA.

SK notifies the entity that requested Certification 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], CP for Digi-ID [5] and CP for Mobile-ID [6].

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

4.3.1.1. ID card and Digi-ID

After checking the authenticity and integrity of the Certificate application received from Trüb Baltic AS, SK automatically issues the corresponding Certificates and allocates correct and unique e-mail address in the eesti.ee domain to the Subscriber. Certificates are loaded to the ID card at Trüb Baltic AS or to the Digi-ID in PBGB.

All issued Certificates are in an inactive state, meaning the OCSP service does not confirm their validity and the certificates are not available via Directory Service. The inactive certificates are stored in a private database of SK. The certificates are activated only after being accepted by the Subscriber.

4.3.1.2. Mobile ID

After checking the authenticity and integrity of the Certificate application received from RA, SK automatically issues the corresponding Certificates and allocates correct and unique e-mail address in the eesti.ee domain to the Subscriber.

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. Mobile ID

The Subscriber is notified by PBGB of the issuance of Mobile ID.

SK notifies RA of the new Certificate issuance to the Subscriber.

RA notifies the Subscriber of the new Certificate issuance.

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 Subscriber has read and agrees to the Terms and Conditions [12]. The Subscriber also confirms that the ID card or Digi-ID has been handed over to him/her. The employee of PBGB Customer Service Point forwards the request for activation of the Certificates to SK. The Certificates on the ID card and Digi-ID are activated by SK immediately.

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

Acceptance of and signing the Terms and Conditions [12] 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. Mobile ID

The following conditions are considered enough for Certificate acceptance:

- the Subscriber has signed a request for Certification at PBGB pursuant to clause 4.2.1.2 of this CPS;
- SK has received corresponding certification application from PBGB.

4.4.2. Publication of the Certificate by the CA

4.4.2.1. ID card and Digi-ID

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

Suspended and revoked Certificates are deleted from Directory Service.

In case of termination of suspension of Certificates, Certificates are re-published in Directory Service. Expired Certificates are deleted from Directory Service on the next day following the expiration.

4.4.2.2. Mobile ID

Certificates are made available via Directory Service at ldap://ldap.sk.ee/ and Digidoc Service [15] after issuance of the Certificates by SK.

Suspended and revoked Certificates are deleted from Directory Service.

In case of termination of suspension of Certificates, Certificates are re-published in Directory Service. Expired Certificates are deleted from Directory Service on the next day following the expiration.

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

SK delivers Certificates issued for ID card and Digi-ID immediately to Trüb Baltic AS for loading to the cards.

SK notifies Telecommunication Service Provider about issued Mobile ID Certificates.

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], CP for Digi-ID [5] and CP for Mobile-ID [6];
- this CPS;
- the Terms and Conditions [12].

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], CP for Digi-ID [5] and CP for Mobile-ID [6];
- this CPS;
- the Terms and Conditions [12].

4.6. Certificate Renewal

Issuing replacement ID card, Digi-ID or Mobile 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 Mobile ID, this request is processed as an application for a new ID card, Digi-ID or Mobile ID.

The re-keying procedures and conditions are different for Mobile ID and smartcards due to technical reasons.

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

4.7.1. Circumstances for Certificate Re-Key

4.7.1.1. ID card and Digi-ID

Certificate re-key is allowed to:

- replace an expired or broken ID card or Digi-ID;
- fix production errors;
- fix ASN.1 encoding errors in Certificates;
- changeover to stronger cryptography.

Certificate re-key to fix production errors is performed upon initial application for ID card or Digi-ID. In this case, only the last Certificates are written to the card or Digi-ID media and remain valid.

Certificate re-key to fix ASN.1 encoding errors in Certificates or changeover to stronger cryptography can be requested:

- in a respective application in public data network only if Authentication Certificate of the ID card or Digi-ID is valid and in active state and at PBGB Customer Service Point.

Certificate re-key to fix ASN.1 encoding errors in Certificates or changeover to stronger cryptography can be requested at PBGB Customer Service Point if:

- failure of the re-key in an application in public data network has resulted in revocation of the Certificates;
- the Certificates are suspended;
- the activation code of the Authentication Certificate (PIN1) is blocked;
- the Certificates are in inactive state.

If the Subscriber has applied for revocation of his/her Certificates, Certificate re-key to fix ASN.1 encoding errors in Certificates or hangeover to stronger cryptography cannot be performed.

4.7.1.2. Mobile ID

Certificate re-key is allowed only if the QSCD has to be replaced.

4.7.2. Who May Request Certification of a New Public Key

4.7.2.1. ID card and Digi-ID

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

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

Certificate re-key process to fix ASN.1 encoding errors in Certificates or changeover to stronger cryptography can only be initiated by the Subscriber.

All the Certification requests are delivered to SK through Trüb Baltic AS.

4.7.2.2. Mobile ID

Certificate re-key process can only be initiated by the Subscriber.

All the Certification requests are delivered to SK through MO.

4.7.3. Processing Certificate Re-Keying Requests

4.7.3.1. ID card and Digi-ID

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

After PBGB has discovered Digi-ID production errors during quality checks, PBGB submits a new CSR to SK through Trüb Baltic AS.

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 or Digi-ID issuance.

The process of Certificate re-key using an application in public data network is the following:

- the Subscriber is identified using the valid Authentication Certificate of the ID card;
- the Subscriber confirms that he/she has read and agrees with the Terms and Conditions [12];
- Certificate re-key is performed;
- the Subscriber is notified of the issuance of the new Certificate by the same application.

The process of Certificate re-key at PBGB Customer Service Point is the following:

- the Subscriber is identified by an employee of PBGB Customer Service Point;
- the Subscriber signs the application for replacement of PIN and PUK codes and confirms that he/she has read and agrees with the Terms and Conditions [12];
- Certificate re-key is performed;
- the Subscriber is notified of the issuance of the new Certificate by an employee of PBGB Customer Service Point.

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.

4.7.3.2. Mobile-ID

MO performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS. Upon successful Authentication, the Subscriber signs an agreement with MO with a Qualified Electronic Signature or handwritten signature and confirms the correctness of the information.

The Subscriber also confirms that the QSCD to be replaced has been issued to him/her. In case the Subscriber has lost his/her Mobile ID due to negligence, the Subscriber can apply for a new Mobile ID. The request for a new Mobile ID is processed pursuant to clause 3.2.3.2 of this CPS.

MO issues new QSCD to the Subscriber and forwards the information that associates the Subscriber with the Private Keys on the issued QSCD and corresponding Public Keys to SK. SK uses corresponding Public Keys for Certification.

MO forwards the request for the Certificates over secure communication channel to SK.

SK verifies validity of the QSCD to be replaced and previously issued Certificates.

In case of positive decision, SK signs the registered Public Keys and issues new Certificates for the valid Mobile ID and notifies PBGB about the issuance of new Certificates.

MO preserves applications for replacement of QSCD and for the Certificates signed by the Subscriber.

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

SK immediately revokes the Certificates that have been replaced and thereafter notifies PBGB of revocation of the Certificates.

4.7.4. Notification of New Certificate Issuance to Subscriber

4.7.4.1. ID card and Digi-ID

If the Certificate re-key is performed to fix production errors or order to replace an expired or broken ID card or Digi-ID, notification of the Subscriber is similar to initial notification pursuant to clause 4.3.2.1 of this CPS.

If the Certificate re-key to fix ASN.1 encoding errors in Certificates or changeover to stronger cryptography is performed in an application in public data network, the Subscriber is notified of the issuance of the new Certificate by the application immediately after the Certificate has been issued.

If the Certificate re-key to fix ASN.1 encoding errors in Certificates or changeover to stronger cryptography is performed at PBGB Customer Service Point, the Subscriber is notified of the issuance of the new Certificate by an employee of PBGB Customer Service Point.

4.7.4.2. Mobile ID

SK notifies MO of the new Certificate issuance to the Subscriber.

MO notifies the Subscriber of the new Certificate issuance.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

4.7.5.1. ID card and Digi-ID

If the Certificate re-key is performed to fix production errors or in order to replace an expired or broken ID card or Digi-ID, the Subscriber confirms that he/she has read and agrees to the Terms and Conditions [12] as stated in clause 4.4.1.1 of this CPS.

If the Certificate re-key is performed in an application in public data network, the Subscriber is notified of the issuance of the new Certificate by the application. Notification by the application is deemed acceptance of a re-keyed Certificate.

If the Certificate re-key is performed at PBGB Customer Service Point, the Subscriber is notified of the issuance of the new Certificate by an employee of PBGB Customer Service Point. Notification by an employee of PBGB Customer Service Point is deemed acceptance of a re-keyed Certificate.

4.7.5.2. Mobile ID

In case the Subscriber applies for replacement of a QSCD (Certificate re-key), the following conditions are considered enough for Certificate acceptance:

- the Subscriber has signed a request for Certification at MO pursuant to clause 4.2.1.2 of this CPS;
- SK has received corresponding certification application from MO.

SK issues the Certificates and notifies RA of the new Certificate issuance to the Subscriber. RA notifies the Subscriber of the new Certificate issuance and respective notification is deemed Certificate acceptance.

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

If the modification requires replacement of the underlying document (e.g. to change the data visually imprinted on the ID card) then this is treated as a new application.

The modification procedures and conditions are different for Mobile ID and smartcards due to technical reasons.

During Certificate modification, all the erroneous or unusable Certificates to be replaced are revoked.

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

4.8.1. Circumstances for Certificate Modification

4.8.1.1. ID card and Digi-ID

Certificate modification is allowed to:

- to change the data visually imprinted on the ID card or Digi-ID and stored in the Personal Data File,
- fix production errors that are discovered during quality checks;

- change e-mail addresses written to Subject Alternative Name field of the Authentication Certificate;
- fix ASN.1 encoding errors in Certificates;
- replace SHA-1 signatures with stronger cryptography.

Certificate modification to fix production errors that are discovered during quality checks is performed upon initial application for ID card or Digi-ID. In this case, only the last Certificates are written to the card or Digi-ID media and remain valid.

Certificate modification to change e-mail addresses written to Subject Alternative Name field of the Authentication Certificate or to fix ASN.1 encoding errors in Certificates or replace SHA-1 signatures with stronger cryptography can be requested:

- in public data network in case the Authentication Certificate of the ID card or Digi-ID is valid and in active state or
- at PBGB Customer Service Point.

4.8.1.2. Mobile ID

Certificate modification is allowed only under following circumstances:

- change e-mail addresses written to the Subject Alternative Name field of the Authentication Certificates;
- fix ASN.1 encoding errors in Certificates;
- replace SHA-1 signatures with stronger cryptography.

4.8.2. Who May Request Certificate Modification

4.8.2.1. ID card and Digi-ID

Certificate modification process to fix production errors of ID card can only be initiated by Trüb Baltic AS.

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

Certificate modification process to change e-mail addresses written to the Subject Alternative Name field of the Authentication Certificates or to fix ASN.1 encoding errors in Certificates or replace SHA-1 signatures with stronger cryptography can only be initiated by the Subscriber.

All the Certification requests are delivered to SK through Trüb Baltic AS.

4.8.2.2. Mobile ID

Certificate modification process can only be initiated by SK.

4.8.3. Processing Certificate Modification Requests

4.8.3.1. ID card and Digi-ID

Refer to clause 4.7.3.1 of this CPS.

4.8.3.2. Mobile ID

SK processes Certificate Modification requests and is not required to coordinate it with the Subscriber.

4.8.4. Notification of New Certificate Issuance to Subscriber

SK notifies the Subscriber of new Certificate issuance.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Refer to clause 4.7.5 of this CPS.

4.8.6. Publication of the Modified Certificate by the CA

Refer to clause 4.7.6 of this CPS.

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

Refer to clause 4.7.7 of this CPS.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1 of the CP [4], CP for Digi-ID [5] and CP for Mobile-ID [6].

4.9.2. Who Can Request Revocation

4.9.2.1. ID card and Digi-ID

PBGB can present an application to revoke the Certificate of ID card or Digi-ID in accordance with IDA [9].

The Subscriber or third party can submit an application for revocation of the Certificate.

4.9.2.2. Mobile ID

PBGB can present an application to revoke the Certificate of Mobile ID in accordance with IDA [9].

MO can present an application for revocation of the Certificate on behalf of the Subscriber.

The Subscriber or third party can submit an application for revocation of the Certificate.

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 [9].

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

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

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] or CP for Digi-ID [5] is verified;
- the Certificate is revoked by SK;
- 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.

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.

Revoked Certificate can not be reinstated.

4.9.3.2. Mobile ID

Certificate revocation is regulated by provisions and procedures of revocation of identity document in IDA [9].

The Subscriber can apply for revocation of the Certificates by submitting an electronically signed application in the web based application submission environment of PBGB. A signed application for revocation of the Certificates can also be submitted at MO Customer Service Point.

An application for revocation is forwarded to SK by PBGB over data exchange layer X-Road and over secure communication channel by an employee of MO Customer Service Point

In case the Subscriber applies for revocation of the Certificate in web based PBGB environment, PBGB verifies the identity of the Subscriber in accordance with the Authentication Certificate related to ID card or Digi-ID.

If the Subscriber submits an application for revocation at MO Customer Service Point, an application for revocation is registered by an employee of MO Customer Service Point. An employee of MO 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.

After SK receives an application for revocation either from PBGB, MO Customer Service Point, the request is processed using a following automatic procedure:

- the compliance of the application for revocation with the CP for Mobile ID [6] is verified;
- the Certificate is revoked by SK;
- 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 an application for revocation is submitted by a third party, the procedure is manually initialized by SK. SK manually archives the documentation on which a revocation application submitted by a third party was based.

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.

Certificate revocation applies to Certificate Pairs only.

If one of the Certificates in a Certificate Pair is revoked, the entire Certificate Pair is revoked. Other Certificate Pairs can remain valid.

In case of a Mobile ID repeal, all related Certificate pairs are revoked.

Revoked Certificates 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. Mobile ID

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

4.9.5. Time Within Which CA Must Process the Revocation Request

After PBGB or MO 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 [12].

4.9.7. CRL Issuance Frequency

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

4.9.8. Maximum Latency for CRLs

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

4.9.9. On-Line Revocation/Status Checking Availability

An OCSP service is free of charge and publicly accessible.

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

4.9.10. On-Line Revocation Checking Requirements

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been established in the Terms and Conditions [12].

4.9.11. Other Forms of Revocation Advertisements Available

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

4.9.12. Special Requirements Related to Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Refer to clause 4.9.13 of the CP [4], CP for Digi-ID [5] and CP for Mobile-ID [6].

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 Customer Service Point of PBGB or SK.

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 Customer Service Point of PBGB or SK. An employee of PBGB or SK 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 [9] and Electronic Identification and Trust Services for Electronic Transactions Act [17] requ sts 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, the Customer Service Point of PBGB or SK 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] or CP for Digi-ID [5] 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 in accordance with 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. Mobile ID

The Subscriber can submit an electronically signed application for suspension of the Certificates to SK Customer Service Point.

If competent authority within the meaning of IDA [9] and Electronic Identification and Trust Services for Electronic Transactions Act [17] requ sts 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).

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

- the suspension request is registered by an employee of SK Customer Service Point;
- electronic signature of the person filing an application for suspension is validated by an employee of SK Customer Service Point;
- the legality to request suspension is verified by SK Customer Service Point employee;
- the compliance of the application for suspension of the Certificate with the CP for Mobile ID [6] is verified;
- 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, the Digidoc Service [15] stops responding with status "VALID" 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;
- the Subscriber is notified of suspension of the Certificate.

After SK has received an application for suspension, 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 an employee of SK Customer Service Point about the situation.

SK processes request for revocation according to clause 4.9.3.2 of this CPS. Revocation does not happen immediately. The tag about special treatment is removed from the database.

The Subscriber has a possibility to verify from the Directory Service, the Digidoc Service [15], the CRL or via OCSP that the Certificate has been suspended.

If the Subscriber applies for suspension, Certificate suspension applies to Certificate Pairs only.

If one of the Certificates in a Certificate Pair is suspended, the entire Certificate Pair is suspended. Other Certificate Pairs can remain valid.

The Subscriber can request suspension of the telecommunication service via the Telecommunication Service Provider Help Line 24 hours a day, 7 days a week. The operator of the Telecommunication Service Provider Help Line verifies the Subscriber by asking the Subscriber his/her safeword or check-up questions about the Subscriber's personal details (e.g. name, personal identification code, address).

Alternatively, the Subscriber can request suspension of the telecommunication service by submitting an application at Telecommunication Service Provider. An employee of the Telecommunication Service Provider verifies the Subscriber in accordance with internal verification procedures.

Suspension of the telecommunication service can result in:

- revocation of the Mobile ID Certificates or
- impossibility to use Mobile ID.

Suspension of the telecommunication service does not automatically result in revocation of the Certificates, the Subscriber is required to request revocation in case he/she is convinced that his/her device is lost or stolen. Otherwise the Certificates remain valid, but the usage of Mobile ID is disabled.

In case the Subscriber requests revocation of the Mobile ID Certificates, the request is processed pursuant to clause 4.9.3.2 of this CPS.

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], CP for Digi-ID [5] and CP for Mobile ID [6].

4.9.18. Who Can Request Termination of Suspension

4.9.18.1. ID card and Digi-ID

Refer to clause 4.9.18 of the CP [4].

4.9.18.2. Mobile ID

Refer to clause 4.9.18 of the CP for Mobile ID [6].

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 Customer Service Point of PBGB or SK. The

termination of suspension application is registered by an employee of the Customer Service Point of PBGB or SK.

An employee of PBGB or SK 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 Customer Service Point of PBGB or SK.

If competent authority within the meaning of IDA [9] and Electronic Identification and Trust Services for Electronic Transactions Act [17] 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] or CP for Digi-ID [5] 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 in accordance with 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. Mobile ID

The Subscriber can request termination of suspension of the Certificates by submitting an electronically signed application to SK Customer Service Point.

If competent authority within the meaning of IDA [9] and Electronic Identification and Trust Services for Electronic Transactions Act [17] 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 a request for termination of suspension, the procedure for processing the request is the following:

- the termination of suspension request is registered by an employee of SK Customer Service Point;
- electronic signature of the person filing an application for termination of suspension is validated by an employee of SK Customer Service Point;
- 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 legality to request termination of suspension is verified by SK Customer Service Point employee;
- the compliance of the application for termination of suspension of the Certificate with the CP for Mobile ID [6] is verified;
- 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, the Digidoc Service [15] st arts responding with status "VALID" 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 can also request termination of suspension of the Certificates by submitting an electronically signed application to MO Customer Service Point. After MO Customer Service Point has received an application for termination of suspension, the procedure for processing the application is the following:

- the application is registered by an employee of MO Customer Service Point;
- electronic signature of the person filing an application for termination of suspension is validated by an employee of MO Customer Service Point;
- the legality to request termination of suspension is verified by MO Customer Service Point employee;
- suspension of the Certificate is terminated in MO's information system by MO Customer Service Point employee;
- MO's information system immediately notifies SK of termination of suspension;
- SK confirms termination of suspension and immediately publishes the Certificate again in the Directory Service, the Digidoc Service

[15] starts responding with status "VALID" and OCSP starts responding with status "GOOD";
- a new CRL is published according to clause 4.9.7 of this CPS.

The Subscriber is immediately notified of the successful completion of procedure of termination of suspension of the Certificate. The Subscriber has a possibility to ascertain on the basis of the Directory Service, the Digidoc Service [15], the next CRL or via OCSP that the 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.

If the Subscriber applies for termination of suspension, termination of suspension applies to Certificate Pairs only.

If suspension of one of the Certificates in a Certificate Pair is terminated, suspension of the entire Certificate Pair is terminated.

If the Subscriber has applied for suspension of the telecommunication service as described in clause 4.9.15.2 of this CPS, the Subscriber can request restoration of the telecommunication service from the Telecommunication Service Provider. Restoration of the telecommunication service enables usage of Mobile ID, except if the Subscriber requested revocation of the Certificates during the time when telecommunication service was suspended.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

SK offers CRL and OCSP services for checking certificate status. Services are accessible over HTTP protocol.

The URL of the CRL service is included in the certificate on the CRL Distribution Point (CDP) field in accordance with the Certificate Profile [3]. 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] starting from 1. November 2016.

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

6.1. Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [2].

6.1.1. Key Pair Generation

Refer to clause 6.1.1 of SK PS [2].

6.1.1.1. ID Card

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

6.1.1.2. Digi-ID

The Subscriber Private Keys are generated during personalisation 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. During re-key, new keys are generated by the Subscriber in the card.

6.1.1.3. Mobile ID

The Private Keys are pre-generated by the SCM in a FIPS 140-2 Level 3 certified cryptographic device. The keys are loaded onto the QSCD in a secure manner. The Subscriber keys are protected by the activation PIN codes handed over and known only to the Subscriber. The SCM deletes private keys from her information system promptly after transferring them on the QSCD. Private Keys are not saved outside of the QSCD in the course of this transfer.

6.1.2. Private Key Delivery to Subscriber

The Subscriber Private Keys are delivered in the chip of the card and QSCD. The confidentiality and non-usage of the generated Private Keys and PIN codes until issuance of the card before delivery to the Subscriber is warranted by respective parties involved in handling the cards. The confidentiality and non-usage of the generated Private Keys and activation codes is also warranted by the inactive state of the ID card and Digi-ID Certificates and that QSCD is non-personalised before it is handed over to the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

6.1.3.1. ID Card

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

6.1.3.2. Digi-ID

The RA is using a custom application for instructing the card to start key generation. During this process the Public Key is delivered to Trüb Baltic AS via a secure and private channel, who in turn creates a signed message to request the Certificates from SK.

6.1.3.3. Mobile ID

The pregenerated Public Keys are delivered in batches from the SCM to MO. An authorized representative of the MO electronically signs the batch and requests loading the keys to a database in the SK. When issuing a Certificate, SK finds the correct Public Key from the database of previously loaded keys based on the serial number of the QSCD.

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

Subscriber keys are 2047 or 2048 bits when RSA and 256 or 384 bits when ECC algorithm is used.

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 (e.g. e > 1 for RSA). More thorough checks are run over database of issued Certificates regularly.

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

Refer to clause 6.1.7 of SK PS [2].

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

6.2.1.1. ID card and Digi-ID

Refer to clause 6.2.1 of SK PS [2].

The chips used to store Subscriber Private keys are QSCD according to eIDAS Regulation [10].

6.2.1.2. Mobile ID

Refer to clause 6.2.1 of SK PS [2].

The chips used to store Subscriber Private keys are QSCD according to eIDAS Regulation [10].

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

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 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 for ID card and Digi-ID are generated inside the card.

The Subscriber Private Keys for Mobile ID are transferred from the HSM to QSCD in a protected environment using a secure electronic channel.

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 Mobile 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 or group of Private Keys corresponding to a Certificate with unique Distinguished Name (i.e. there are separate PIN-s for Authentication Key and Signature Key, but RSA key for Authentication and ECC key for Authentication can be protected with the same PIN);
- The Subscriber must enter the activation code of the Authentication Certificate (PIN1) at least once after ID card or Digi-ID has been inserted into the card reader device or the mobile hanset has booted;
- The Subscriber must enter the activation code of the Qualified Electronic Signature Certificate (PIN2) before every single operation done with the corresponding Private Key;
- The usage of all Private Keys protected by a single PIN will be blocked after 3 consecutive incorrect tries;
- PIN can be unblocked using a PUK code;
- The usage of PUK code will be blocked after 3 consecutive incorrect tries;
- User can change the PIN and PUK codes.

The length of the activation codes is limited to:

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

If the PUK codes of ID card or Digi-ID are lost or blocked, the Subscriber can apply for replacement codes in the Customer Service Points of PBGB or SK. Replacement PIN-envelopes are not issued for E-resident Digi-ID and Mobile ID.

PIN and PUK codes for activating Private Keys of Mobile ID are different from PIN and PUK codes of the SIM card.

6.2.9. Method of Deactivating Private Key

Refer to clause 6.2.9 of SK PS [2].

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

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 Mobile ID SIM cards are QSCD according to eIDAS [10].

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

Activation codes are printed in one copy by TRÜB Baltic AS straight to the security envelope which is handed over to the Subscriber unopened. Copies of the activation codes are not stored by Trüb Baltic AS.

Activation codes are protected in such way that it is impossible to read them without breaking security element. The Subscriber has prerogative to refuse from accepting of activation codes with altered security element.

The replacement PIN envelopes are anonymous before issuing in the Customer Service Point. The envelopes are numbered and there is a cryptographically protected link between the number of envelope and the corresponding codes inside. During issuance an employee of the 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 Customer Service Point. The algorithm used and the details of communications protocol are described in ID Card documentation [16].

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

All activation codes of a single ID card are replaced at once.

Prior to issuing replacement activation codes RA performs Subscriber Authentication.

6.4.1.2. Digi-ID

The anonymous cards are initialised with fixed PIN code. During personalisation a replacement envelope is issued straight away according to protocol described in clause 6.4.1.1 of this CPS and ID card documentation [16].

6.4.1.3. Mobile ID

Activation codes are pregenerated by the SCM printed on the plastic of the QSCD containment under the secure layer. Activation codes are protected in such way that it is impossible to read them without breaking security element. The Subscriber has prerogative to refuse from accepting of activation codes with altered security element.

6.4.2. 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.sk.ee/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.sk.ee/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.sk.ee/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 [13]. Corresponding fee includes fee for the Certificate issuance.

The fee for the certificate issuance is considered business secret between SK and Trüb Baltic AS.

Certificate renewal is not performed.

9.1.1.2. Mobile ID

The Subscriber pays monthly fee for Mobile ID according to the rate provided for in MO's price list.

MO is entitled to charge a fee for a new Mobile ID and new QSCD.

The Subscriber signs different agreements for Mobile ID and QSCD with MO.

MO signs an agreement for Mobile ID solely with the Subscriber and can sign an agreement for QSCD with other party (e.g. legal person) than the Subscriber.

MO is entitled to charge a fee if the Mobile ID is still in valid state for more than 365 days and the Subscriber applies for the Certificates which validity end date is longer compared to validity end date of the Certificates issued for the valid Mobile ID.

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

Certificate renewal is not performed.

9.1.2. Certificate Access Fees

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

Mobile ID Certificates are also available in Digidoc Service [15].

Directory Service is free of charge and is accessible on ldap://ldap.sk.ee.

9.1.3. Revocation or Status Information Access Fees

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

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

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

The fee for Digidoc Service [15] is specified in the Subscriber or Relying Party agreement.

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

9.1.4. Fees for Other Services

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

Fees for issuance of replacement PIN envelopes are specified in SK Customer Service Point 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 [13].

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

9.6.1.1. ID card and Digi-iD

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, the CP [4] and the CP for Digi-ID [5];
- 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.

9.6.1.2. Mobile ID

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, the CP for Mobile ID [6];
- 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;
- it accepts and registers the issuance of the QSCD-s and corresponding Public Keys presented by MO;
- it accepts and registers the requests of the Certificates presented by MO, verifies validity of the QSCD to be replaced and previously issued Certificates (in case of Certificate re-key), decides the issuance of the certificates and forwards the information on issuance of Certificates to PBGB;
- it accepts and registers the Certificate requests presented by PBGB and issues the corresponding Certificates;
- it accepts, registers and processes the applications for revocation of Mobile ID Certificates presented by MO and forwards the information on revocation of the Certificates to PBGB;
- the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
- the certification keys used in the supply of the certification service are activated on the basis of shared control;
- it provides security with its internal security procedures.

9.6.2. RA Representations and Warranties

9.6.2.1. 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 issues ID card and Digi-ID to Subscribers by first activating the certificates loaded thereon;
- it accepts Subscriber applications for ID card and Digi-ID Certificate creations, suspensions, terminations of suspension, revocations;
- it accepts reasoned applications from the Subscriber for fixing ASN.1 encoding errors in Certificates and changeover to stronger cryptography and 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 Trüb Baltic AS about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

9.6.2.1.2 SK Customer Service Point

Refer to clause 9.6.2 of SK PS [2].

SK Customer Service Point ensures that:

- it accepts applications for the ID card and Digi-ID certificate suspensions, terminations of suspension, revocations of the certificates and assignation 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.

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

9.6.2.1.3 Help Line

Refer to clause 9.6.2 of SK PS [2].

The Help Line ensures that:

- it accepts applications for the ID card and Digi-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.

9.6.2.2. Mobile ID

9.6.2.2.1 RA

Refer to clause 9.6.2 of SK PS [2].

RA ensures that:

- it accepts applications from the Subscribers for the issuance of the Certificates and forwards them to SK;
- it checks the correctness and completeness of the applications submitted by the Subscribers;
- it identifies and verifies the Subscriber submitting an application for the issuance of the Certificates;
- it validates QSCD ownership and ensures the validity of the Public Keys presented for Certification;
- it accepts notifications from SK about Certificates issued by SK;
- the employees, who are involved with information related to certification service, are not punished for intentional crime;
- it provides security with its internal security procedures.

RA forwards true and complete data to SK.

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

9.6.2.2.2 PBGB

PBGB ensures that:

- it accepts applications for Certificates, decides approval of the applications and forwards the approved Certificate applications to SK;
- it accepts applications for revocation of Certificates, decides approval of the applications and forwards the approved Certificate revocation applications to SK;
- while processing the listed applications, it verifies accuracy and integrity of the applications;
- it accepts notifications from SK about Certificates issued by SK;
- it accepts notifications from SK about Certificates revoked by SK;
- it verifies the applicant's identity and his/her powers to carry out the operation in accordance with the effective legislation;
- it follows requirements described in this CPS in the information system (including its web-based application submission environment) that is related to the certification service;
- it follows availability and security requirements on its web-based application submission system at least to the level of the requirements described in this CPS;
- the employees, who are involved with information related to certification service, are not punished for intentional crime;
- it provides security with its internal security procedures.

9.6.2.2.3 Mobile Operator

MO ensures that:

- it follows availability and security requirements on the information system related to Mobile ID service at least to the level of the requirements described in this CPS;

- it provides security with its internal security procedures;
- the employees, who accept applications regarding QSCD and Certificates and/or are involved with information related to certification service, are not punished for intentional crime.

9.6.2.2.4 MO Customer Service Point

Refer to clause 9.6.2 of SK PS [2].

MO Customer Service Point ensures that:

- it accepts applications for QSCD issuance and replacement for valid Mobile ID (Certificate re-key);
- it accepts applications for termination of suspension of Mobile ID Certificates;
- it accepts applications for suspension and closure of the telecommunication service;
- it accepts applications for revocations of the Certificates and forwards them to SK;
- it forwards the applications for QSCD to SK and hands over QSCD to the Subscriber;
- it preserves signed applications for QSCD change and for replacement of QSCD for valid Mobile ID (Certificate re-key);
- it forwards the request for the Certificates in case of Certificate re-key to SK;
- it verifies accuracy and integrity of the listed applications;
- it verifies identity of the applicant and his/her powers to carry out the operation in accordance with the relevant legislation and internal security procedures;
- it provides security with its internal security procedures.

9.6.2.2.5 SK Customer Service Point

Refer to clause 9.6.2 of SK PS [2].

SK Customer Service Point ensures that:

- it accepts electronically signed applications of suspension and termination of suspension of Mobile ID Certificates;
- it provides security with its internal security procedures.

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

9.6.3. Subscriber Representations and Warranties

9.6.3.1. 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 and corresponding certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her private key in accordance with this CPS;
- he/she immediately informs SK of a possibility of unauthorised use of his/her private key and suspends or revokes his/her certificates;
- he/she immediately suspends or revokes his/her certificates if his/her private key has gone out of his/her possession;
- he/she is aware that Electronic Signatures given on the basis of expired, revoked or suspended certificates are invalid.

The Subscriber is not responsible for the acts performed during the suspension of certificates. In case the Subscriber terminates suspension of certificates, the Subscriber is solely and fully responsible for any consequences of Authentication and Electronic Signature using the certificates during the time when the certificates were suspended.

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

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

The Subscriber has to accept the Terms and Conditions [12].

9.6.3.2. Mobile 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 personal data to MO while submitting an application for QSCD or for change of QSCD;
- he/she presents true and correct personal data to PBGB while submitting an application for Mobile ID Certificates;
- he/she presents true and correct personal data to MO while submitting an application for replacement of QSCD (Certificate re-key) and confirms that the QSCD to be replaced has been issued to him/her;
- he/she notifies PBGB in case of change of personal data in accordance with the effective legislation;

- he/she notifies MO in case of Mobile ID becoming unusable, lost or destroyed in accordance with the effective legislation;
- he/she uses his/her private keys and corresponding certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her private key in accordance with this CPS;
- in case of a change in his/her personal details stored in the certificate he/she applies for a new QSCD and Mobile ID Certificates in order to continue usage of the Mobile ID service;
- 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 or the device has been stolen;
- he/she is aware that Electronic Signatures given on the basis of expired, revoked or suspended certificates are invalid.

The Subscriber is not responsible for the acts performed during the suspension of certificates. In case the Subscriber terminates suspension of certificates, the Subscriber is solely and fully responsible for any consequences of Authentication and Electronic Signature using the certificates during the time when the certificates were suspended.

If the Subscriber has a suspicion that Mobile ID has gone out of control of him/her at the time of suspension of the certificates and/or the telecommunication service, the Subscriber is obliged to revoke the certificates.

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

The Subscriber has to accept the Terms and Conditions [12].

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, the CP [4], CP for Digi-ID [5] and CP for Mobile ID [6].

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

A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CP [4], CP for Digi-ID [5] and CP for Mobile ID [6].

A Relying Party uses CRL service on its own responsibility.

9.6.5. Representations and Warranties of Other Participants

9.6.5.1. ID card and Digi-ID

9.6.5.1.1 Trüb Baltic AS

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

Trüb Baltic AS provides security with its internal security procedures.

9.6.5.2. Mobile ID

9.6.5.2.1 SIM-card Manufacturer

SCM is responsible for all operations and procedures regarding the production of QSCD, including secure key generation and loading as well as Public Key delivery to SK.

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 [12].

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 [12], before agreeing to and signing it.

The Subcriber'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 [9];
- State Fees Act [13];
- Personal Data Protection Act [14].

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://sk.ee/en/repository/sk-ps/;
3. Certificate, CRL and OCSP Profile for personal identification documents of the Republic of Estonia, published: https://sk.ee/en/repository/profiles/;
4. SK ID Solutions AS - Certificate Policy for ID card, published: https://sk.ee/en/repository/CP/;
5. SK ID Solutions AS – Certificate Policy for Digi-ID, published: https://sk.ee/en/repository/CP/;
6. SK ID Solutions AS - Certificate Policy for Mobile ID of the Republic of Estonia, published: https://sk.ee/en/repository/CP/;
7. 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;
8. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
9. Identity Documents Act, RT I 1999, 25, 365, published: https://www.riigiteataja.ee/en/eli/ee/511042016001/consolide/current;
10. 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;
11. ISO/IEC 7816, Parts 1-4, published: http://iso.org;
12. Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
13. State Fees Act, RT I, 30.12.2014, 1, published: https://www.riigiteataja.ee/en/eli/ee/511022015002/consolide/current;
14. Personal Data Protection Act, RT I 2007, 24, 127, published: https://www.riigiteataja.ee/en/eli/ee/507032016001/consolide/current;
15. Digidoc Service: https://sk.ee/en/services/validity-confirmation-services/digidoc-service/;
16. ID card documentation webpage: http://www.id.ee/index.php?id=35772;
17. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current.