AS Sertifitseerimiskeskus - NQ-SK Certification Practice Statement

Version 1.0

1.January 2017

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

1. Introduction

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

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

- "AS Sertifitseerimiskeskus Trust Services Practices Statement" [1] (hereinafter referred to as SK PS) describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Practice Statements describe parts that are specific to each Subordinate CA or Time-Stamping Unit;
- Technical Profiles are in separate documents.

Pursuant to the IETF RFC 3647 [2] this CPS is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [2], section headings that do not apply have the statement **"Not applicable"**. References to SK PS [1] and the "Certificate and OCSP Profile for Smart-ID" [3] (hereinafter referred to as Certificate Profile) documents are included where applicable.

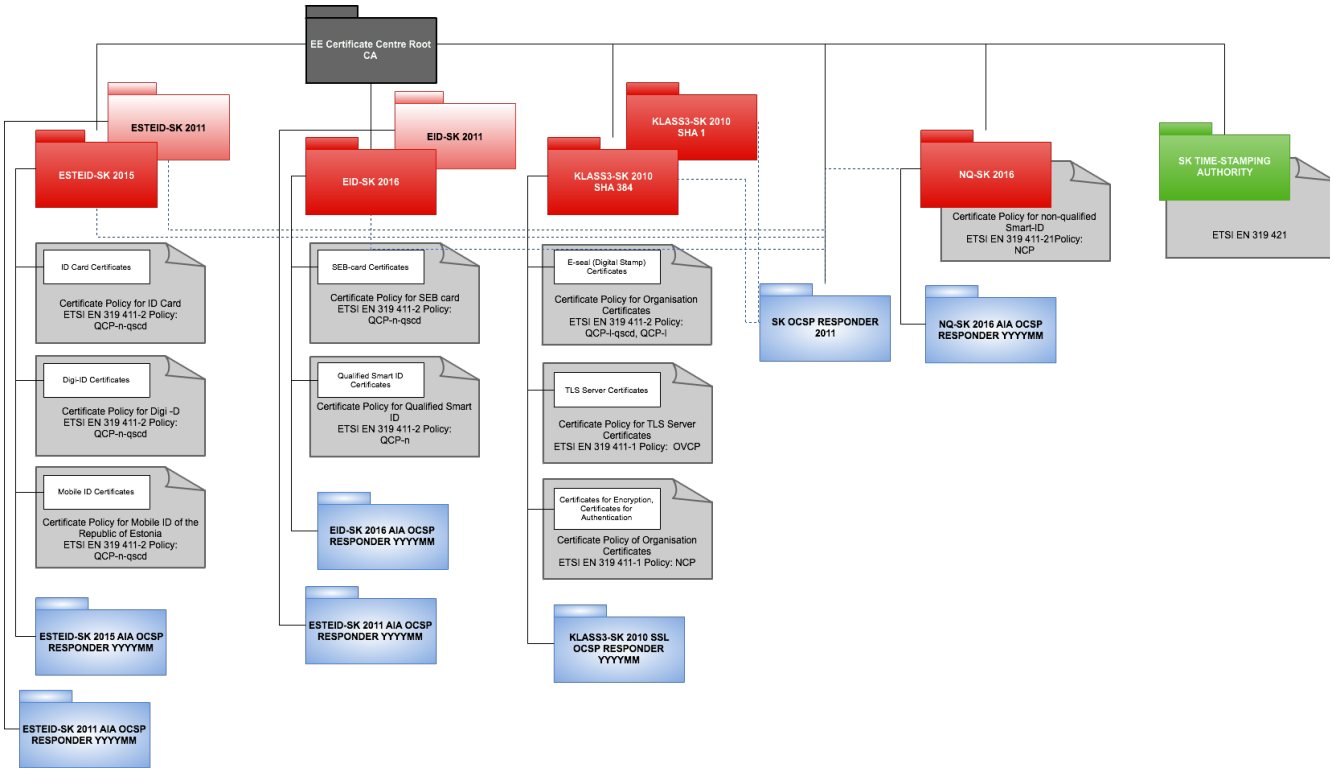
1.1. Overview

This CPS describes the practices used to comply with "AS Sertifitseerimiskeskus - Certificate Policy for non-qualified Smart-ID" [4] (hereinafter referred to as CP).

The policy is compliant with ETSI EN 319 411-1 Policy: NCP [5].

SK is currently using the following certificate chain:

EE Certification Centre Root CA chain, valid 2010-2030



This CPS covers operation of NQ-SK 2016.

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

- NCP;
- CP [4];
- This CPS.

1.2. Document Name and Identification

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

1.3. PKI Participants

1.3.1. Certification Authorities

SK operates as a Certification Authority that issues Certificates for the non-qualified Smart-ID (hereinafter referred to as NQ Smart-ID).

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 NQ-SK 2016 that is identified by the following certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            57:a9:f3:ec:a2:2f:0e:28:57:c5:4e:f5:61:36:e0:5a
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification
Centre Root CA/emailAddress=pki@sk.ee
        Validity
            Not Before: Aug 30 09:16:37 2016 GMT
            Not After : Dec 17 23:59:59 2030 GMT
        Subject: C=EE, O=AS
Sertifitseerimiskeskus/2.5.4.97=NTREE-10747013, CN=NQ-SK 2016
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:dd:91:14:4d:0f:17:ce:ea:82:94:f4:60:eb:18:
                    b3:50:73:8d:4f:03:ea:6a:0c:a0:84:70:38:52:c3:
                    56:e7:90:2f:e7:0e:e9:a0:e0:f6:b0:42:4f:31:92:
                    5c:83:1e:bd:92:86:bb:05:ad:3a:39:c2:9b:39:51:
                    c8:31:c5:33:2a:6f:df:1b:98:cc:50:62:08:6a:c6:
                    ee:4d:aa:aa:5a:66:8a:5b:6d:28:fe:a8:36:14:ce:
                    b6:64:5c:89:55:7b:e1:c5:a5:4b:79:71:ef:56:36:
                    91:26:79:e9:d5:02:5b:78:65:a3:75:fe:ca:c3:7e:
                    fd:cd:48:c9:9c:17:6a:fd:5e:25:08:22:10:da:bf:
                    14:3e:42:03:f2:dc:2a:e0:4f:42:5a:df:2c:3f:3c:
                    ba:45:fd:a8:c2:35:05:9a:19:62:47:62:48:0d:57:
                    3a:e7:ac:a8:4a:60:38:60:a2:b7:37:95:2a:86:7d:
                    37:e1:5b:65:df:e6:49:6f:05:9a:24:3d:f6:e1:0f:
                    6e:9c:b2:73:de:26:34:10:40:9d:8b:a2:8b:77:67:
                    df:d0:3f:37:d8:fd:09:ea:a7:98:63:92:f7:ea:8c:
                    a9:2c:5f:6c:00:b7:f5:01:f8:79:38:b1:11:be:e8:
                    da:9a:dd:bf:a0:c6:a3:1c:8a:1d:5e:23:f2:3d:dc:
                    88:ba:38:2e:cb:8a:38:4d:da:4d:11:f4:be:7e:02:
                    b8:10:5e:19:40:41:86:46:78:20:02:fe:e9:c7:9a:
                    90:a4:89:44:2b:10:9a:b6:ee:4b:2d:9b:3a:04:36:
                    7c:10:9c:5d:e6:86:af:35:29:01:99:ba:5f:c6:bb:
                    0d:5f:b1:03:a8:94:02:c4:48:45:86:e9:d4:cf:d6:
                    cc:da:2d:e6:da:e0:b6:0d:ef:4e:db:f6:9b:91:39:
                    55:e4:d5:62:e8:6a:ed:77:d4:a6:67:21:d7:3f:f8:
                    ab:6e:da:78:b8:49:52:f7:fa:a2:9b:27:bf:a8:a8:
                    87:e2:14:0a:a5:4a:e0:8f:4c:ab:2c:74:50:b8:f6:
                    6e:d5:1b:86:d7:9e:b6:1e:03:9b:2f:51:08:c2:be:
                    90:0d:9b:35:ea:46:ce:83:99:d7:2d:28:fb:97:52:
                    3f:96:fe:09:d0:36:82:ce:bc:81:24:2b:7d:13:0f:
                    f4:4a:77:87:a1:bb:3c:d8:8f:da:a2:ae:1a:81:0c:
                    58:3e:22:9a:a1:f4:e0:72:2b:b6:98:e9:ff:4a:67:
```

```
                    aa:8a:98:ab:6d:70:f6:f8:47:b6:ab:06:db:90:a0:
                    19:6a:69:d7:17:a0:68:a0:a3:f9:2b:fe:25:d5:45:
                    a6:d6:7c:65:4c:ef:78:90:a3:7e:91:66:b9:25:ad:
                    2b:b9:6b
                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:

7A:B7:85:5F:A1:F3:CC:41:B7:AE:E9:EA:06:51:0A:E0:F9:02:C8:AC
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: 0.4.0.2042.1.1
                  CPS: https://www.sk.ee/repositoorium/CPS

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen: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 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

            qcStatements:
                0.0...+.......0.......I..
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://www.sk.ee/repository/crls/eeccrca.crl

    Signature Algorithm: sha384WithRSAEncryption
        ae:e0:72:ec:10:10:69:2a:65:f0:6a:05:e9:16:49:84:1a:a4:
        ce:0b:f7:98:5a:bb:70:55:93:67:cf:f3:01:fb:3f:1c:e9:3c:
        b1:c1:6d:9c:0e:63:70:33:03:1f:a2:35:d3:e3:8e:eb:43:fc:
        65:6a:2f:f9:82:31:a4:47:04:44:f0:fe:56:f7:48:7f:26:43:
        b7:ad:45:86:e1:ab:2b:bc:f0:30:9a:42:22:50:7b:07:20:70:
        d5:1c:2b:12:9a:12:cd:12:03:dd:33:8c:cf:f3:cf:cb:12:65:
        7c:f5:92:2f:51:61:a3:cd:96:1c:80:19:63:61:e0:25:2b:87:
        42:cb:8f:fb:53:5e:09:5b:d1:42:c2:f1:63:14:ec:9f:0d:ca:
        68:63:0c:5b:57:b2:64:6e:1b:30:f4:9f:2e:cf:3c:63:b2:91:
        82:be:8a:b9:8b:37:93:1a:e4:55:f9:6b:55:fb:2c:ba:5b:f5:
        0e:9e:99:98:38:9e:a3:c7:35:28:62:ae:9f:9d:01:94:f8:9f:
        42:2d:5c:63:8c:4f:09:8f:6e:5f:b9:64:94:dc:1b:cf:b3:c7:
```

```
26:b3:b4:73:be:fb:99:bc:f8:10:5a:6f:08:66:de:8b:e4:fe:
84:1c:ec:de:11:1d:e6:de:77:ed:11:18:46:d8:e5:c4:f8:c1:
c9:fa:89:dc
```

1.3.2. Registration Authorities

1.3.2.1 Smart-ID Provider

Smart-ID Provider performs RA duties.

Refer to clause 1.3.5 of this CPS.

1.3.2.2 Customer Service Point

Servicing Certificates of NQ Smart-ID (revocations) is carried out in Customer Service Points.

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

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 NQ Smart-ID usage.

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

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

The Help Line may be contacted at 9001807 or 1807.

1.3.3. Subscribers

Refer to clause 1.3.3 of the CP [4].

1.3.4. Relying Parties

Relying Parties are legal persons who are making decisions based on the Certificate issued by SK.

Relying Party is a 3rd party, which uses services provided by the Smart-ID System to authenticate Subscribers and to allow Subscribers to electronically sign documents or transactions.

Relying Party validates the identity from NQ Smart-ID Certificate against personal information known by Identity Provider on first authentication of this Subscriber to its system.

1.3.5. Other Participants

1.3.5.1 Smart-ID Provider

Smart-ID Provider is an organisation that is legally responsible for the Smart-ID System. Smart-ID Provider offers solely authentication technology.

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

1.3.5.2 Identity Provider

Identity Provider is an organisation who is providing electronic authentication means and is responsible for creating electronic identities which are used for issuing NQ Smart-ID Certificates.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Refer to clause 1.4 of the CP [4].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS is administered by SK.

AS Sertifitseerimiskeskus

Registry code 10747013

Pärnu Ave 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@sk.ee

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

1.5.2. Contact Person

Business Development Manager

Email: info@sk.ee

1.5.3. Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4. CPS Approval Procedures

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

In case the CP is amended, the CPS is reviewed as well in order to verify the need for its amendments.

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

Amendments which are relevant to Identity Providers and RA are coordinated with Identity Providers and RA.

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

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CPS the following terms have the following meaning.

Term	Definition
Advanced Electronic Signature	Electronic Signature which meets the requirements provided in Article 26 of eIDAS [6].
Authentication	Unique identification of a person by checking his/her alleged identity.
Authentication Certificate	Certificate is intended for Authentication.
AS Sertifitseerimiskeskus Trust Services Practice Statement	A statement of practices that SK employs in providing Trust Services.

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 with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one 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.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed and used.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Distinguished Name	Subject name in the infrastructure of Certificates that is unique for every Subscriber.
Identity Provider	An organisation who is providing electronic authentication means and who is responsible for creating electronic identities which are used for issuing NQ Smart-ID Certificates. Identity Provider has been verified by Smart-ID Provider to follow the Requirements for Identity Providers [9] for non-qualified certificates.
Mobile Device	A tablet computer or smartphone that runs a mobile device operating system (Apple iOS, Google Android).
non-qualified Electronic Signature Certificate	An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name of that person.
NQ Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the non-qualified Electronic Signature Certificate and their corresponding Private Keys.
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for the Private Key that corresponds to Authentication Certificate and for the Private Key that corresponds to the 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.
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.
Relying Party	Entity that relies on the information contained within a Certificate.
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.
Smart-ID Account	Subscriber has to register a Smart-ID Account to use services provided by the Smart-ID System. Smart-ID Account binds Smart-ID Application instance to a Subscriber's identity in the Smart-ID System. In the course of Smart-ID Account creation and registration, the identity of the Smart-ID Account owner (Subscriber) is proofed by a Registration Authority and the relation between the identity and a key pair is certified by a Certificate Authority. Smart-ID Account has an Advanced Electronic Signature key and an Authentication key.
Smart-ID Application	A technical component of the Smart-ID system. A Smart-ID Application installed on a Subscriber's Mobile Device that provides access to non-qualified Smart-ID service.
Smart-ID Portal	The interaction point with the Smart-ID System for the Subscriber that is accessible via a web browser. The Portal provides access to Smart-ID Account registration and management functionality.
Smart-ID Provider	An organisation that is legally responsible for the Smart-ID system. SK is the Smart-ID provider.
Smart-ID Server	A technical component of the Smart-ID system, handles back-end operations.
Smart-ID System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The Smart-ID system provides services that allow Subscribers (Smart-ID Account owners) to authenticate themselves to services, to give Electronic Signatures, and to manage their Smart-ID Accounts.
Subject	In this document, the Subject is the same as the Subscriber.

Subscriber	A natural person to whom the NQ Smart-ID Certificates are issued.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon receipt of the Certificates.
UTF-8	Variable length character encoding which uses 8 bit code units capable of encoding all possible characters defined by Unicode.
Verified Electronic Authentication	Electronic Authentication based on Identity Provider that has been verified to follow the Requirements for Identity Providers [9] for non-qualified certificates.
Smart-ID HSM Module	The hardware security module used in the Smart-ID system. FIPS 140-2 Level 3 certified cryptographic device.

1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement. This document is a CPS.
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [6] 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.
HSM	Hardware security module is a physical computing device that safeguards and manages digital cryption keys and provides cryptoprocessing.
KWK	Key-wrap-keypair
KTK	Key-tranmission-keypair
NCP	Normalised Certificate Policy from ETSI EN 319 411-1 [5]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PKI	Public Key Infrastructure
RA	Registration Authority
SK	AS Sertifitseerimiskeskus, Certification Service provider
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement [1]

2. Publication and Repository Responsibilities

2.1. Repositories

Refer to clause 2.1 of SK PS [1].

2.2. Publication of Certification Information

Refer to clause 2.2 of SK PS [1].

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], the Certificate Profile [3] and the "Terms and Conditions for Use of Certificates of non-qualified Smart-ID" [7] (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].

Refer to clause 9.3.1 of SK PS [1].

2.3. Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.4. Access Controls on Repositories

Refer to clause 2.4 of SK PS [1].

3. Identification and Authentication

3.1. Naming

3.1.1. Type of Names

Type of names assigned to the Subscriber is described in the Certificate Profile [3].

3.1.2. Need for Names to be Meaningful

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

Meaning of names in different fields of the Certificates is described in the Certificate Profile [3].

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Subscriber names are encoded in UTF-8 format.

SK uses the name from the national population registry.

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) and Serial Number (S) fields to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Trademarks are not allowed.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

There is a single process flow that includes key generation, Certificate Request and issuance.

Both the Subscriber and Smart-ID Provider have to participate in the key generation procedure. The Certificate Request sent to CA includes a cryptographic signature created by the newly generated keys.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

SK receives the identity data from the Identity Provider and is entitled to validate it against the identity data from the national population registry.

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

The Subscriber can apply for NQ Smart-ID only personally. SK checks whether the applicant has legal capacity.

3.2.6. Criteria for Interoperation

Not applicable.

Operations of NQ-SK 2016 have not any effect to operations of other intermediate CA's of EE Certification Centre Root CA.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Refer to clause 3.2 of this CPS.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to clause 3.2 of this CPS.

3.4. Identification and Authentication for Revocation Request

Refer to clause 4.9.3 of this CPS.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

The Subscriber can enroll herself.

SK accepts only applications from the Subscriber who is previously authenticated by the Identity Provider.

4.1.2. Enrolment Process and Responsibilities

The Subscriber fills an application for NQ Smart-ID in the Smart-ID Application upon successful Verified Electronic Authentication. The Subscriber confirms the correctness and integrity of the information presented to SK.

The Subscriber confirms agreement to the Terms and Conditions.

The Subscriber can apply for NQ Smart-ID if he/she has legal capacity.

Smart-ID System validates the Subscriber's identity and forwards the application to SK.

SK archives the Subscriber's application.

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

SK verifies compliance of the data in the CSR with the data in national population registry and application. If the data contained in the CSR and application is identical, and if the data in the application and the national population registry substantially matches, SK generates Certificates corresponding to the registry.

SK sends Certificates to Smart-ID System.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber is identified and authenticated by the data presented by the Identity Provider, and if necessary by the data from the national population registry.

4.2.2. Approval or Rejection of Certificate Applications

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

SK refuses to issue a Certificate if:

- the Certificate request does not comply with the technical requirements set in applicable agreements;
- there is no matching application for the CSR;
- the Subscriber cannot be identified from the national population registry;
- the Subscriber's data in the application does not substantially match with the data in the national population registry;
- the Subscriber lacks legal capacity.

SK notifies RA and Subscriber of the refusal to issue a Certificate.

4.2.3. Time to Process Certificate Applications

Refer to clause 4.2.3 of the CP [4].

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

After verifying that the data contained in the CSR and application is identical, and that the data in the application and the national population registry substantially matches, SK automatically issues Certificates corresponding to the application.

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

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

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The Subscriber confirms Certificate issuance in Smart-ID Application.

Corresponding confirmation is deemed Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

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

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

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

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

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

- the CP [4];
- this CPS;
- the Terms and Conditions [7].

4.5.2. Relying Party Public Key and Certificate Usage

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

- the CP [4];
- this CPS;
- the Terms and Conditions [7].

4.6. Certificate Renewal

Renewal of Certificates is not allowed.

4.7. Certificate Re-Key

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

4.7.1. Circumstances for Certificate Re-Key

Certificate re-key is allowed to:

- fix errors during certification.

4.7.2. Who May Request Certification of a New Public Key

Certificate re-key process to fix errors during certification can only be initiated by SK.

4.7.3. Processing Certificate Re-Keying Requests

If the Certificate re-key is performed to fix production errors only Smart-ID Server's Private Key is generated pursuant to clause 6.1.1 of this CPS.

4.7.4. Notification of New Certificate Issuance to Subscriber

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

RA notifies the Subscriber of the new Certificate issuance.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to clause 4.4.1 of this CPS.

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

Refer to clause 4.4.2 of this CPS.

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

Refer to clause 4.4.3 of this CPS.

4.8. Certificate Modification

Certificate Modification is not allowed

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1 of the CP [4].

4.9.2. Who Can Request Revocation

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

RA can request revocation of the Subscriber's Certificates on the basis of Subscriber application.

CA can request revocation for any of the reasons listed in clause 4.9.1 of the CP [4].

4.9.3. Procedure for Revocation Request

The Subscriber can request revocation of NQ Smart-ID Certificates as follows.

The Subscriber can request revocation of NQ Smart-ID Certificates via the Help Line.

The operator of the Help Line verifies the Subscriber by using the identification data in the Subscriber's application. After the Subscriber's identity and legality to request revocation is verified, the operator of the Help Line revokes the NQ Smart-ID Certificates.

Revocation request submitted via the Help Line is recorded.

Alternatively, the Subscriber can request revocation of NQ Smart-ID via self-service web portal or Smart-ID Application, where the Subscriber is authenticated using Verified Electronic Authentication. The Subscriber has to confirm the application there.

The self-service web portal or Smart-ID Application sends the request for revocation to SK.

The Subscriber can also submit a signed application for revocation of the Certificates to the Customer Service Point.

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

- The revocation application is registered by an employee of the Customer Service Point;
- The person filing an application for revocation is verified;
- The compliance of the application for revocation with the CP [4] is verified in SK’s information system;
- The documentation on which the application for revocation was based is archived;
- The Subscriber is notified of revocation of the Certificates.

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 Smart-ID System that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

4.9.4. Revocation Request Grace Period

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 an application for revocation has been submitted, SK immediately processes an application for 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 [7].

4.9.7. CRL Issuance Frequency

CRL for NQ-SK 2016 is not issued.

4.9.8. Maximum Latency for CRLs

Not applicable.

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 [7].

4.9.11. Other Forms of Revocation Advertisements Available

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

4.9.12. Special Requirements Related to Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Suspension is not performed.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

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

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

4.10.2. Service Availability

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

4.10.3. Operational Features

None.

4.11. End of Subscription

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

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

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

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

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

Refer to clause 5.1 of SK PS [1].

5.2. Procedural Controls

Refer to clause 5.2 of SK PS [1].

5.3. Personnel Controls

Refer to clause 5.3 of SK PS [1].

5.4. Audit Logging Procedures

Refer to clause 5.4 of SK PS [1].

5.5. Records Archival

5.5.1. Types of Records Archived

Refer to clause 5.5.1 of SK PS [1].

All physical records from issuance process and from applications for 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 [1].

5.5.3. Protection of Archive

Refer to clause 5.5.3 of SK PS [1].

5.5.4. Archive Backup Procedures

Refer to clause 5.5.4 of SK PS [1].

5.5.5. Requirements for Time-Stamping of Records

Refer to clause 5.5.5 of SK PS [1].

5.5.6. Archive Collection System (Internal or External)

Refer to clause 5.5.6 of SK PS [1].

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 [1].

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. NQ-SK 2016).

5.7. Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [1].

5.8. CA or RA Termination

Refer to clause 5.8 of SK PS [1].

6. Technical Security Controls

6.1. Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [1].

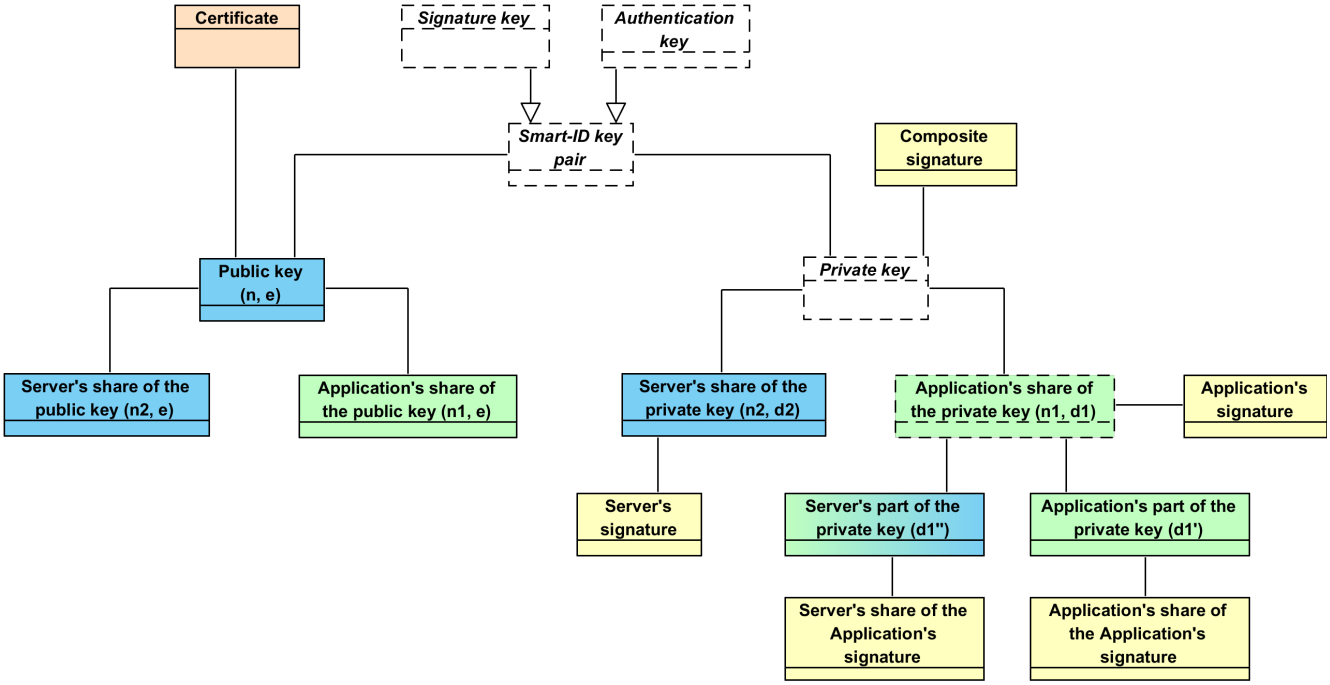
6.1.1. Key Pair Generation

Refer to clause 6.1.1 of SK PS [1].

Non-Qualified Smart-ID Key Pair Terminology

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

1. 'Public key' - is the public verification key in the public-key cryptography. This corresponds to the regular RSA public key. The relation between the 'Public key' and a 'Subscriber's Identity' is attested by a Certificate. Public key has the following components: 'Application's share of the public key' and 'Server's share of the public key'.
2. 'App's share of the public key' - is generated in the Smart-ID app, along with the generation of the 'App's share of the private key'.
3. 'Server's share of the public key' - is generated in the Smart-ID server, along with the generation of the 'Server's share of the private key'.
4. 'Private key' - is the confidential component of the key pair in the public-key cryptography. 'Private key' is used for creating digital signatures. In the Smart-ID System, the value of 'Private key' itself is never generated and the 'Private key' exists only in the form of it's components. 'Private key' has the following components:
    - 4.1 'App's share of the private key', which is a regular RSA private key. It is further divided to the following components:
        - 4.1.1 'App's part of the private key'
        - 4.1.2 'Server's part of the private key'
    - 4.2 'Server's share of the private key', which is a regular RSA private key.
5. 'Application's share of the private key' - is the component of the private key that is generated in the Smart-ID app. The share is divided into two parts immediately after generation and the share itself is deleted.
6. 'App's part of the private key' - is the component of the private key, which is generated in the Smart-ID app and stored in the Smart-ID app and is protected with the Subscriber's PIN-code.
7. 'Server's part of the private key' - is the component of the private key, which is generated in the Smart-ID app and securely transmitted to the server. 'Server's part of the private key' is stored in the server's database and protected with Key-Wrapping-Key inside the HSM.
8. 'Server's share of the private key' - is the component of the private key, which is generated in the HSM and stored inside the HSM.



Non-Qualified Smart-ID Key Pair Generation

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

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

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

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

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

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

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

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

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

Generation of Subscriber's 'Public key'

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

6.1.2. Private Key Delivery to Subscriber

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

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

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

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

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

1. The KTK is generated inside the Smart-ID HSM module. The KTK is 2048-bit RSA keypair.
2. The public key of the KTK is embedded in the binary distribution of the Smart-ID app.
3. The 'Server's part of the private key' is encoded and encrypted with the public key of the KTK (according to the RFC 7516) and transmitted to the Smart-ID server inside the TLS channel, for additional confidentiality and authenticity.

4. The Smart-ID server uses the HSM to decrypt the 'Server's part of the private key' and stores it securely in the database, wrapped with another long-term KWK. The KWK is generated and stored inside the Smart-ID HSM module.

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

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

6.1.3. Public Key Delivery to Certificate Issuer

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

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

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

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

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

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

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

6.1.4. CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [1].

6.1.5. Key Sizes

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

6.1.6. Public Key Parameters Generation and Quality Checking

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

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

Refer to clause 6.1.7 of SK PS [1].

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

Refer to clause 6.2.1 of SK PS [1].

Non-Qualified Smart-ID app cryptographic library standards

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

Non-Qualified Smart-ID server cryptographic library standards

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

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

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

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

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

The access to the KWK key, which protects the 'Server's part of the private key', is divided into two parts that are secured by different persons in Trusted Roles. For activation of the KWK key the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [1].

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

The access to the 'Server's share of the private key', is divided into two parts that are secured by different persons in Trusted Roles. For activation of the key, the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [1] .

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [1].

SK does not offer Key Escrow services to Subscribers.

6.2.4. Private Key Backup

Refer to clause 6.2.4 of SK PS [1].

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

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

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

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

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

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

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

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

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

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

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

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

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

6.2.5. Private Key Archival

Refer to clause 6.2.5 of SK PS [1].

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

6.2.6. Private Key Transfer Into or From a Cryptographic Module

Refer to clause 6.2.6 of SK PS [1].

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

6.2.7. Private Key Storage on Cryptographic Module

Refer to clause 6.2.7 of SK PS [1].

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

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

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

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

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

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

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

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

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

6.2.8. Method of Activating Private Key

Refer to clause 6.2.8 of SK PS [1].

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

Activating 'App's part of the private key'

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

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

The following rules apply:

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

.

Activating 'Server's part of the private key'

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

Activating 'Server's share of the private key'

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

6.2.9. Method of Deactivating Private Key

Refer to clause 6.2.9 of SK PS [1].

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

Deactivating 'App's part of the private key'

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

Deactivating 'Server's part of the private key'

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

Deactivating 'Server's share of the private key'

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

6.2.10. Method of Destroying Private Key

Refer to clause 6.2.10 of SK PS [1].

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

Destroying 'App's part of the private key'

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

Destroying 'Server's part of the private key'

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

Destroying 'Server's share of the private key'

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

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to clause 6.3.1 of SK PS [1].

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 [1].

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 [1].

The initial activation data is generated by the Smart-ID Application or chosen by the Subscriber.

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

6.4.2. Activation Data Protection

Refer to clause 6.4.2 of SK PS [1].

The initial activation data is generated by the Smart-ID Application or chosen by the Subscriber. After that, activation codes themselves are never stored by the Smart-ID Provider nor in the Smart-ID Application.

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

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Refer to clause 6.5.1 of SK PS [1].

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 [1].

Subscriber is responsible for applying reasonable protections on her device.

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [1].

Subscriber is responsible for applying reasonable protections on her device.

6.7. Network Security Controls

Refer to clause 6.7 of SK PS [1].

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

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

Subscriber is responsible for applying reasonable protections on her device.

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [1].

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 for NQ Smart-ID Certificates is not issued.

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 [1].

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Certificate issuance for the Subscriber is free of charge.

Certificate renewal is not performed.

9.1.2. Certificate Access Fees

Valid and activated Certificates are available via OCSP service.

There are no public records about the Certificates.

9.1.3. Revocation or Status Information Access Fees

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

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

9.1.4. Fees for Other Services

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

9.1.5. Refund Policy

Refer to clause 9.1.5 of SK PS [1].

Financial settlements are considered business secret of Identity Provider and SK.

9.2. Financial Responsibility

SK is not financially liable for the information contained in NQ Smart-ID Certificates.

9.2.1. Insurance Coverage

Refer to clause 9.2.1 of SK PS [1].

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 [1].

9.3. Confidentiality of Business Information

Refer to clause 9.3 of SK PS [1].

9.4. Privacy of Personal Information

Refer to clause 9.4 of SK PS [1].

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CPS.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Refer to clause 9.6.1 of SK PS [1].

SK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- the supply of the certification service is in accordance with this CPS and the CP [4];
- it keeps account of the certificates issued by it and of their validity;
- it 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.

If SK has withdrawn Identity Provider status, SK is entitled to revoke all the Certificates issued for identities provided by this Identity Provider.

9.6.2. RA Representations and Warranties

9.6.2.1 Smart-ID Provider

Smart-ID Provider ensures that:

- it accepts Subscriber applications for issuance of NQ Smart-ID Certificates;
- it provides self-service web portal in accordance with the technical requirements set in applicable agreements.

9.6.2.2 Customer Service Point

Refer to clause 9.6.2 of SK PS [1].

The Customer Service Point ensures that:

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

9.6.2.3 Help Line

Refer to clause 9.6.2 of SK PS [1].

The Help Line ensures that:

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

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

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

9.6.3. Subscriber Representations and Warranties

Refer to clause 9.6.3 of SK PS [1].

The Subscriber ensures that:

- he/she adheres to the requirements provided by SK in this CPS;
- he/she presents true and correct information to Smart-ID System;
- in case of a change in his/her personal details, he/she notifies Smart-ID Provider of the correct details during a reasonable time;
- he/she uses his/her private keys and corresponding certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her private key in accordance with this CPS;
- he/she immediately informs SK of a possibility of unauthorised use of his/her private key and revokes his/her certificates;
- he/she immediately revokes his/her certificates if his/her private key has gone out of his/her possession;
- he/she immediately revokes his/her certificates or applies for new NQ Smart-ID if his/her PIN codes have gone out of his/her control;
- he/she is aware that Electronic Signatures given on the basis of expired or revoked certificates are invalid.

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

The Subscriber has to accept the Terms and Conditions [7].

9.6.4. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [1].

A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in this CPS and the CP [4].

If not enough evidence is enclosed to the Certificate or 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 an Electronic Signature.

A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CP [4].

A Relying Party validates the identity from NQ Smart-ID Certificate against personal information known by Relying Party on first authentication of this Subscriber to it's system.

A Relying Party is obliged not to create any new identities relying solely on the information from NQ Smart-ID Certificates.

A Relying Party is obliged to start changing the Subscriber's name in its database if the name in the Certificate and Identity Provider's database does not match.

9.6.5. Representations and Warranties of Other Participants

9.6.5.1 Smart-ID Provider

Smart-ID Provider ensures that:

- it adheres to the key generation and storage procedures under its control and described in this CPS;
- it adheres to provisions of fees described in this CPS;
- it transfers the correct Certificate and correct Certificate status information;
- before giving out Identity Provider status to an entity, the identity quality level of that entity is evaluated by verifying that the entity follows Requirements for Identity Providers [9] for non-qualified certificates.

Smart-ID Provider is entitled to withdraw Identity Provider status if it obtains evidence that Requirements for Identity Providers [9] for non-qualified certificates are not followed by Identity Provider.

9.6.5.2. Identity Provider

Identity Provider ensures compliance with the Requirements for Identity Providers [9] for non-qualified certificates.

9.7. Disclaimers of Warranties

Refer to clause 9.7 of SK PS [1].

9.8. Limitations of Liability

Refer to clause 9.8 of SK PS [1].

9.9. Indemnities

Indemnities between the Subscriber and SK are regulated in the Terms and Conditions [7].

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 [1].

9.10.3. Effect of Termination and Survival

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

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

terminates.

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

9.11. Individual Notices and Communications with Participants

The Subscriber is granted a right to get familiarized with the Terms and Conditions [7], before agreeing to and signing it.

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

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to clause 1.5.4 of this CPS.

9.12.2. Notification Mechanism and Period

Refer to clause 2.2.1 of this CPS.

9.12.3. Circumstances Under Which OID Must be Changed

Not applicable.

9.13. Dispute Resolution Provisions

Refer to clause 9.13 of SK PS [1].

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 [1].

Additionally, SK ensures compliance with the Personal Data Protection Act [8].

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 [1].

9.17. Other Provisions

Not applicable.

10. References

1. AS Sertifitseerimiskeskus Trust Services Practice Statement, published: https://sk.ee/en/repository/sk-ps/;
2. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
3. Certificate and OCSP Profile for Smart-ID, published: https://sk.ee/en/repository/profiles/;
4. AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID, published: https://sk.ee/en/repository/CP/;
5. ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
6. 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;
7. Terms and Conditions for Use of Certificates of non-qualified Smart-ID, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
8. Personal Data Protection Act, RT I 2007, 24, 127, published: https://www.riigiteataja.ee/en/eli/ee/507032016001/consolide/current;
9. Requirements for Identity Providers, published: https://sk.ee/en/services/smartid.