# AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID

Version 1.0

OID: 1.3.6.1.4.1.10015.17.1

Effective since 01.01.2017

| Version History | | |
|---|---|---|
| **Date** | **Version** | **Changes** |
| 1 January 2017 | 1.0 | First public edition. |

# 1. Introduction

## 1.1. Overview

This document, named "AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID" (hereinafter referred to as CP), defines procedural and operational requirements that Sertifitseerimiskeskus (hereinafter referred to as SK) adheres to and requires entities to adhere to when issuing and managing Certificates for the non-qualified Smart-ID (hereinafter referred to as NQ Smart-ID). These Certificates facilitate electronic signatures and electronic authentication of natural persons. Each NQ Smart-ID contains one pair of Certificates consisting of the Authentication Certificate and the non-qualified Electronic Signature Certificate and their corresponding Private Keys. Each Private Key is protected by separate activation data (PIN code).

Smart-ID is the new generation electronic identity, which provides the Subscriber with the means for Electronic Authentication and Electronic Signature. It can be used with a modern smartphone or a tablet device, no SIM-cards or card-readers are required. A Subscriber may apply for a NQ Smart-ID Account online using an Electronic Authentication method, such as authentication services provided by the Identity Providers. A Subscriber can have several active Smart-ID Accounts. Every mobile device owned by the Subscriber may be related to only one Smart-ID Account, which contains a Certificate Pair. The Subscriber can keep track of Smart-ID Accounts using a self-service Smart-ID Portal.

Issuing and managing Certificates for NQ Smart-ID is based on Regulation (EU) N° 910/2014 [6] which establishes a legal framework for electronic signatures.

**This document describes only restrictions to the Normalised Certificate Policy (NCP) from ETSI EN 319 411-1 [3].**

**The semantics of “no stipulation” in this document means that no additional restrictions are set and relevant provisions from NCP are applied directly.**

Issuing and managing Certificates for Authentication and Certificates for Electronic Signatures for NQ Smart-ID is based on the requirements of the Policy NCP: Normalised Certificate Policy.

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

- NCP,
- this CP,
- CPS.

To preserve IETF RFC 3647 [2] outline, this CP is divided into nine parts, section headings that do not apply, are designated as **"Not applicable"**. Each top-level chapter includes references to the relevant sections in ETSI EN 319 411-1 [3].

In this CP modal verbs in capital letters are to be interpreted as described in Clause 3.2 of the ETSI Drafting Rules [5] (Verbal forms for the expression of provisions).

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

## 1.2. Document Name and Identification

Refer to Clause 5.3 of ETSI EN 319 411-1 [3].

This document is named “AS Sertifitseerimiskeskus – Certificate Policy for non-qualified Smart-ID".

This CP is identified by OID: 1.3.6.1.4.1.10015.17.1

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

| Parameter | OID reference |
|---|---|
| Internet attribute | 1.3.6.1 |
| Private entity attribute | 4 |
| Registered business attribute given by private business manager IANA | 1 |
| SK attribute in IANA register | 10015 |
| Certification service attribute | 17.1 |

Certificates for Authentication and Certificates for Electronic Signature for NQ Smart-ID issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [3] clause 5.3 a) for NCP: 0.4.0.2042.1.1

  itu-t(0) identified-organization(4) etsi(0)

  other-certificate-policies(2042)

  policy-identifiers(1) ncp (1)
- This CP.

## 1.3. PKI Participants

Refer to Clause 5.4 of ETSI EN 319 411-1 [3].

### 1.3.1. Certification Authorities

No stipulation.

### 1.3.2. Registration Authorities

Smart-ID Provider performs RA duties.

### 1.3.3. Subscribers

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

Subscriber CAN be only a natural person.

### 1.3.4. Relying Parties

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

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 SHALL validate the identity from NQ Smart-ID Certificate against personal information known by relying party on first authentication of this Subscriber to its system. Relying party SHALL NOT create any new identities relying solely on information from NQ Smart-ID Certificates.

### 1.3.5. Other Participants

Smart-ID Provider is an organisation that is legally responsible for the Smart-ID system. Smart-ID Provider offers authentication technology only and based on the information provided by Smart-ID Provider new identity SHALL NOT be created.

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.

Identity Provider is 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.

## 1.4. Certificate Usage

Refer to Clause 5.5 of ETSI EN 319 411-1 [3].

### 1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Certificate for Electronic Signature is intended for:

- creating Advanced Electronic Signatures compliant with eIDAS [6].

Authentication Certificate is intended for:

- Authentication.

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

- Subscriber Certificates compliant with NCP,
- OCSP response verification Certificates,
- Internal Certificates for technical needs.

### 1.4.2. Prohibited Certificate Uses

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

- unlawful activity (including cyber attacks and attempt to infringe the Certificate or the NQ Smart-ID),
- issuance of new Certificates and information regarding Certificate validity,

- enabling other parties to use the Subscriber’s Private Key,

- enabling the Certificate issued for electronic signing to be used in an automated way,

- using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

The Subscriber Authentication Certificate SHALL NOT be used to create Advanced Electronic Signatures compliant with eIDAS [6].

## 1.5. Policy Administration

### 1.5.1. Organization Administering the Document

This CP 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

No stipulation.

### 1.5.4. CPS Approval Procedures

Amendments which do not change the meaning of this CP, such as spelling corrections, translation activities and contact details updates, SHALL be documented in the Versions and Changes section of this document.

In this case the fractional part of the document version number SHALL be enlarged.

In the case of substantial changes, the new CP version SHALL be clearly distinguishable from the previous ones, and the serial number SHALL be enlarged by one.

The amended CP along with the enforcement date, which cannot be earlier than 30 days after publication, SHALL be published electronically on SK website.

Amendments which are relevant to Identity Provider and RA SHALL be coordinated with Identity Provider and RA.

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

## 1.6. Definitions and Acronyms

### 1.6.1. Terminology

In this CP 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. |
| Certificate | Public Key, together with additional information, laid down in the Certificate Profile [4], 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 [12] 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.<br>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 [11] 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 [12] for non-qualified certificates. |

### 1.6.2. Acronyms

| Acronym | Definition |
|---|---|
| CA | Certification Authority |
| CP | Certificate Policy. This document is a CP. |
| CPS | Certification Practice Statement |
| 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. |
| NCP | Normalised Certificate Policy from ETSI EN 319 411-1 [3] |
| 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 |

# 2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [3].

## 2.1. Repositories

SK SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0,5% annually.

## 2.2. Publication of Certification Information

### 2.2.1. Publication and Notification Policies

This CP, the Certification Practice Statement [1], the Certificate Profile [4], as well as the Terms and Conditions [11] together with the enforcement dates SHALL be published on SK website https://sk.ee/en/repository/ no less than 30 days prior to taking effect.

### 2.2.2. Items not Published in the Certification Practice Statement

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

## 2.3. Time or Frequency of Publication

No stipulation.

### 2.3.1. Directory Service

Not applicable.

## 2.4. Access Controls on Repositories

No stipulation.

# 3. Identification and Authentication

Refer to Clause 6.2 of ETSI EN 319 411-1 [3].

## 3.1. Naming

The Distinguished Name of the Subscriber SHALL comply with conventions set in the Certificate Profile [4].

### 3.1.1. Type of Names

No stipulation.

### 3.1.2. Need for Names to be Meaningful

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

### 3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

### 3.1.4. Rules for Interpreting Various Name Forms

International letters SHALL be encoded in UTF-8.

### 3.1.5. Uniqueness of Names

SK SHALL ensure that Certificates with matching Common Name (CN) and SerialNumber fields are not issued to different Subscribers.

### 3.1.6. Recognition, Authentication, and Role of Trademarks

Not applicable.

## 3.2. Initial Identity Validation

### 3.2.1. Method to Prove Possession of Private Key

CSR SHALL be signed with the key, for which the Certificate has been requested.

### 3.2.2. Authentication of Organization Identity

Not applicable.

### 3.2.3. Authentication of Individual Identity

RA SHALL perform Subscriber Authentication using electronic authentication means prior to requesting issuance of the Subscriber's Certificates from the CA.

Authentication SHALL be carried out by RA by means of Verified Electronic Authentication.

### 3.2.4. Non-Verified Subscriber Information

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

### 3.2.5. Validation of Authority

The Subscriber SHALL apply for NQ Smart-ID only personally.

Applying for NQ Smart-ID through a representative SHALL BE prohibited.

### 3.2.6. Criteria for Interoperation

No stipulation.

## 3.3. Identification and Authentication for Re-Key Requests

### 3.3.1. Identification and Authentication for Routine Re-Key

Subscriber SHALL be identified electronically using the valid Verified Electronic Authentication method.

### 3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to Clause 3.2 of this CP.

## 3.4. Identification and Authentication for Revocation Request

No stipulation.

# 4. Certificate Life-Cycle Operational Requirements

Refer to Clause 6.3 of ETSI EN 319 411-1 [3].

## 4.1. Certificate Application

### 4.1.1. Who Can Submit a Certificate Application

Certificate application MAY be submitted by the Subscriber via RA.

SK SHALL accept certificate applications only from RA.

The Certificate application process SHALL ensure that the Subject has possession or control of the Private Key associated with the Public

Key presented for certification.

### 4.1.2. Enrolment Process and Responsibilities

Subscriber SHALL request for Certificates in the Smart-ID Application upon successful Verified Electronic Authentication.

RA SHALL perform Subscriber Authentication.

## 4.2. Certificate Application Processing

### 4.2.1. Performing Identification and Authentication Functions

The Subscriber's identity WILL be validated by RA by means of Verified Electronic Authentication.

Upon successful Authentication, the Subscriber SHALL accept the Terms and Conditions [11].

RA SHALL submit a request for the NQ Smart-ID Certificate issuance to the CA.

CA SHALL accept requests only from RA.

CA CAN check the identification data provided by RA against national population registry.

### 4.2.2. Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate if the Certificate request does not comply with the technical requirements set in the applicable agreements.

CA SHALL refuse to issue a Certificate if the Subscriber's data in Certificate request does not match substantially with the data from national population registry.

If the data contained in a Certificate request needs to be modified, the corresponding amendment SHALL be coordinated with RA.

If the CA refuses to issue a Certificate, RA and Subscriber SHALL be notified.

### 4.2.3. Time to Process Certificate Applications

In accordance with the applicable agreements.

## 4.3. Certificate Issuance

### 4.3.1. CA Actions During Certificate Issuance

After the Subscriber has accepted the Certificate, OCSP SHALL start responding with "GOOD" and the Certificate SHALL be made available via the Smart-ID System.

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

CA SHALL notify RA of the new Certificate issuance to the Subscriber.

RA SHALL notify the Subscriber of the new Certificate issuance.

## 4.4. Certificate Acceptance

### 4.4.1. Conduct Constituting Certificate Acceptance

Smart-ID Application SHALL notify the Subscriber of Certificate issuance.

Subscriber SHALL confirm the issued Certificate.

This confirmation SHALL be treated as Certificate acceptance.

### 4.4.2. Publication of the Certificate by the CA

Certificate SHALL be published by the CA immediately after the Subscriber has accepted it, OCSP SHALL start responding with "GOOD" and the Certificate SHALL be made available via the Smart-ID System.

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

No stipulation.

## 4.5. Key Pair and Certificate Usage

### 4.5.1. Subscriber Private Key and Certificate Usage

No stipulation.

### 4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

## 4.6. Certificate Renewal

Not allowed.

## 4.7. Certificate Re-Key

Re-key is any repeated application for NQ Smart-ID, if the Subscriber has a Smart-ID account.

Repeated application for NQ Smart-ID is processed same as the initial application for NQ Smart-ID.

Certificate re-key SHALL be allowed also in the case of errors during certification.

### 4.7.1. Circumstances for Certificate Re-Key

If a Subscriber has had a Smart-ID previously, the Subscriber MAY apply for Certificate Re-Key.

Certificate re-key SHALL BE allowed also for fixing invalid Certificates that do not comply with the Certificate Profile [4].

### 4.7.2. Who May Request Certification of a New Public Key

Subscriber together with RA CAN initiate the re-key process.

In case fixing invalid Certificates re-key MAY be performed by the CA internally.

SK SHALL NOT accept re-key requests from other parties except for the RA.

### 4.7.3. Processing Certificate Re-Keying Requests

The Certificate re-key process is as follows:

- RA SHALL Authenticate the Subscriber as stated in Clause 3.3.1 of this CP,
- Upon successful Authentication, the Subscriber SHALL accept the Terms and Conditions [11],
- Smart-ID Server's and Smart-ID Application's Private Keys are generated as described in Clause 6.1.1 of this CP,
- RA SHALL apply for Certification at the CA on behalf of the Subscriber by sending a CSR to the CA,
- CA SHALL sign the Public Keys and OCSP SHALL start responding with "GOOD" and the Certificate SHALL be made available via the Smart-ID System.

In case fixing invalid Certificates only Smart-ID Server's Private Key is generated as described in Clause 6.1.1 of this CP.

### 4.7.4. Notification of New Certificate Issuance to Subscriber

CA SHALL notify RA of the new Certificate issuance to the Subscriber.

RA SHALL notify 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 CP.

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

Refer to Clause 4.4.2 of this CP.

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

Refer to Clause 4.4.3 of this CP.

## 4.8. Certificate Modification

Not allowed.

## 4.9. Certificate Revocation and Suspension

### 4.9.1. Circumstances for Revocation

If the Subscriber loses control over one or more of the keys or PIN codes, the Subscriber SHALL apply for Certificate revocation immediately.

SK has the right to revoke NQ Smart-ID Certificates if one or more of the following occurs:

- the Subscriber requests revocation of the Certificates using the Smart-ID application or Smart-ID Portal or using for identification the RA ;
- the Subscriber has blocked the PIN codes;
- SK obtains evidence that Subscriber has lost control over Private Keys or PIN codes;
- the Subscriber notifies SK that the original Certificate request was not authorised and does not retroactively grant authorisation;
- SK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- SK obtains evidence that the Certificate was misused;
- SK is made aware that a Subscriber has violated one or more of its obligations under the Terms and Conditions [11];
- SK is made aware of a material change in the information contained in the Certificate;
- SK is made aware that the Certificate was not issued in accordance with the CPS and/or CP;
- SK determines that any of the information appearing in the Certificate is inaccurate or misleading;
- SK ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- SK's right to issue Certificates is revoked or terminated, unless SK has made arrangements to continue maintaining the OCSP repository;
- SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate;
- revocation is required by the CP;
- the technical content or format of the Certificate presents an unacceptable risk to Relying Parties;
- In case SK has withdrawn Identity Provider status, SK has the right to revoke all the Certificates which were issued for identities provided by this Identity Provider.

In the case of Certificate re-key the erroneous Certificate SHALL BE revoked.

If the new Certificates are issued for an existing Smart-ID account, old Certificates SHALL BE revoked.

### 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 this CP.

### 4.9.3. Procedure for Revocation Request

Certificate revocation SHALL apply to all the Certificates related to the Subscriber's Smart-ID Account.

If one of the Certificates needs to be revoked, all the Certificates of the same Smart-ID Account SHALL BE revoked.

In the case of a Smart-ID repeal, all related Certificates SHALL BE revoked.

### 4.9.4. Revocation Request Grace Period

No stipulation.

### 4.9.5. Time Within Which CA Must Process the Revocation Request

No stipulation.

### 4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation.

### 4.9.7. CRL Issuance Frequency

Not applicable.

### 4.9.8. Maximum Latency for CRLs

Not applicable.

### 4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

### 4.9.10. On-Line Revocation Checking Requirements

No stipulation.

### 4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

### 4.9.12. Special Requirements Related to Key Compromise

No stipulation.

### 4.9.13. Circumstances for Suspension

Not allowed.

### 4.9.14. Who Can Request Suspension

Not applicable.

### 4.9.15. Procedure for Suspension Request

Not applicable.

### 4.9.16. Limits on Suspension Period

Not applicable.

### 4.9.17. Circumstances for Termination of Suspension

Not applicable.

### 4.9.18. Who Can Request Termination of Suspension

Not applicable.

### 4.9.19. Procedure for Termination of Suspension

Not applicable.

## 4.10. Certificate Status Services

### 4.10.1. Operational Characteristics

No stipulation.

### 4.10.2. Service Availability

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

### 4.10.3. Operational Features

No stipulation.

## 4.11. End of Subscription

No stipulation.

## 4.12. Key Escrow and Recovery

### 4.12.1. Key Escrow and Recovery Policy and Practices

Not allowed.

### 4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

# 5. Facility, Management, and Operational Controls

Refer to Clause 6.4 of ETSI EN 319 411-1 [3].

# 6. Technical Security Controls

Refer to Clause 6.5 of ETSI EN 319 411-1 [3].

## 6.1. Key Pair Generation and Installation

### 6.1.1. Key Pair Generation

- Smart-ID Server and Smart-ID application SHALL generate RSA key pairs independently.

- Smart-ID Server's Private Key SHALL be generated on a FIPS 140-2 Level 3 certified HSM.

- Smart-ID Application SHALL further divide its Private Key into two parts. The two parts SHALL NOT BE distinguished from random numbers.

- Smart-ID Application SHALL send one of these parts to the Smart-ID Server over a secure communication channel.

- Smart-ID Application SHALL NOT store the key part sent to the Smart-ID Server, and SHALL store the other part encrypted with Activation Data.

### 6.1.2. Private Key Delivery to Subscriber

Not applicable.

### 6.1.3. Public Key Delivery to Certificate Issuer

The Smart-ID Provider SHALL deliver the Public Key to the CA using a secure communication channel.

### 6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

### 6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [4].

### 6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

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

Allowed key usage flags SHALL be set as described in the Certificate Profile [4].

## 6.2. Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1. Cryptographic Module Standards and Controls

The HSM module used to generate Smart-ID Server's Private Keys SHALL be certified with FIPS 140-2 Level 3 standard.

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

No stipulation.

### 6.2.3. Private Key Escrow

No stipulation.

### 6.2.4. Private Key Backup

No stipulation.

### 6.2.5. Private Key Archival

No stipulation.

### 6.2.6. Private Key Transfer Into or From a Cryptographic Module

No stipulation.

### 6.2.7. Private Key Storage on Cryptographic Module

No stipulation.

### 6.2.8. Method of Activating Private Key

Each of the Smart-ID Certificates SHALL be protected with its PIN code.

The Subscriber SHALL be prompted to enter the PIN code of the Authentication Certificate before any single operation done with the Private Key used for Authentication.

The Subscriber SHALL be prompted to enter the PIN code of the Electronic Signature Certificate before any single operation done with the Private Key used for electronic signing.

It SHALL NOT be possible to try all possible PIN codes sequentially.

It SHALL be possible to create different PIN codes for the keys with different intended purposes - e.g. it SHALL be possible to create different PIN codes for the keys of the Authentication and Electronic Signature Certificates, correspondingly.

The length of the PIN codes SHALL be at least:

- for the Authentication Key 4 numbers;
- for the Signature Key 5 numbers.

### 6.2.9. Method of Deactivating Private Key

No stipulation.

### 6.2.10. Method of Destroying Private Key

No stipulation.

### 6.2.11. Cryptographic Module Rating

No stipulation.

## 6.3. Other Aspects of Key Pair Management

### 6.3.1. Public Key Archival

No stipulation.

### 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The validity period of the Subscriber Certificates SHALL NOT exceed the validity period stated in the Certificate Profile [4].

## 6.4. Activation Data

### 6.4.1. Activation Data Generation and Installation

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

PIN codes SHALL NOT be stored by the Smart-ID Provider nor by the Smart-ID Application.

### 6.4.2. Activation Data Protection

The Subscriber SHALL memorise the PIN codes and not share them with anyone else.

PIN codes SHALL NOT be stored by the Smart-ID Provider nor by the Smart-ID Application.

If the PIN codes are not under the control of the Subscriber, the Subscriber SHALL apply for a new NQ Smart-ID or apply for Certificate revocation immediately.

### 6.4.3. Other Aspects of Activation Data

No stipulation.

## 6.5. Computer Security Controls

### 6.5.1. Specific Computer Security Technical Requirements

No stipulation.

### 6.5.2. Computer Security Rating

No stipulation.

## 6.6. Life Cycle Technical Controls

### 6.6.1. System Development Controls

No stipulation.

### 6.6.2. Security Management Controls

No stipulation.

### 6.6.3. Life Cycle Security Controls

No stipulation.

## 6.7. Network Security Controls

No stipulation.

## 6.8. Time-Stamping

No stipulation.

# 7. Certificate, CRL, and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1 [3].

## 7.1. Certificate Profile

The Certificate SHALL comply with the profile described in the Certificate Profile [4].

## 7.2. CRL Profile

Not applicable.

## 7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [4].

# 8. Compliance Audit and Other Assessments

Not applicable.

# 9. Other Business and Legal Matters

Refer to Clause 6.8 of ETSI EN 319 411-1 [3]

## 9.1. Fees

### 9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

### 9.1.2. Certificate Access Fees

No stipulation.

### 9.1.3. Revocation or Status Information Access Fees

No stipulation.

### 9.1.4. Fees for Other Services

No stipulation.

### 9.1.5. Refund Policy

No stipulation.

## 9.2. Financial Responsibility

### 9.2.1. Insurance Coverage

No stipulation.

### 9.2.2. Other Assets

No stipulation.

### 9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

## 9.3. Confidentiality of Business Information

No stipulation.

## 9.4. Privacy of Personal Information

### 9.4.1. Privacy Plan

No stipulation.

### 9.4.2. Information Treated as Private

No stipulation.

### 9.4.3. Information Not Deemed Private

No stipulation.

### 9.4.4. Responsibility to Protect Private Information

No stipulation.

### 9.4.5. Notice and Consent to Use Private Information

No stipulation.

### 9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

### 9.4.7. Other Information Disclosure Circumstances

No stipulation.

## 9.5. Intellectual Property rights

SK obtains intellectual property rights to this CP.

## 9.6. Representations and Warranties

### 9.6.1. CA Representations and Warranties

CA is not responsible for the identity of the Subscriber.

### 9.6.2. RA Representations and Warranties

No stipulation.

### 9.6.3. Subscriber Representations and Warranties

No stipulation.

### 9.6.4. Relying Party Representations and Warranties

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

Relying Party SHALL validate the identity from NQ Smart-ID Certificate against personal information known by relying party on first authentication of this Subscriber to it's system. Relying party SHALL NOT create any new identities relying solely on the information from NQ Smart-ID Certificates.

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

### 9.6.5. Representations and Warranties of Other Participants

Before giving out Identity Provider status to entity, Smart-ID Provider SHALL evaluate the identity quality level of the entity by verifying that th is entity is following Requirements for Identity Providers [12] for non-qualified certificates.

In case Smart-ID Provider obtains evidence that Identity Provider has not been following Requirements for Identity Providers [12] for non-qualified certificates it CAN withdraw Identity Provider status of this entity.

Identity Provider SHALL follow the Requirements for Identity Providers [12] for non-qualified certificates.

## 9.7. Disclaimers of Warranties

No stipulation.

## 9.8. Limitations of Liability

No stipulation.

## 9.9. Indemnities

No stipulation.

## 9.10. Term and Termination

### 9.10.1. Term

Refer to Clause 2.2.1 of this CP.

### 9.10.2. Termination

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

### 9.10.3. Effect of Termination and Survival

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

## 9.11. Individual Notices and Communications with Participants

No stipulation.

## 9.12. Amendments

### 9.12.1. Procedure for Amendment

Refer to Clause 1.5.4 of this CP.

### 9.12.2. Notification Mechanism and Period

Refer to Clause 1.5.4 of this CP.

### 9.12.3. Circumstances Under Which OID Must be Changed

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

## 9.13. Dispute Resolution Provisions

No stipulation.

## 9.14. Governing Law

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

## 9.15. Compliance with Applicable Law

SK SHALL ensure compliance with the following requirements:

- eIDAS [6] - 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,
- Electronic Identification and Trust Services for Electronic Transactions Act [7],
- Personal Data Protection Act [9],
- related European Standards:
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [10],
  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [3],
  - EN 419 211 Protection profiles for secure signature creation device [8].

## 9.16. Miscellaneous Provisions

### 9.16.1. Entire Agreement

No stipulation.

### 9.16.2. Assignment

No stipulation.

### 9.16.3. Severability

No stipulation.

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

No stipulation.

### 9.16.5. Force Majeure

No stipulation.

## 9.17. Other Provisions

Not allowed.

# 10. References

1. AS Sertifitseerimiskeskus - NQ-SK Certification Practice Statement, published: https://sk.ee/en/repository/CPS/
2. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt
3. 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
4. Certificate and OCSP Profile for Smart-ID, published: https://sk.ee/en/repository/profiles/
5. ETSI Drafting Rules (Verbal forms for the expression of provisions)
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. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current
8. ETSI EN 419 211 Protection profiles for secure signature creation device
9. Personal Data Protection Act, 16.01.2016, published: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current

10. ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
11. Terms and Conditions for Use of Certificates of non-qualified Smart-ID, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/
12. Requirements for Identity Providers, published: https://sk.ee/en/services/smartid