AS Sertifitseerimiskeskus – Certificate Policy for Qualified Smart-ID

Version 1.0

OID: 1.3.6.1.4.1.10015.17.2

Effective since 01.01.2017

Version History		
Date	**Version**	**Changes**
01.01.2017	1.0	First public edition.

1. Introduction
    - 1.1. Overview
    - 1.2. Document Name and Identification
    - 1.3. PKI Participants
        - 1.3.1. Certification Authorities
        - 1.3.2. Registration Authorities
        - 1.3.3. Subscribers
        - 1.3.4. Relying Parties
        - 1.3.5. Other Participants
    - 1.4. Certificate Usage
        - 1.4.1. Appropriate Certificate Uses
        - 1.4.2. Prohibited Certificate Uses
    - 1.5. Policy Administration
        - 1.5.1. Organization Administering the Document
        - 1.5.2. Contact Person
        - 1.5.3. Person Determining CPS Suitability for the Policy
        - 1.5.4. CPS Approval Procedures
    - 1.6. Definitions and Acronyms
        - 1.6.1. Terminology
        - 1.6.2. Acronyms
2. Publication and Repository Responsibilities
    - 2.1. Repositories
    - 2.2. Publication of Certification Information
        - 2.2.1. Publication and Notification Policies
        - 2.2.2. Items not Published in the Certification Practice Statement
    - 2.3. Time or Frequency of Publication
    - 2.4. Access Controls on Repositories
3. Identification and Authentication
    - 3.1. Naming
        - 3.1.1. Type of Names
        - 3.1.2. Need for Names to be Meaningful
        - 3.1.3. Anonymity or Pseudonymity of Subscribers
        - 3.1.4. Rules for Interpreting Various Name Forms
        - 3.1.5. Uniqueness of Names
        - 3.1.6. Recognition, Authentication, and Role of Trademarks
    - 3.2. Initial Identity Validation
        - 3.2.1. Method to Prove Possession of Private Key
        - 3.2.2. Authentication of Organization Identity
        - 3.2.3. Authentication of Individual Identity
        - 3.2.4. Non-Verified Subscriber Information
        - 3.2.5. Validation of Authority
        - 3.2.6. Criteria for Interoperation
    - 3.3. Identification and Authentication for Re-Key Requests
        - 3.3.1. Identification and Authentication for Routine Re-Key
        - 3.3.2. Identification and Authentication for Re-Key After Revocation
    - 3.4. Identification and Authentication for Revocation Request
4. Certificate Life-Cycle Operational Requirements
    - 4.1. Certificate Application
        - 4.1.1. Who Can Submit a Certificate Application
        - 4.1.2. Enrolment Process and Responsibilities

- 4.2. Certificate Application Processing
  - 4.2.1. Performing Identification and Authentication Functions
  - 4.2.2. Approval or Rejection of Certificate Applications
  - 4.2.3. Time to Process Certificate Applications
- 4.3. Certificate Issuance
  - 4.3.1. CA Actions During Certificate Issuance
  - 4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate
- 4.4. Certificate Acceptance
  - 4.4.1. Conduct Constituting Certificate Acceptance
  - 4.4.2. Publication of the Certificate by the CA
  - 4.4.3. Notification of Certificate Issuance by the CA to Other Entities
- 4.5. Key Pair and Certificate Usage
  - 4.5.1. Subscriber Private Key and Certificate Usage
  - 4.5.2. Relying Party Public Key and Certificate Usage
- 4.6. Certificate Renewal
- 4.7. Certificate Re-Key
- 4.8. Certificate Modification
- 4.9. Certificate Revocation and Suspension
  - 4.9.1. Circumstances for Revocation
  - 4.9.2. Who Can Request Revocation
  - 4.9.3. Procedure for Revocation Request
  - 4.9.4. Revocation Request Grace Period
  - 4.9.5. Time Within Which CA Must Process the Revocation Request
  - 4.9.6. Revocation Checking Requirements for Relying Parties
  - 4.9.7. CRL Issuance Frequency
  - 4.9.8. Maximum Latency for CRLs
  - 4.9.9. On-Line Revocation/Status Checking Availability
  - 4.9.10. On-Line Revocation Checking Requirements
  - 4.9.11. Other Forms of Revocation Advertisements Available
  - 4.9.12. Special Requirements Related to Key Compromise
  - 4.9.13. Circumstances for Suspension
  - 4.9.14. Who Can Request Suspension
  - 4.9.15. Procedure for Suspension Request
  - 4.9.16. Limits on Suspension Period
  - 4.9.17. Circumstances for Termination of Suspension
  - 4.9.18. Who Can Request Termination of Suspension
  - 4.9.19. Procedure for Termination of Suspension
- 4.10. Certificate Status Services
  - 4.10.1. Operational Characteristics
  - 4.10.2. Service Availability
  - 4.10.3. Operational Features
- 4.11. End of Subscription
- 4.12. Key Escrow and Recovery
  - 4.12.1. Key Escrow and Recovery Policy and Practices
  - 4.12.2. Session Key Encapsulation and Recovery Policy and Practices

5. Facility, Management, and Operational Controls
6. Technical Security Controls
   - 6.1. Key Pair Generation and Installation
     - 6.1.1. Key Pair Generation
     - 6.1.2. Private Key Delivery to Subscriber
     - 6.1.3. Public Key Delivery to Certificate Issuer
     - 6.1.4. CA Public Key Delivery to Relying Parties
     - 6.1.5. Key Sizes
     - 6.1.6. Public Key Parameters Generation and Quality Checking
     - 6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)
   - 6.2. Private Key Protection and Cryptographic Module Engineering Controls
     - 6.2.1. Cryptographic Module Standards and Controls
     - 6.2.2. Private Key (n out of m) Multi-Person Control
     - 6.2.3. Private Key Escrow
     - 6.2.4. Private Key Backup
     - 6.2.5. Private Key Archival
     - 6.2.6. Private Key Transfer Into or From a Cryptographic Module
     - 6.2.7. Private Key Storage on Cryptographic Module
     - 6.2.8. Method of Activating Private Key
     - 6.2.9. Method of Deactivating Private Key
     - 6.2.10. Method of Destroying Private Key
     - 6.2.11. Cryptographic Module Rating
   - 6.3. Other Aspects of Key Pair Management
     - 6.3.1. Public Key Archival
     - 6.3.2. Certificate Operational Periods and Key Pair Usage Periods
   - 6.4. Activation Data
     - 6.4.1. Activation Data Generation and Installation

6.4.2. Activation Data Protection
6.4.3. Other Aspects of Activation Data
6.5. Computer Security Controls
6.5.1. Specific Computer Security Technical Requirements
6.5.2. Computer Security Rating
6.6. Life Cycle Technical Controls
6.6.1. System Development Controls
6.6.2. Security Management Controls
6.7. Life Cycle Security Controls
6.8. Network Security Controls
6.9. Time-Stamping
7. Certificate, CRL, and OCSP Profiles
7.1. Certificate Profile
7.2. CRL Profile
7.3. OCSP Profile
8. Compliance Audit and Other Assessments
9. Other Business and Legal Matters
9.1. Fees
9.1.1. Certificate Issuance or Renewal Fees
9.1.2. Certificate Access Fees
9.1.3. Revocation or Status Information Access Fees
9.1.4. Fees for Other Services
9.1.5. Refund Policy
9.2. Financial Responsibility
9.2.1. Insurance Coverage
9.2.2. Other Assets
9.2.3. Insurance or Warranty Coverage for End-Entities
9.3. Confidentiality of Business Information
9.3.1. Scope of Confidential Information
9.3.2. Information Not Within the Scope of Confidential Information
9.3.3. Responsibility to Protect Confidential Information
9.4. Privacy of Personal Information
9.4.1. Privacy Plan
9.4.2. Information Treated as Private
9.4.3. Information Not Deemed Private
9.4.4. Responsibility to Protect Private Information
9.4.5. Notice and Consent to Use Private Information
9.4.6. Disclosure Pursuant to Judicial or Administrative Process
9.4.7. Other Information Disclosure Circumstances
9.5. Intellectual Property rights
9.6. Representations and Warranties
9.6.1. CA Representations and Warranties
9.6.2. RA Representations and Warranties
9.6.3. Subscriber Representations and Warranties
9.6.4. Relying Party Representations and Warranties
9.6.5. Representations and Warranties of Other Participants
9.7. Disclaimers of Warranties
9.8. Limitations of Liability
9.9. Indemnities
9.10. Term and Termination
9.10.1. Term
9.10.2. Termination
9.10.3. Effect of Termination and Survival
9.11. Individual Notices and Communications with Participants
9.12. Amendments
9.12.1. Procedure for Amendment
9.12.2. Notification Mechanism and Period
9.12.3. Circumstances Under Which OID Must be Changed
9.13. Dispute Resolution Provisions
9.14. Governing Law
9.15. Compliance with Applicable Law
9.16. Miscellaneous Provisions
9.16.1. Entire Agreement
9.16.2. Assignment
9.16.3. Severability
9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)
9.16.5. Force Majeure
9.17. Other Provisions
10. References

1. Introduction

1.1. Overview

This document, named "AS Sertifitseerimiskeskus – Certificate Policy for 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 qualified Smart-ID (hereinafter referred to as Q Smart-ID). These Certificates facilitate electronic signatures and electronic authentication of natural persons. Each Smart-ID contains one pair of Certificates consisting of the Authentication Certificate and the (qualified) Electronic Signature Certificate, each protected with its Activation Data.

Q Smart-ID is the new generation electronic identification (eID) solution. Q Smart-ID is a PKI based personal identification tool which can be used to authenticate in different e-services and to give electronic signatures which are recognized in the EU member states.

For easy onboarding, the user has to install the special application from Google Play or App Store and perform the registration process. During the registration, the user is identified and Q Smart-ID is issued based on the user's existing identity document. The application can be used with any modern smartphone or tablet.

In the first, pilot phase, it's possible to apply for Q Smart-ID using an existing mobile identity document. In next phases, Q Smart-ID account can be registered also online with the user's other eID document or via authentication service provided by bank. Later on, the user can apply for Q Smart-ID at the bank office and identify himself with a physical identity document.

The current version of the CP describes only the pilot phase of the Q Smart-ID issuance and usage.

Issuing and managing Certificates for Q 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 Policy for EU qualified Certificates issued to natural persons where the Private Key and the related Certificate reside on a QSCD (QCP-n-qscd) and the Policy for EU qualified certificate issued to a natural person (QCP-n) from ETSI EN 319 411-2 [4] and Normalised Certificate Policy requiring a Secure Cryptographic Device (NCP+) from ETSI EN 319 411-1 [3].

The semantics of "no stipulation" in this document is that no additional restrictions are set and relevant provisions from QCP-n-qscd, QCP-n and NCP+ are applied directly.

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

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

Q Smart-ID Certification Service Electronic Signature Certificates described in this CP SHALL be registered as a trust service according to the Trusted List of Estonia.

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

- QCP-n-qscd and QCP-n,
- 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] and ETSI EN 319 411-2 [4].

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).

1.2. Document Name and Identification

Refer to Clause 5.3 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

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

This CP is identified by OID: 1.3.6.1.4.1.10015.17.2

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	17.2

Qualified Electronic Signature Certificate for Q Smart-ID issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-2 [4] clause 5.3 c) for QCP-n-qscd: 0.4.0.194112.1.2

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

- ETSI EN 319 411-2 [4] clause 5.3 a) for QCP-n: 0.4.0.194112.1.0

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)

- This CP.

Authentication Certificates for Q Smart-ID issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [3] clause 5.3 b) for NCP+: 0.4.0.2042.1.2 itu-t(0) identified-Organisation(4) etsi(0) other certificate-policies(2042) policy-identifiers(1) ncpplus (2)
- This CP.

1.3. PKI Participants

Refer to Clause 5.4 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

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

E-service Provider 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.

1.3.5. Other Participants

Smart-ID Provider is an organisation that is legally responsible for the Smart-ID system.

SK fulfills the role of Smart-ID Provider in Republic of Estonia. SK maintains Smart-ID platform, which consists of the Smart-ID application and the Smart-ID Server.

1.4. Certificate Usage

Refer to Clause 5.5 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Certificate for Electronic Signature is intended for:

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

Authentication Certificate is intended for:

- Authentication
- Encryption.

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

- Subscriber Certificates compliant with NCP+, QCP-n-qscd or QCP-n,
- 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 Q 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 Mnt 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@sk.ee

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

1.5.2. Contact Person

Business Development Manager

Email: info@sk.ee

1.5.3. Person Determining CPS Suitability for the Policy

No stipulation.

1.5.4. CPS Approval Procedures

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

All amendments to this CP SHALL be coordinated with 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
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [12], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.
Smart-ID Application	A technical component of the Smart-ID system. A mobile Smart-ID Application instance installed on a Subscriber's Mobile Device that provides access to qualified Smart-ID service.
Smart-ID Provider	An organization 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 (Account owners) to authenticate themselves to E-Service Providers, to give Electronic Signatures requested by E-Service Providers, and to manage their Smart-ID accounts.
Advanced Electronic Signature	Electronic Signature which meets the requirements provided in Article 26 of eIDAS [6].
Distinguished Name	Subject name in the infrastructure of Certificates that is unique for every Subscriber.
E-Service Provider	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.
Mobile Device	A tablet computer or smartphone that runs a mobile device operating system (Apple iOS, Google Android).
Object Identifier	An identifier used to uniquely name an object (OID).
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. 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.
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. In the Smart-ID System, Public key exists only in the form of it's components and consists of the following components: 'Application's share of the public key' and 'Server's share of the public key'.
Relying Party	Entity that relies on the information contained within a Certificate.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Subscriber	A natural person to whom the qualified Smart-ID Certificates are issued as a public service if he/she has a statutory right.
Subject	In this document, the Subject is the same as the Subscriber.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon receipt of the Certificates.

Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Electronic Signature Certificate.
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 for which the identity of a person has been verified. The person's identity is verified by physical presence and personal authentication, prior to issuing electronic authentication credentials to the person. The person confirms the receipt of electronic credentials with a signature.

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.
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] and ETSI EN 319 411-2 [4].

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 [12], 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 E-Service Provider MAY be left out of CPS.

The CPS NEED NOT cover internal procedures of the RA and E-Service Provider.

2.3. Time or Frequency of Publication

No stipulation.

2.4. Access Controls on Repositories

No stipulation.

3. Identification and Authentication

Refer to Clause 6.2 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

3.1. Naming

The Distinguished Name of the Subscriber SHALL comply with conventions set in the Certificate Profile [12].

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 means of Verified Electronic Authentication prior to requesting issuance of the Subscriber's Certificates from the CA.

CA SHALL rely on identification data in signature of the application.

Application SHALL be signed with Qualified Certificate.

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 Q Smart-ID only personally.

The Subscriber SHALL be over 18 of age.

3.2.6. Criteria for Interoperation

No stipulation.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Refer to Clause 3.2 of this CP.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to Clause 3.2 of this CP.

3.4. Identification and Authentication for Revocation Request

No stipulation.

4. Certificate Life-Cycle Operational Requirements

Refer to Clause 6.3 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

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

RA SHALL perform Subscriber Authentication.

CA SHALL verify that the data in CSR matches the data in Qualified Certificate used for application signing.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

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

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

CA SHALL accept requests only from RA. SK SHALL rely upon identification data in the application.

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;
- the Subscriber's signature of the application for Q Smart-ID is invalid or does not meet the requirements for Qualified Electronic Signature laid out in eIDAS Regulation [6];
- the signatory of the application for Q Smart-ID is another person and not the Subscriber;
- the Subscriber is under 18 years of age.

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

No stipulation.

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 RA immediately in Smart-ID System after the Subscriber has accepted it.

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 Q Smart-ID, if the Subscriber has a Q Smart-ID account.

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

4.8. Certificate Modification

Certificate modification SHALL be allowed only in the case of errors during certification.

Certificate modification request is processed same as the initial application for Q Smart-ID.

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 Activation Codes, the Subscriber SHALL apply for Certificate revocation immediately.

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

- the Subscriber requests revocation of the Certificate in written form, using the Smart-ID Application; 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;
- 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 of Certificate modification the erroneous Certificate SHALL BE revoked.

If the new Certificates are issued for an existing Q 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.

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 Q Smart-ID account.

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

In case of a Q 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] and ETSI EN 319 411-2 [4].

6. Technical Security Controls

Refer to Clause 6.5 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

- The server and application SHALL generate RSA key pairs independently.
- The server's Private Key SHALL be generated on a FIPS 140-2 Level 3 certified HSM.
- Application SHALL further divide its Private Key into two parts. The two parts SHALL NOT BE distinguished from random numbers.
- Application SHALL send one of these parts to the server over a secure communication channel.

- Application SHALL NOT store the key part sent to the 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 [12].

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 [12].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The HSM module used to generate 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 Q Smart-ID keys SHALL be protected with its Activation Data.

The Subscriber SHALL be prompted to enter the activation 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 activation 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 Activation Codes sequentially.

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

The length of the activation 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 [12].

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The initial activation data SHALL be generated by the Smart-ID Application and SHALL be delivered to the Subscriber using the Smart-ID Application.

Copies of activation codes SHALL NOT be stored by the Smart-ID Service Provider.

6.4.2. Activation Data Protection

Activation codes SHALL be displayed once to the Subscriber by the Smart-ID Application.

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

Copies of the activation codes SHALL NOT be stored by the Smart-ID Application.

If the Activation Data is not under the control of the Subscriber, the Subscriber SHALL apply for a new Q 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.

6.7. Life Cycle Security Controls

No stipulation.

6.8. Network Security Controls

No stipulation.

6.9. Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

7.1. Certificate Profile

The Certificate SHALL comply with the profile described in the Certificate Profile [12].

7.2. CRL Profile

No CRL is required.

7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [12].

8. Compliance Audit and Other Assessments

Refer to Clause 6.7 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

9. Other Business and Legal Matters

Refer to Clause 6.8 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4]

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.

9.3.1. Scope of Confidential Information

No stipulation.

9.3.2. Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3. Responsibility to Protect Confidential Information

No stipulation.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation.

9.4.2. Information Treated as Private

No stipulation.

9.4.3. Information Not Deemed Private

No stipulation.

9.4.4. Responsibility to Protect Private Information

No stipulation.

9.4.5. Notice and Consent to Use Private Information

No stipulation.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CP.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

No stipulation.

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 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

No stipulation.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to Clause 1.5.4 of this CP.

9.12.2. Notification Mechanism and Period

Refer to Clause 1.5.4 of this CP.

9.12.3. Circumstances Under Which OID Must be Changed

OID SHALL change when the scope of this CP changes or when the new type of the Certificate 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 – 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. ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities;
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;
8. ETSI EN 419 211 Protection profiles for secure signature creation device;
9. Personal Data Protection Act, 06.01.2016, 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 Qualified Smart-ID, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;
12. Certificate and OCSP Profile for Smart-ID, published: https://sk.ee/en/repository/profiles/.