Document Information	
Name	Certificate Policy for Mobile ID of the Republic of Estonia
Version number	9.0
Version history	
Version No. and date	Changes
15.08.2020 9.0	Clause 3.2.3 - Changed identity verification process for MO, added description of Authentication of the Subscriber electronically. Clause 4.1.2 - Defined Mobile ID issuance process with electronic identification by MO and additional temporary issuance process for the emergency situation. Clause 1.6.1, 4.4.2 - Replaced DigiDocService with Mobile ID Service Integration API. Clause 10 - added reference to Mobile ID REST API. SK URL-s and e-mail addresses are corrected and updated through the CP.
10.04.2020 8.0	Clause 1.5.4 - Added that SK performs annual review of this CP.
01.05.2019 7.0	Clause 1.6.1 - Specified CRL definition. Clause 4.9.1 - Specified circumstances for Certificate revocation and added that revoked Certificate shall not be reinstated.
24.10.2017 6.0	Due to change of SK's business name from AS Sertifitseerimiskeskus to SK ID Solutions AS, name of the CP has been changed accordingly. Also, former business name has been replaced with the new one in clauses 1.1, 1.2, 1.5.1 and 1.6.2 of this CP. Clause 1.1 - Removed paragraph which stated that the CP is a complete redesign of the previous AS Sertifitseerimiskeskus - Certification Practice Statement and ESTEID Card Certification Policy. Clauses 1.1, 1.3.2 and 1.3.5 - Lingual corrections. Clause 1.6.2 - Added new acronyms and minor changes. Clause 3.2.3 - Corrected the wording by stating that in case of Certificate re-key, MO and PBGB are obligated to authenticate the Subscriber either electronically or via physical presence. Clauses 4.9.1, 4.9.2, 4.9.3, 4.9.13, 4.9.17, 4.9.18, 4.9.19, 9.15 - Replaced Estonian eIDAS supplement Act with Electronic Identification and Trust Services for Electronic Transactions Act. Clauses 4.1.2 and 4.2.1 - Added the possibility for the Subscriber to apply for Mobile ID Certificates at PBGB. Clause 4.2.1 - Lingual corrections. Clause 4.7 - Corrected what is treated as Certificate re-key in the context of this CP.

	Clause 4.7.3 - Specified Certificate re-key process.
01.11.2016 5.0	Redesigned the Certificate Policy in accordance with the IETF RFC 3647 [1] and eIDAS [7].
27.06.2016 4.0	Complemented clause 1.4 Identifying the Certification Policy. Complemented clause 1.5.2.1 Client Service Points. Complemented clause 1.5.3 PPA. Complemented clause 1.5.4.1 Client. Complemented clause 2.1.1 Obligations of SK. Complemented clause 2.1.2 Obligations of PPA. Complemented clause 2.1.3 Obligations of MO. Complemented clause 2.1.4.1 Obligations of MO Client Service Point. Complemented clause 2.1.5 Obligations of Clients. Complemented clause 4.1 Submission of Applications for Certificates. Complemented clause 4.2 Processing of Applications for Certificates. Complemented clause 4.2.1 Decision Making. Complemented clause 4.2.2 Certificate Issuance. Complemented clause 4.6.1 The Powers of Revoking a Certificate. Complemented clause 4.6.2 Submission of Application for Revocation.
01.01.2016 3.0	Complemented clause 1.2 Terminology. Changed clause 1.5 Organization and Area of Application. Changed clause 1.6 Contacts of PPA. Changes in clause 2.1 Obligations. Complemented clause 2.4.4 Directory Service. Changed clause 3.1 Identification of Client. Changed clause 3.3 Distinguished Name. Changed clause 4.1 Submission of Applications for Certificates. Changes in clause 4.2.4 Certificate Renewal. Complemented clause 4.4 Suspension of Certificates. Changed clause 4.5 Termination of Suspension. Changed clause 4.6 The Certificate Revocation. Renewed clause 9 Referred and Related Documents.
01.01.2015 2.0	Amendments aimed to bring this Certification Policy in line with the Identity Documents Act (RT I, 29.10.2014, 6) amending the terms and conditions of issuing Mobile-ID.
01.02.2011 1.1	Final version.
11.01.2011 0.1	Initial draft.
Effective from date	15.08.2020

1. Introduction

1.1. Overview

This document, named "SK ID Solutions AS – Certificate Policy for Mobile ID of the Republic of Estonia" (hereinafter referred to as CP), defines procedural and operational requirements that SK ID Solutions AS adheres to and requires entities to adhere to when issuing and managing Certificates for the digital identity in a mobile-ID format (hereinafter referred to as Mobile ID) issued by the Republic of Estonia. Mobile ID is issued to a natural person for a specific period of time stated in the IDA [8] and is related to the Mobile phone number. Mobile ID contains related Qualified Electronic Signature Creation Device (SIM-card) and two pairs of Certificates. These Certificates facilitate electronic signatures and electronic identification of natural persons. The Certificates always come in pairs: each Mobile ID contains two pairs of Certificates consisting of the Authentication Certificate and the Qualified Electronic Signature Certificate and their corresponding Private Keys. Each Private Key is protected by Activation Data (PIN code) and each Mobile ID has a single Unlock (PUK code). A single person can have only one valid Mobile ID at any point in time.

Issuing and managing Certificates for Mobile ID is based on Regulation (EU) N° 910/2014 [7] 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) from ETSI EN 319 411-2 [3] and Normalised Certificate Policy requiring a Secure Cryptographic Device (NCP+) from ETSI EN 319 411-1 [2].

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

Issuing and managing Qualified Electronic Signature Certificates for Mobile 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 in a QSCD.

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

The Certification Service for Qualified Electronic Signature Certificates for Mobile ID described in this CP SHALL be qualified trust service according to the Trusted List of Estonia.

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

- QCP-n-qscd
- NCP+
- This CP

- CPS

To preserve IETF RFC 3647 [1] 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 [2] and ETSI EN 319 411-2 [3].

In this CP modal verbs in capital letters are to be interpreted as described in Clause 3.2 of the ETSI Drafting Rules [6](Verbal forms for the expression of provisions).

Terms 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 [2] and ETSI EN 319 411-2 [3].

This document is named “SK ID Solutions – Certificate Policy for Mobile ID of the Republic of Estonia".

This CP is identified by OID: 1.3.6.1.4.1.10015.1.3

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	1.3

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

- ETSI EN 319 411-2 [3] 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)

- This CP

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

- ETSI EN 319 411-1 [2] 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 [2] and ETSI EN 319 411-2 [3].

1.3.1. Certification Authorities

No stipulation.

1.3.2. Registration Authorities

The PBGB as well as MO CAN appear in multiple roles throughout the document. Throughout the rest of this CP a following distinction is made based on the role:

- PBGB and MO are together referred to as RA when they are performing technical actions that are not specific to any particular organisation – e.g. Subscriber Authentication
- PBGB and MO are explicitly referred to by their corresponding names, when they are performing actions specific to a particular type of organisation, e.g. MO when issuing QSCD compliant SIM-cards (hereinafter referred to as QSCD) to the Subscriber, or PBGB when it is representing Republic of Estonia in the role of Document Issuer according to IDA [8] during initial identification of persons or making decisions about their eligibility for Mobile ID

PBGB and MO have different roles, their corresponding responsibilities are described in a greater detail in the subsequent chapters of this document.

1.3.3. Subscribers

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

Subscriber SHALL be only a natural person entitled by IDA [8].

1.3.4. Relying Parties

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

1.3.5. Other Participants

SCM produces QSCD, generates key pairs and loads them into a QSCD.

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

Telecommunication service provider facilitates communication between the Subscriber's device and QSCD.

1.4. Certificate Usage

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

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Qualified Electronic Signature Certificate is intended for

- Creating Qualified Electronic Signatures compliant with eIDAS [7]

Authentication Certificate is intended for

- Authentication
- Secure e-mail

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

- Subscriber Certificates compliant with QCP-n-qscd or NCP+
- OCSP response verification Certificates
- Internal Certificates for technical needs

1.4.2. Prohibited Certificate Uses

Subscriber's 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 Mobile 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)

Subscriber's Authentication Certificate SHALL NOT be used to create Qualified Electronic Signatures compliant with eIDAS [7].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CP is administered by SK.

SK ID Solutions AS

Registry code 10747013

Pärnu Ave 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@skidsolutions.eu

http://www.skidsolutions.eu/en/

1.5.2. Contact Person

Business Development Manager

Email: info@skidsolutions.eu

1.5.3. Person Determining CPS Suitability for the Policy

No stipulation.

1.5.4. CP 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.

SK performs annual review of this CP to ensure compliance of the present document and Certification service provided under this CP with the applicable requirements.

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 [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 and Certificate Revocation Lists with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Directory Service	Trust service related to publication of Certificate validity information.

Term	**Definition**
Mobile ID Service Integration API	SOAP-based Digidoc Services [14] and MID REST API [16] that can be used to add Mobile-ID authentication, digital signing and pulling Subscriber certificate functionality to an e-service or application.
Distinguished Name	Subject name in the infrastructure of Certificates that is unique for every Subscriber.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Mobile ID	A form of digital identity, the Certificates of which enabling electronic identification and electronic signature are connected to the SIM-card of Mobile phone.
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS [7] Regulation.
Qualified Electronic Signature	Advanced electronic signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS [7] Regulation.
Relying Party	Entity that relies on the information contained within a Certificate.

Term	Definition
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.
Secure Cryptographic Device	Device which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subscriber	A natural person to whom the Certificates of Mobile ID 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 [5] upon receipt of the Certificates.

1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014 [7] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
IDA	Identity Documents Act [8]
MO	Mobile Operator
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [2]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device

Acronym	Definition
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [3]
RA	Registration Authority
SCM	SIM-card Manufacturer
SK	SK ID Solutions AS

2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [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 down-time 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 [15], the Certificate Profile [4], as well as the Terms and Conditions [5] together with the enforcement dates SHALL be published on SK website https://skidsolutions.eu/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, PBGB and MO MAY be left out of CPS.

CPS MAY not cover internal procedures of PBGB and MO.

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 [2] and ETSI EN 319 411-2 [3].

3.1. Naming

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

3.1.1. Types 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

Pursuant to IDA [8], international letters SHALL be encoded according to ICAO transcription rules where necessary. Rules for generating e-mail addresses SHALL be as listed in clause 6.1 of the Certificate Profile [4].

3.1.5. Uniqueness of Names

SK SHALL ensure that Certificates with matching Common Name (CN), SerialNumber and e-mail addresses in Subject Alternative Name (SAN) 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

MO SHALL perform Subscriber Authentication and issue a QSCD to the Subscriber.

The Subscriber SHALL sign the corresponding application form and thus confirm the ownership of the issued QSCD.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

Authentication of Subscribers is carried out by RA as follows.

MO SHALL perform Subscriber Authentication in two occasions:

- When the Subscriber applies for a new Mobile ID
- When the Subscriber needs to replace the QSCD for a valid Mobile ID (Certificate re-key)

MO SHALL Authenticate the Subscriber via physical presence or electronically. For the electronic Authentication to be possible, the Subscriber has to have capability to give Qualified Electronic Signature.

PBGB SHALL Authenticate the Subscriber electronically or via physical presence to verify eligibility to use Mobile ID. For the electronic Authentication to be possible, the Subscriber has to have a valid digital identity of the Republic of Estonia or the identity card of the Republic of Estonia.

Authentication SHALL be carried out by RA in accordance with Chapter 3 of IDA [8].

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

According to IDA [8], the Subscriber cannot apply for Mobile ID through a representative.

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

Certificate re-key is the replacement of the Subscriber's QSCD with a new one for a valid Mobile ID.

The Subscriber's QSCD is replaced when the QSCD is, for instance, damaged or needs replacement for some other reasons.

For the description of the Authentication procedure for re-key requests refer to Clause 3.2.3 of this CP.

3.3.2. Identification and Authentication for Re-Key After Revocation

In the case of re-key after revocation the Subscriber identity SHALL be validated in accordance with 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 [2] and ETSI EN 319 411-2 [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

The responsibilities and process for making decisions about eligibility to apply for a Certificate are laid out in Chapter 3 of IDA [8].

If the Subscriber applies for a new Mobile ID, the existing Mobile ID SHALL BE terminated and the new Mobile ID SHALL be issued to the Subscriber.

One of the required prerequisites for applying for Mobile ID is existing and valid digital identity of the Republic of Estonia or identity card of the Republic of Estonia.

SK is responsible for assigning the correct e-mail address in the eesti.ee domain to the Certificate for Authentication:

- Re-use the previous one if the Subscriber already has an address assigned
- Generate a previously unused address according to clause 6.1 of the Certificate Profile [4] if the Subscriber has a new name
- Generate a previously unused address according to clause 6.1 of the Certificate Profile [4] if the Subscriber has not been previously assigned an address

CA is responsible for keeping track of e-mail address assignments.

Mobile ID issuance with physical identification is as follows:

- MO SHALL Authenticate the Subscriber as stated in Clause 3.2.3 of this CP
- Upon successful Authentication, the Subscriber SHALL sign a Mobile ID agreement with MO
- MO SHALL issue a QSCD to the Subscriber, and personalise it at the CA. For QSCD personalisation, MO supplies CA with information that binds the Subscriber to the Private Keys on the issued QSCD and the corresponding Public Keys, which CA uses for certification
- The Subscriber SHALL request for certification electronically in PBGB information system or via physical presence at PBGB. PBGB SHALL Authenticate the Subscriber as stated in Clause 3.2.3 of this CP and verify the Subscriber's eligibility to use Mobile ID according to IDA [8]

Mobile ID issuance with electronic identification is as follows:

- In case when the Subscriber already has QSCD with no Mobile ID related to it, existing QSCD MAY be used for Mobile ID enrolment, otherwise MO SHALL deliver new QSCD to the Subscriber
- MO SHALL verify that the QSCD is under the Subscriber’s control
- The Subscriber SHALL sign in MO self service environment Mobile ID agreement by using Qualified Electronic Signature
- MO SHALL Authenticate the Subscriber as stated in Clause 3.2.3 by relying on identification data provided in the signature of the Mobile ID agreement
- MO SHALL personalise the QSCD at the CA. For QSCD personalisation, MO supplies CA with information that binds the Subscriber to the Private Keys on the issued QSCD and the corresponding Public Keys, which CA uses for certification
- The Subscriber SHALL request for certification electronically in PBGB information system or via physical presence at PBGB. PBGB SHALL Authenticate the Subscriber as stated in Clause 3.2.3 of this CP and verify the Subscriber's eligibility to use Mobile ID according to IDA [8]

Mobile ID issuance with electronic identification with the exception that the Mobile ID agreement is signed by the Subscriber on his/her device by Qualified Electronic Signature and sent to MO by e-mail MAY applied in the emergency situation declared by the Estonian government until two weeks after termination of the emergency situation. To apply the temporary issuance process MO SHALL have received written consent from CA. First time the emergency situation process applied was in time period starting from 13.04.2020 until 31.05.2020 due the emergency situation declared by Estonian prime minister on 12.03.2020.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber may apply for Certification in the following ways:

- When applying for a new Mobile ID, the Subscriber applies for Certification electronically in the information system of PBGB or via physical presence at PBGB. PBGB applies for Certification at the CA on behalf of the Subscriber
- When replacing a QSCD (Certificate re-key), MO applies for Certification at the CA on behalf of the Subscriber

In both cases, RA Authenticates the Subscriber as stated in Clause 3.2.3 of this CP.

Upon successful Authentication the Subscriber MAY apply for Certification by signing the corresponding request either at MO or PBGB.

SK SHALL accept Certification applications only from RA and SHALL rely upon identification information provided by RA.

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.

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, an entity that requested certification SHALL be notified.

4.2.3. Time to Process Certificate Applications

In accordance with the applicable laws and 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

When the Subscriber is applying for a new Mobile ID, the following conditions SHALL be met for Certificate acceptance:

- The Subscriber has signed a request for Certification at the PBGB as stated in Clause 4.2.1 of this CP
- CA has received corresponding certification application from the PBGB

When the Subscriber is replacing a QSCD (Certificate re-key), the following conditions SHALL be met for Certificate acceptance:

- The Subscriber has signed a request for Certification at the MO as stated in Clause 4.2.1 of this CP
- CA has received corresponding certification application from the MO

4.4.2. Publication of the Certificate by the CA

Certificate SHALL be made available via the Directory Service and Mobile ID Service Integration API, OCSP SHALL start responding with "GOOD".

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

Telecommunication service provider SHALL be notified about the issued Certificates.

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

Certificate re-key is the replacement of the Subscriber's QSCD with a new one for a valid Mobile ID.

4.7.1. Circumstances for Certificate Re-Key

Certificate re-key SHALL BE allowed only in the case when the QSCD has to be replaced in result of negligence of the Subscriber or when the QSCD is damaged or needs replacement for some other reasons.

If the Subscriber has lost his/her Mobile ID due to negligence, the Subscriber SHALL apply for a new Mobile ID and this request SHALL be processed as an application for a new Mobile ID as stated in Clause 3.2.3 of this CP.

4.7.2. Who May Request Certification of a New Public Key

Only the Subscriber and MO together CAN initiate the re-key process.

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:

- MO SHALL Authenticate the Subscriber as stated in Clause 3.2.3 of this CP
- Upon successful Authentication, the Subscriber SHALL sign an agreement with MO and confirm that the QSCD to be replaced has been issued to him/her
- MO SHALL issue a new QSCD to the Subscriber, and personalise it at the CA. For QSCD personalisation, MO supplies CA with information that binds the Subscriber to the Private Keys on the issued QSCD and the corresponding Public Keys, which CA uses for certification
- MO SHALL apply for Certification at the CA on behalf of the Subscriber
- CA SHALL verify validity of the QSCD to be replaced and the issued Certificates

The validity period of the issued Certificates SHALL NOT exceed the validity period of the corresponding Mobile ID.

The Certificates that have been replaced SHALL be revoked immediately.

4.7.4. Notification of New Certificate Issuance to Subscriber

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

MO 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

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

4.8.1. Circumstances for Certificate Modification

Certificate modification is allowed to:

- Change e-mail addresses written to the Subject Alternative Name field of the Authentication Certificates
- Fix ASN.1 encoding errors in Certificates
- Replace SHA-1 signatures with stronger cryptography

Additional circumstances for Certificate modification SHALL be agreed upon with PBGB and the CP and CPS SHALL be updated to reflect the changes.

4.8.2. Who May Request Certificate Modification

Certificate Modification MAY be performed by the CA internally or requested by PBGB.

4.8.3. Processing Certificate Modification Requests

CA SHALL process Certificate Modification requests and is not required to negotiate it with the Subscriber.

Certificates that are being replaced SHALL be revoked immediately.

The validity period of the newly issued Certificates SHALL NOT exceed the validity period of the corresponding Mobile ID.

4.8.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6. Publication of Modified Certificate by the CA

Refer to Clause 4.4.2 of this CP.

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

Refer to Clause 4.4.3 of this CP.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances for Certificate revocation SHALL be as laid down in IDA [8] and Article 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

In addition to the circumstances in the referred laws and more precisely, SK has the right to revoke the Certificate if one or more of the following occurs:

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

MO has the right to request revocation of Mobile ID Certificates if one or more of the following occurs:

- The Subscriber requests revocation via MO
- QSCD is replaced (for example QSCD is damaged, migration to other MO, application for new Mobile ID)
- Telecommunication service is terminated
- Telecommunication service contract is terminated
- MO obtains evidence that the Subscriber has lost control over Private Keys or PIN codes (for example SIM-card has been transferred to another person)
- The Subscriber has violated one or more of its obligations to MO (for example the Subscriber has not fulfilled its financial obligations)

Revoked Certificate SHALL NOT be reinstated.

4.9.2. Who Can Request Revocation

Entities eligible to request Certificate revocation SHALL be as laid down in IDA [8] and Article 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.3. Procedure for Revocation Request

The procedure for revocation request SHALL be as laid down in IDA [8] and Article 20 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

Certificate revocation SHALL apply to Certificate Pairs only.

If one of the Certificates in a Certificate Pair needs to be revoked, the entire Certificate Pair is revoked. Other Certificate Pairs MAY remain valid.

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

No stipulation.

4.9.8. Maximum Latency for CRLs

No stipulation.

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

Circumstances for Certificate suspension SHALL be as laid down in Article 17 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.14. Who Can Request Suspension

Anyone can request Certificate suspension.

4.9.15. Procedure for Suspension Request

It SHALL be possible to request the suspension of the telecommunication service which enables Mobile ID usage via phone 24 hours a day, 7 days a week. The suspension of the telecommunication service results in impossibility to use Mobile ID.

Certificate suspension SHALL be possible to request at the CA. Certificate suspension SHALL apply to Certificate Pairs only. If one of the Certificates in a Certificate Pair needs to be suspended, the entire Certificate Pair is suspended. Other Certificate Pairs MAY remain valid.

Certificate suspension SHALL leave a uniquely identifiable trace.

4.9.16. Limits on Suspension Period

No limits.

4.9.17. Circumstances for Termination of Suspension

Circumstances for termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

It SHALL be possible to terminate the suspension of the telecommunication service at MO. When the telecommunication service suspension is terminated, it is possible to use Mobile ID again.

The Subscriber SHALL be able to request Termination of Certificate suspension at MO, if:

- The Subscriber has been issued QSCD, the Subscriber has signed a Mobile ID agreement and the Certificates are in suspended state and
- The owner of the Subscriber's mobile telephone number changes, but the Subscriber continues to use the number and Mobile ID

Termination of Certificate suspension SHALL be possible at CA. Termination of Certificate suspension SHALL apply to Certificate Pairs only. If the suspension of one of the Certificates in a Certificate Pair needs to be terminated, the suspension of the entire Certificate Pair is terminated.

4.9.18. Who Can Request Termination of Suspension

Entities who can request termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

4.9.19. Procedure for Termination of Suspension

The procedure for termination of Certificate suspension SHALL be as laid down in Article 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [10].

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 down-time 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 [2] and ETSI EN 319 411-2 [3].

6. Technical Security Controls

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

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Private Key SHALL be generated on the QSCD or in a FIPS 140-2 Level 3 certified HSM during the SIM-card manufacturing process after which keys SHALL be securely transferred to the SIM-card. If a special secure module is used for key generation, private keys SHALL be deleted from the SIM-card manufacturer's information system promptly after they are transferred onto the SIM-card. Private Keys SHALL NOT be saved outside of the SIM-card in the course of this transfer.

6.1.2. Private Key Delivery to Subscriber

The SCM SHALL manufacture non-personalised QSCDs and generate non-personalised key pairs.

Private Keys SHALL be loaded into the QSCD, which SHALL be delivered to MO.

MO SHALL perform Subscriber Authentication, personalise QSCD and issue QSCD to the Subscriber in accordance with Clause 4.1.2 of this CP.

6.1.3. Public Key Delivery to Certificate Issuer

The SCM SHALL manufacture non-personalised QSCDs and generate non-personalised key pairs.

Public Keys SHALL be handed over to MO.

MO, in turn, SHALL hand Public Keys over to CA for registration.

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

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

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

The Subscriber SHALL be prompted to enter the PIN code of the Authentication Certificate at least once after the phone has been turned on.

The Subscriber SHALL be prompted to enter the PIN code of the Qualified Electronic Signature Certificate before every single operation done with the corresponding Private Key.

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 Qualified 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

The PUK code SHALL be at least 8 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 of the corresponding Mobile ID agreement and comply with IDA [8].

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The initial activation data SHALL be generated by the SCM and SHALL be delivered to the Subscriber in a concealed form.

Copies of PIN codes SHALL NOT be stored by the SCM.

6.4.2. Activation Data Protection

PIN codes SHALL be printed on the plastic of the SIM-card containment under the secure layer in a manner that they cannot be read without damaging the security feature, and handed over to the Subscriber by MO.

The Subscriber SHALL confirm that the security feature has not been damaged at the time of the receipt of PIN codes.

Copies of the PIN codes SHALL NOT be stored by MO.

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 [2] and ETSI EN 319 411-2 [3].

7.1. Certificate Profile

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

7.2. CRL Profile

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

7.3. OCSP Profile

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

8. Compliance Audit and Other Assessments

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

9. Other Business and Legal Matters

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

An employee of CA SHALL NOT be punished for an intentional crime.

9.6.2. RA Representations and Warranties

An employee of RA SHALL NOT be punished for an intentional crime.

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

An employee of PBGB SHALL NOT be punished for an intentional crime.

An employee of MO SHALL NOT be punished for an intentional crime.

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 [7] - 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 [10]
- Identity Documents Act [8]
- State Fees Act [14]
- Personal Data Protection Act [12]

Related European Standards:

ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [13],

ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [2],

ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [3],

EN 419 211 Protection profiles for secure signature creation device [10].

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. 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
2. 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;
3. 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 issuing qualified certificates;
4. Certificate, CRL and OCSP Profile for personal identification documents of the Republic of Estonia, published: https://skidsolutions.eu/en/repository/profiles/;
5. Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia, published: https://skidsolutions.eu/en/repository/conditions-for-use-of-certificates/;
6. ETSI Drafting Rules (Verbal forms for the expression of provisions);
7. 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;
8. Identity Documents Act, RT I 1999, 25, 365, published: https://www.riigiteataja.ee/en/eli/511042016001/consolide/current;
9. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published:https://www.riigiteataja.ee/en/eli/527102016001/consolide/current;
10. ETSI EN 419 211 Protection profiles for secure signature creation device;
11. State Fees Act, published: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current
12. Personal Data Protection Act, 06.01.2016, published: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current;
13. ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
14. DigiDocService specification, published: https://sk-eid.github.io/dds-documentation/;

15. SK ID Solutions AS - ESTEID-SK Certification Practice Statement, published: https://skidsolutions.eu/en/repository/CPS/;
16. Mobile ID REST API https://github.com/SK-EID/MID.