SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania

OID: 1.3.6.1.4.1.10015.18.1

Document Information	
Name	Certificate Policy for Mobile-ID of Lithuania
Version No	3.0
Version History	
Date and Version No	Changes
12.05.2021 3.0	• Clause 1.5.2, 1.5.4 - replaced business development manager with head of trust services; • clause 1.6.1, 4.1.2, 4.4.2, 10. - defined Mobile-ID Service Integration API introduction due to Digidoc Services decommission; • clause 2.2.1 - updated SK website hostname; • clause 9.15, 10. - replaced Personal Data Protection Act with General Data Protection Regulation; • clause 10. - updated name of CPS and weblink of Electronic Identification and Trust Services for Electronic Transactions Act; • throughout the document replaced term 'reliable source' with 'authoritative source'.
10.04.2020 2.0	• Clause 1.5.4 - added that SK performs annual review of this CP.
01.03.2018 1.0	• First public edition.
Effective since	12.05.2021

1. Introduction

1.1. Overview

This document, named "SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania" (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 Mobile-ID of Lithuania (hereinafter referred to as Mobile-ID). Mobile-ID is a form of digital identity, the Cerfiticates are connected to the SIM-card (Qualified Electronic Signature Creation Device) of Mobile phone. Mobile-ID is issued to a natural person. Mobile-ID Certificates facilitate electronic signatures and electronic identification of natural persons. 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 several valid Mobile-ID's, in this case every Mobile-ID is related to different Mobile phone number and SIM-card.

Issuing and managing Certificates for Mobile-ID is based on the Regulation (EU) N° 910/2014 [1] which establishes a legal framework for electronic signatures.

This document describes only restrictions to Policy for EU qualified certificate 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 Normalized Certificate Policy requiring a secure cryptographic device (NCP+) from ETSI EN 319 411-1 [2].

The semantics of "no stipulation in addition to QCP-n-qscd and NCP+" 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 [4] 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 [5] (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 AS – Certificate Policy for Mobile-ID of Lithuania".

This CP is identified by OID: 1.3.6.1.4.1.10015.18.1

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

Parameter	**OID reference**
Internet attribute	1.3.6.1
Private entity attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	18.1

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-organization(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-organization(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 in addition to QCP-n-qscd and NCP+.

1.3.2. Registration Authorities

MO is operating as RA.

RA is performing Subscriber Authentication and associates the Subscriber to the specific QSCD and issues the QSCD to the Subscriber.

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.

1.3.5. Other Participants

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

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[1].

Authentication Certificate is intended for:

- authentication.

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

- subscriber Certificates compliant with 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[1].

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

https://www.skidsolutions.eu/

1.5.2. Contact Person

Head of trust services

Email: info@skidsolutions.eu

1.5.3. Person Determining CPS Suitability for the Policy

No stipulation in addition to QCP-n-qscd and NCP+.

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, are documented in the Versions and Changes section of the present 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 head of trust services 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.
Authentication Certificate	Certificate is intended for Authentication.
Certificate	Public key, together with some other information, laid down in the Certificate Profile [6], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one 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.

Term	Definition
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	In the context of this document, service related to issuing Certificates, managing revocation, modification and re-key of the Certificates.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
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.
Mobile-ID Service Integration API	MID REST API [13] that can be used to add Mobile-ID authentication, digital signing and pulling Subscriber certificate functionality to an e-service or application.
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for a Private Key.
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 corresponding Private Key or CA and that is used by Relying Party to verify electronic signatures created 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[1] 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 Certificate	Qualified Electronic Signature Certificate according to eIDAS Regulation [9].
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS[1] Regulation.
Relying Party	Entity that relies upon the information contained within a Certificate or Certificate status information provided by SK.

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.
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 [7] upon receipt the Certificates.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [1] 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
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
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [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 [12] , the Certificate Profile [6] , as well as the Terms and Conditions [7] with the enforcement dates, SHALL be published on SK website https://www.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 and RA MAY be left out of CPS.

2.3. Time or Frequency of Publication

No stipulation in addition to QCP-n-qscd and NCP+.

2.4. Access Controls on Repositories

No stipulation in addition to QCP-n-qscd and NCP+.

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 Certificate SHALL comply with conventions set in the Certificate Profile [6].

3.1.1. Types of Names

No stipulation in addition to QCP-n-qscd and NCP+.

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

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

The Subscriber SHALL sign the corresponding application form and thereby 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.

RA SHALL perform Subscriber Authentication when the Subscriber applies for a new Mobile-ID.

RA SHALL Authenticate the Subscriber:

- via physical presence checks and handwritten signature; or
- using means of electronic authentication and Qualified Electronic Signature compliant with eIDAS[1].

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 Mobile-ID only personally.

The Subscriber SHALL have legal capacity.

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

For the description of the Authentication procedure for re-key requests refer to Clause 3.2 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 in addition to QCP-n-qscd and NCP+.

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

Subscriber WILL request for Certificates via RA.

The enrolment process is as follows.

- RA SHALL Authenticate the Subscriber as stated in Clause 3.2.3 of this CP;
- RA SHALL issue a QSCD to the Subscriber;
- RA SHALL perform additional checks related to the Subscriber's identity validation;
- upon successful Authentication, the Subscriber SHALL sign a Mobile-ID agreement with RA, accept the Terms and Conditions [7], confirm that the QSCD has been issued to him/her and correctness of the information presented to RA;
- RA SHALL personalise the QSCD at the CA. For QSCD personalisation, RA 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;
- RA SHALL apply for Certification at the CA on behalf of the Subscriber;
- RA SHALL archive the agreement signed by the Subscriber;
- CA SHALL verify validity of the QSCD, perform the necessary checks, sign the Public Keys and the Certificate SHALL be made available via the Mobile-ID Service Integration API [13] and OCSP SHALL start responding with "GOOD".

RA is responsible for submitting correct identification data (names, personal codes, dates) to the SK.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber may apply for Certification in the following ways:

- physically;
- electronically.

RA applies for Certification at the CA on behalf of the Subscriber.

RA Authenticates the Subscriber as stated in Clause 3.2.3 of this CP.

Upon successful Authentication, the Subscriber SHALL accept the Terms and Conditions [7] .

RA SHALL submit a Certificate request to the CA.

CA SHALL accept Certificate requests only from RA.

CA MAY check the identification data provided by RA against authoritative source.

4.2.2. Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate if:

- the information about QSCD does not exist in the CA database;
- the application data does not validate;
- the Certificate request does not comply with the technical requirements set in applicable agreements;
- the Subscriber lacks legal capacity;
- the identification data does not match with the data in authoritative source.

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 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 in addition to QCP-n-qscd and NCP+.

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

No stipulation in addition to QCP-n-qscd and NCP+.

4.4.2. Publication of the Certificate by the CA

Certificate SHALL be made available via the Mobile-ID Service Integration API [13] and 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 in addition to QCP-n-qscd and NCP+.

4.5.2. Relying Party Public Key and Certificate Usage

No stipulation in addition to QCP-n-qscd and NCP+.

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.

Certificate re-key SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks or electronical Authentication methods.

During Certificate re-key, the Certificates to be replaced SHALL be revoked.

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

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 when the QSCD is damaged or needs replacement for some other reasons.

4.7.2. Who May Request Certification of a New Public Key

Only the Subscriber 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

Refer to clause 4.1.2 of this CP.

The Certificates that have been replaced SHALL be revoked immediately. All Mobile-ID Certificates SHALL be replaced simultaneously.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation in addition to QCP-n-qscd and NCP+.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation in addition to QCP-n-qscd and NCP+.

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.

During Certificate modification, the Certificates to be replaced SHALL be revoked.

4.8.1. Circumstances for Certificate Modification

Certificate modification SHALL be allowed for fixing invalid Certificates that do not comply with the Certificate Profile [6].

4.8.2. Who May Request Certificate Modification

Certificate modification MAY be performed by the CA internally.

SK SHALL NOT accept modification requests from other parties.

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 in addition to QCP-n-qscd and NCP+.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No stipulation in addition to QCP-n-qscd and NCP+.

4.8.6. Publication of the 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

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

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

- the Subscriber requests revocation via service point of the RA;
- SK obtains evidence that Subscriber has lost control over Private Keys or PIN codes;
- the Subscriber notifies SK that the original Certificate request was not authorised and does not retroactively grant authorisation;
- SK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- SK obtains evidence that the Certificate was misused;
- SK is made aware that a Subscriber has violated one or more of its obligations under the Terms and Conditions [7];
- 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;
- if such an obligation is foreseen by the law or any legislation established on the basis thereof.

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

- the Subscriber requests revocation via service point of the RA;
- QSCD is replaced (for example QSCD is damaged, migration to other MO, application for new Mobile-ID);
- telecommunication service contract is terminated;
- RA 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).

In case of Certificate modification the erroneous Certificate SHALL BE revoked.

In case of Certificate re-key the Certificates to be replaced SHALL be revoked.

4.9.2. Who Can Request Revocation

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

RA and CA MAY request revocation for any of the reasons listed in Clause 4.9.1 of this CP.

Competent authority MAY request revocation of the Subscriber Certificates if such an obligation is foreseen by the Estonian or Lithuanian law or any legislation established on the basis thereof.

4.9.3. Procedure for Revocation Request

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

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

SK SHALL verify that competent authority is authorised to request revocation.

Only in cases where 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 MAY revoke only the Certificate Pair which is compromised or no longer complies with the requirements and the other Certificate Pair remains valid.

4.9.4. Revocation Request Grace Period

No stipulation in addition to QCP-n-qscd and NCP+.

4.9.5. Time Within Which CA Must Process the Revocation Request

No stipulation in addition to QCP-n-qscd and NCP+.

4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

4.9.10. On-Line Revocation Checking Requirements

No stipulation in addition to QCP-n-qscd and NCP+.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation in addition to QCP-n-qscd and NCP+.

4.9.12. Special Requirements Related to Key Compromise

No stipulation in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

4.11. End of Subscription

No stipulation in addition to QCP-n-qscd and NCP+.

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 RA.

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

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation in addition to QCP-n-qscd and NCP+.

6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [6].

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation in addition to QCP-n-qscd and NCP+.

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 [6].

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 in addition to QCP-n-qscd and NCP+.

6.2.3. Private Key Escrow

No stipulation in addition to QCP-n-qscd and NCP+.

6.2.4. Private Key Backup

No stipulation in addition to QCP-n-qscd and NCP+.

6.2.5. Private Key Archival

No stipulation in addition to QCP-n-qscd and NCP+.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

No stipulation in addition to QCP-n-qscd and NCP+.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

6.2.10. Method of Destroying Private Key

No stipulation in addition to QCP-n-qscd and NCP+.

6.2.11. Cryptographic Module Rating

No stipulation in addition to QCP-n-qscd and NCP+.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation in addition to QCP-n-qscd and NCP+.

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 [6] .

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 RA.

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 RA.

6.4.3. Other Aspects of Activation Data

No stipulation in addition to QCP-n-qscd and NCP+.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

No stipulation in addition to QCP-n-qscd and NCP+.

6.5.2. Computer Security Rating

No stipulation in addition to QCP-n-qscd and NCP+.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

No stipulation in addition to QCP-n-qscd and NCP+.

6.6.2. Security Management Controls

No stipulation in addition to QCP-n-qscd and NCP+.

6.6.3. Life Cycle Security Controls

No stipulation in addition to QCP-n-qscd and NCP+.

6.7. Network Security Controls

No stipulation in addition to QCP-n-qscd and NCP+.

6.8. Time-Stamping

No stipulation in addition to QCP-n-qscd and NCP+.

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 [6].

7.2. CRL Profile

Not applicable.

7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [6].

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 in addition to QCP-n-qscd and NCP+.

9.1.2. Certificate Access Fees

No stipulation in addition to QCP-n-qscd and NCP+.

9.1.3. Revocation or Status Information Access Fees

No stipulation in addition to QCP-n-qscd and NCP+.

9.1.4. Fees for Other Services

No stipulation in addition to QCP-n-qscd and NCP+.

9.1.5. Refund Policy

No stipulation in addition to QCP-n-qscd and NCP+.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation in addition to QCP-n-qscd and NCP+.

9.2.2. Other Assets

No stipulation in addition to QCP-n-qscd and NCP+.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation in addition to QCP-n-qscd and NCP+.

9.3. Confidentiality of Business Information

No stipulation in addition to QCP-n-qscd and NCP+.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.2. Information Treated as Private

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.3. Information Not Deemed Private

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.4. Responsibility to Protect Private Information

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.5. Notice and Consent to Use Private Information

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation in addition to QCP-n-qscd and NCP+.

9.4.7. Other Information Disclosure Circumstances

No stipulation in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

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 the Card Manufacturer SHALL NOT be punished for an intentional crime.

9.7. Disclaimers of Warranties

No stipulation in addition to QCP-n-qscd and NCP+.

9.8. Limitations of Liability

No stipulation in addition to QCP-n-qscd and NCP+.

9.9. Indemnities

No stipulation in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

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 in addition to QCP-n-qscd and NCP+.

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[1] - 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 [8];
- General Data Protection Regulation [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 [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 [11].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation in addition to QCP-n-qscd and NCP+.

9.16.2. Assignment

No stipulation in addition to QCP-n-qscd and NCP+.

9.16.3. Severability

No stipulation in addition to QCP-n-qscd and NCP+.

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

No stipulation in addition to QCP-n-qscd and NCP+.

9.16.5. Force Majeure

No stipulation in addition to QCP-n-qscd and NCP+.

9.17. Other Provisions

Not allowed.

10. References

1. 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;
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. 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;
5. ETSI Drafting Rules (Verbal forms for the expression of provisions): https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/37_directives_apr_2017_part2%20(EDRs).pdf;
6. Certificate and OCSP Profile for Mobile-ID of Lithuania, published: https://www.skidsolutions.eu/en/repository/profiles/;
7. Terms and Conditions for Use of Certificates of Mobile-ID of Lithuania, published: https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/;
8. Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current;
9. General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
10. ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
11. ETSI EN 419 211 Protection profiles for secure signature creation device;
12. SK ID Solutions AS - EID-Q SK Certification Practice Statement, published: https://www.skidsolutions.eu/en/repository/CPS/;
13. Mobile-ID REST API: https://github.com/SK-EID/MID.