SK ID Solutions AS - Certificate Policy for Qualified Smart-ID

OID: 1.3.6.1.4.1.10015.17.2

Document Information	
Name	Certificate Policy for Qualified Smart-ID
Version No	10.1
Version History	
Date and Version No	Changes
05.12.2024 10.1	• Included references of eIDAS electronic identification requirements applicable to Authentication Certificates.
15.04.2024 10.0	• Regular review and update of references performed; • Clause 1.6.1 – Amended definition of 'Smart-ID App'; • Clause 4.9.1 – Amended options for Certificate revocation in case of vital status change; • Clause 4.9.2 – Added that RA can request Certificate revocation due to mistake made during Certificate application process.
17.05.2022 9.0	• Clause 3.2.5 - removed restriction for minors in Automated Biometric Identity Verification process; • Clause 3.3.1 - improved wording; • Clause 4.1.2 - added that in case of minor the Secondary Subscriber Authentication is substituted with legal representative's consent; • Clause 4.4.2 - corrected wording for CSR content.
17.02.2022 8.0	• Clause 1.1 – added reference for app stores, where Smart-ID application can be downloaded from; • Clause 1.6.1 – refined definition of Registration Authority; • Clause 4.9.1 – refined circumstances for revocation of certificates.

12.05.2021 7.0	• Throughout the document replaced term 'reliable source' with 'authoritative source'; • clause 1.1 – updated user identity verification methods and removed RA procedure to upgrade from non-qualified Smart-ID to Qualified Smart-ID; • clause 1.3.5, 1.6.1 – clarified term 'Identity Provider'; • clause 1.3.5, 1.6.1, 3.2.3, 4.2.2, 9.6.5, 10. - added new participant Secondary Subscriber Authentication Provider and Secondary Subscriber Authentication process with respective amendments in CP; • clause 1.5.2, 1.5.4 - replaced business development manager with head of trust services; • clause 1.6.1 – added term 'Electronic Machine Readable Travel Document'; • clause 1.6.1, 10. - updated name of CPS; • clause 2.2.1 - updated SK website hostname; • clause 3.2.3 – refined wording of clause; • clause 4.1.2 – clarified CA right for validating data of Subscriber and his/her legal representative; replaced requirement that in case of Automated Biometric Identity Verification, the Subscriber SHALL have or have had Smart-ID Account. Instead Secondary Subscriber Authentication is performed; • clause 4.2.2 - added substantial match for Subscriber's and his/her legal representative's data, and refusal basis threat to Smart-ID System or Subscriber identity; clarified refusal basis in case of invalid signature.Clause 4.9.1 - added SK rights to revoke Certificates if Subscriber's personal details have changed or Subscriber's vital status has changed; • clause 10 - updated weblink of Electronic Identification and Trust Services for Electronic Transactions Act.
21.02.2020 6.0	• Added issuance of Q Smart-ID via Automated Biometric Identity Verification. Therefore, clauses 1.1, 1.3.2, 1.3.5, 1.6.1, 1.6.2, 3.2.3, 3.2.5, 4.1.2, 4.2.1, 4.2.2, 4.4.1 and 9.6.5 of this CP have been amended accordingly; • clause 1.5.4 - added that SK performs annual review of this CP; • clause 4.2.2 - added that CA shall refuse to issue a Certificate if the Subscriber's or his/her legal representative's data in the Certificate application does not match with the data from reliable source. Additionally replaced the grounds "The Subscriber's or his/her legal representative's data in Certificate request does not match with the data from reliable source" with the following "The Subscriber's or his/her legal representative's data in CSR does not match with the Subscriber's identification data in the Certificate application."; • clause 4.9.1 - left out that if SK has withdrawn Identity Provider status, SK has the right to revoke all the Certificates which were issued for identities provided by this Identity Provider.
08.11.2018 5.0	• Certification service for Q Smart-ID is provided in accordance with the requirements of the Policy QCP-n-qscd. Therefore, clauses 1.1, 1.2, 1.4.1, 1.4.2, 1.6.2, 6.1.1, 6.2.1 and 6.2.8 have been amended accordingly; • please note: Issuance of the Certificates for Q Smart-ID under the Policy QCP-n was performed until 07.11.2018. These Certificates shall be served in accordance with this Certificate Policy until the validity of the last Certificate pair issued under the Policy QCP-n.

06.07.2018 4.1	• Specified circumstances for certificate re-key in clause 4.7.1; • clause 9.15 - replaced General Data Protection Act with General Data Protection Regulation; • amended the wording throughout the document; • updated the references in paragraph 10.
01.06.2017 4.0	• Added requirements for Certificate issuance to minors. Therefore, clauses 3.2.5, 4.1.2 and 4.2.2 of this CP have been changed accordingly; • specified formulation and replaced "national population registry" with "reliable source" in clauses 4.1.2, 4.2.1 and 4.2.2 of this CP.
01.04.2017 3.0	• Amended and corrected the CP throughout due to adding issuance of the Certificates in RA office; • amended the wording and added specifications and corrections throughout the document; • clause 4.7.3 - specified formulation when old certificates shall be revoked.
16.01.2017 2.0	• Chapter 1.1 - replaced existing identity document with valid Qualified Electronic Signature Certificate and added Q Smart-ID; left out description of issuance of Qualified Smart-ID in the next phases; • chapter 4.2.2 - added that CA may refuse to issue a Certificate if the Subscriber's signature of the application for Q Smart-ID is not given with his/her existing Q Smart-ID.
01.01.2017 1.0	• First public edition.
Effective from date	05.12.2024

1. Introduction

1.1. Overview

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

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

The Subscriber may apply for a Q Smart-ID Account online or via Automated Biometric Identity Verification as well physically in the office. The user has to install the special application from the app store referred on www.smart-id.com webpage and perform the registration process. The application can be used with any modern smartphone or tablet, no SIM-cards or card-readers are required. During the registration, the user identity is verified using methods defined in eIDAS article 24 (1) points (a), (b), (c) and (d).

A Subscriber can have several active Smart-ID Accounts unless imposed otherwise. Every mobile device owned by the Subscriber may be related to only one Smart-ID Account, which contains a Certificate Pair. The Subscriber can keep track of Smart-ID Accounts by using a self-service Smart-ID Portal.

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

This document describes only restrictions to the Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD (QCP-n-qscd) from ETSI EN 319 411-2 [4] and Normalised Certificate Policy requiring a Secure Cryptographic Device (NCP+) from ETSI EN 319 411-1 [3].

The semantics of "no stipulation in 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 Q Smart-ID is based on the requirements of the Policy QCP-n-qscd: Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD.

Issuing and managing Authentication Certificates for Q Smart-ID is based on the requirements of the COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 [15] and the Policy NCP+: Normalised Certificate Policy requiring a Secure Cryptographic Device.

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

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

- QCP-n-qscd;
- NCP+;
- this CP;
- CPS.

To preserve IETF RFC 3647 [2] outline, this CP is divided into nine parts, section headings that do not apply, are designated as **"Not applicable"**. Each top-level chapter includes references to the relevant sections in ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

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

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

1.2. Document Name and Identification

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

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

This CP is identified by OID: 1.3.6.1.4.1.10015.17.2

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

Parameter	OID reference
Internet attribute	1.3.6.1
Private entity attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	17.2

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

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

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

- This CP.

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

- ETSI EN 319 411-1 [3] clause 5.3 b) for NCP+: 0.4.0.2042.1.2;

  itu-t(0) identified-Organisation(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
- This CP.

1.3. PKI Participants

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

1.3.1. Certification Authorities

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

1.3.2. Registration Authorities

In case of electronic authentication RA duties are performed by Smart-ID Provider.

In case of Subscriber Authentication via physical presence checks, RA duties are performed by customer service points.

1.3.3. Subscribers

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

Subscriber can be only a natural person.

1.3.4. Relying Parties

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

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

1.3.5. Other Participants

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

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

Identity Provider is an organisation who is providing electronic identification means under electronic identification scheme and who is responsible for creating electronic identities which are used for issuing Q Smart-ID Certificates.

Biometric Verification Provider is an organisation who offers eMRTD reading and validation services, service for biometric verification and liveness detection of Subscriber during Automated Biometric Identity Verification.

Secondary Subscriber Authentication Provider is an organisation who facilitates or performs Secondary Subscriber Authentication during enrolment process. Purpose of Secondary Subscriber Authentication is ensuring Subscriber awareness about ongoing Smart-ID registration.

1.4. Certificate Usage

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

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes:

Certificate for Electronic Signature is intended for:

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

Authentication Certificate is intended for:

- authentication.

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

- Subscriber Certificates compliant with NCP+ or QCP-n-qscd;
- OCSP response verification Certificates.

1.4.2. Prohibited Certificate Uses

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

- unlawful activity (including cyber attacks and attempt to infringe the Certificate or the Smart-ID System);
- issuance of new Certificates and information regarding Certificate validity;
- enabling other parties to use the Subscriber's Private Key;
- enabling the Certificate issued for electronic signing to be used in an automated way;
- using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

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

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, SHALL be documented in the Versions and Changes section of this document.

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

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

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

Amendments which are relevant to RA 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
Advanced Electronic Signature	Electronic Signature which meets the requirements provided in Article 26 of eIDAS [6].
Advanced Electronic Signature Certificate	Advanced Electronic Signature Certificate according to eIDAS [6].
Authentication	Unique identification of a person by checking his/her alleged identity.
Authentication Certificate	Certificate is intended for Authentication.
Automated Biometric Identity Verification	Remote on-boarding process for Q Smart-ID by using the Smart-ID App wherein the Subscriber's identity is verified by his/her biometric characteristics.
Biometric Verification Provider	An organisation who offers eMRTD reading and validation services, service for biometric verification and liveness detection of Subscriber during Automated Biometric Identity Verification.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [12], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates 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.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed and used.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Distinguished Name	Subject name in the infrastructure of Certificates that is unique for every Subscriber.
Electronic Machine Readable Travel Document	An identity or travel document (ID-card or passport) that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the document holder.
E-Service Provider	A 3rd party, which uses services provided by the Smart-ID System to authenticate Subscribers and to allow Subscribers to electronically sign documents or transactions.
Identity Provider	An organisation who is providing electronic identification means under electronic identification scheme and who is responsible for creating electronic identities which are used for issuing Q Smart-ID Certificates. Identity Provider has been verified by Smart-ID Provider to follow the Requirements for Identity Providers [13] for qualified certificates.

Term	Definition
Mobile Device	A tablet computer or smartphone that runs a mobile device operating system (Apple iOS, Google Android).
Object Identifier	An identifier used to uniquely name an object (OID).
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. In the Smart-ID system, the value of Private Key itself is never generated and the Private Key exists only in the form of its components.
Public Key	The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key.
Q Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the qualified Electronic Signature Certificate and their corresponding Private Keys.
Qualified Electronic Signature	Qualified Electronic Signature according to eIDAS [6].
Qualified Electronic Signature Certificate	Qualified Electronic Signature Certificate according to eIDAS [6].
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications and Certificate revocation applications, check the applications and/or forward the applications to the Certificate Authority.
Relying Party	Entity that relies on the information contained within a Certificate.
Secondary Subscriber Authentication	A process that ensures Subscriber awareness about ongoing Smart-ID registration. The authentication method for verifying Subscriber awareness is either delivery of authentication message to Subscriber or requesting Subscriber to perform authentication with electronic identification mean. Secondary Subscriber Authentication provides definite and integral connection to information stating creation of a new Smart-ID account for Subscriber.
Secondary Subscriber Authentication Provider	An organisation, which facilitates or performs Secondary Subscriber Authentication during enrolment process for assurance of Subscriber awareness. Secondary Subscriber Authentication Provider is responsible for delivering authentication messages to Subscriber or for performing Secondary Subscriber Authentication with electronic identification mean. Secondary Subscriber Authentication Provider has been verified by Smart-ID Provider to follow the Requirements for Secondary Subscriber Authentication Providers [14].
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.

Term	Definition
Smart-ID Account	Subscriber has to register a Smart-ID Account to use services provided by the Smart-ID System. Smart-ID Account binds Smart-ID App instance to a Subscriber's identity in the Smart-ID System. In the course of Smart-ID Account creation and registration, the identity of the Smart-ID Account owner (Subscriber) is proofed by a Registration Authority and the relation between the identity and a key pair is certified by a Certificate Authority. Smart-ID Account has an Advanced or Qualified Electronic Signature key and an Authentication key.
Smart-ID App	A technical component of the Smart-ID System. A Smart-ID App installed on a Subscriber's Mobile Device that provides access to qualified Smart-ID service. Smart-ID App may have a companion app that facilitates specific user interactions with Smart-ID App. Companion app is installed on smart device that is securely linked with Subscriber's Mobile Device.
Smart-ID Portal	The interaction point with the Smart-ID System for the Subscriber that is accessible via a web browser. The Portal provides access to Smart-ID Account registration and management functionality.
Smart-ID Provider	An organisation that is legally responsible for the Smart-ID System. SK is the Smart-ID provider.
Smart-ID Server	A technical component of the Smart-ID System, handles back-end operations.
Smart-ID System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The Smart-ID System provides services that allow Subscribers (Smart-ID Account owners) to authenticate themselves to services, to give Electronic Signatures, and to manage their Smart-ID Accounts.
Subject	In this document, the Subject is the same as the Subscriber.
Subscriber	A natural person to whom the Q Smart-ID Certificates are issued.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions [11] upon receipt of the Certificates.
UTF-8	Variable length character encoding which uses 8 bit code units capable of encoding all possible characters defined by Unicode.
Verified Electronic Authentication	Electronic Authentication based on Identity Provider that has been verified to follow the Requirements for Identity Providers [13] for qualified certificates.

1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy. This document is a CP.
CPS	Certification Practice Statement
CSR	Certificate Signing Request

Acronym	Definition
eIDAS	Regulation (EU) No 910/2014 [6] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
eMRTD	Electronic Machine Readable Travel Document
EU	European Union
HSM	Hardware security module is a physical computing device that safeguards and manages digital cryption keys and provides cryptoprocessing.
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [3].
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PKI	Public Key Infrastructure
QCP-n-qscd	Policy for EU qualified Certificates issued to natural persons where the Private Key and the related Certificate reside on a QSCD from ETSI EN 319 411-2 [4].
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority
SK	SK ID Solutions AS, Certification Service provider

2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [3] and ETSI EN 319 411-2 [4].

2.1. Repositories

SK SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled 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 CPS [1], the Certificate Profile [12], as well as the Terms and Conditions [11] together with the enforcement dates SHALL be published on SK website https://www.skidsolutions.eu/resources/ no less than 30 days prior to taking effect.

2.2.2. Items not Published in the Certification Practice Statement

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

2.3. Time or Frequency of Publication

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

2.3.1. Directory Service

Not applicable.

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

3.1. Naming

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

3.1.1. Type of Names

No stipulation 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

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

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

Identity of Subscriber is verified prior to requesting issuance of the Subscriber's Certificates from the CA.

RAs in form of customer service points SHALL perform Subscriber identification by the physical presence checks.

RAs in form of electronic environments SHALL perform Subscriber identification remotely by:

- using electronic identification means of Verified Electronic Authentication; or
- means of a certificate of a qualified electronic signature, which has been issued in compliance with eIDAS article 24 (1) point (a) or (b); or
- using Automated Biometric Identity Verification.

In case of Automated Biometric Identity Verification, Biometric Verification Provider SHALL perform Subscriber Authentication by:

- verifying authenticity of the Subscriber's eMRTD presented for verification;
- reading the Subscriber's personal data from the Subscriber's eMRTD presented for verification;

- performing liveness detection of the Subscriber's facial image; and
- performing match of the Subscriber's facial image captured in the liveness session during registration with the data set on the chip on his/her eMRTD presented for verification.

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information SHALL NOT be allowed in a Certificate.3

3.2.5. Validation of Authority

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

Applying for Q Smart-ID through a representative SHALL be permitted only to minors.

The Subscriber SHALL have legal capacity, except for the minor.

CA MAY verify the right of representation of the Subscriber's legal representative.

3.2.6. Criteria for Interoperation

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

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

RA SHALL perform Subscriber Authentication using means of Verified Electronic Authentication, Automated Biometric Identity Verification or via physical identification prior to requesting issuance of the Subscriber's Certificates from the CA.

Application SHALL be signed with Qualified Electronic Signature compliant with eIDAS Regulation [6], handwritten signature or existing valid Q Smart-ID Qualified Electronic Signature Certificate.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to Clause 3.2 of this CP.

3.4. Identification and Authentication for Revocation Request

No stipulation 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 [3] and ETSI EN 319 411-2 [4].

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Certificate application MAY be submitted by the Subscriber via RA.

SK SHALL accept Certificate applications only from RA.

Certificate application process SHALL ensure that the Subject has possession or control of the Private Key associated with the Public Key presented for certification.

4.1.2. Enrolment Process and Responsibilities

Subscriber WILL request for Certificates in the Smart-ID App upon successful Verified Electronic Authentication, biometric verification or physical identification in RA office.

RA or Biometric Verification Provider SHALL perform Subscriber identity verification.

CA MAY validate data presented about Subscriber and his/her legal representative against authoritative source.

In case of Automated Biometric Identity Verification, Secondary Subscriber Authentication SHALL be performed by Secondary Subscriber Authentication Provider. If Subscriber is minor, then Secondary Subscriber Authentication is substituted with legal representative's consent confirmed with signing the application by legal representative.

CA SHALL verify that the data in CSR matches the data in the Certificate used for application signing or with data on the application from customer service point.

If CA cannot verify the Subscriber or his/her legal representative or the right of representation of the legal representative from authoritative source, CA SHALL NOT issue Certificate.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber's identity SHALL be validated by RA by means of Verified Electronic Authentication or physical identification or by Biometric Verification Provider in case of Automated Biometric Identity Verification.

The Subscriber SHALL accept the Terms and Conditions [11].

The Subscriber SHALL submit Certificate application.

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

CA SHALL accept 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 Certificate request does not comply with the technical requirements set in the applicable agreements;
- the Subscriber's or his/her legal representative's data in the Certificate application does not match substantially with the data from authoritative source;
- the Subscriber's data in CSR does not match with the Subscriber's identification data in the Certificate application;

- the Subscriber's or his/her legal representative's signature for the application for Q Smart-ID is invalid (incl. Qualified Electronic Signature does not meet the requirements laid out in eIDAS Regulation [6];
- the signatory of the application for Q Smart-ID is a person other than the Subscriber or his/her legal representative;
- the Subscriber lacks legal capacity or his/her legal representative lacks right of representation;
- the eMRTD is unsuccessfully used for biometric verification and there is a reasonable doubt for its misuse;
- integrity and trustworthiness of the data read from the eMRTD cannot be verified;
- the eMRTD has not been issued by a respective document issuer;
- authenticity of the eMRTD cannot be verified;
- the facial image read from the data set on the chip on eMRTD does not match with the facial image of the Subscriber performing the liveness session;
- the liveness of the Subscriber's facial image cannot be verified;
- the eMRTD is expired or revoked;
- the Secondary Subscriber Authentication is unsuccessfully performed;
- Smart-ID System's security monitoring mechanism has detected threat to system or Subscriber identity.

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

4.2.3. Time to Process Certificate Applications

In accordance with the applicable agreements.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

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

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

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

Smart-ID App SHALL notify the Subscriber of the new Certificate issuance.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

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

Subscriber SHALL confirm correctness of the issued Certificate.

This confirmation SHALL be treated as Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

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

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

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

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

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

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

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

4.7.1. Circumstances for Certificate Re-Key

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

Certificate re-key SHALL be allowed also for fixing invalid Certificates that do not comply with the Certificate Profile [12].

In case of re-key for fixing invalid Certificate, if the Subscriber's data has been changed, the Subscriber SHALL submit the new certificate application.

4.7.2. Who May Request Certification of a New Public Key

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

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

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

4.7.3. Processing Certificate Re-Keying Requests

The Certificate re-key process is as follows:

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

In case the new Certificates are issued for a Mobile Device with an existing Smart-ID Account, old Certificates of the existing Smart-ID Account SHALL BE revoked.

In case fixing invalid Certificates the erroneous Certificates SHALL BE revoked.

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

4.7.4. Notification of New Certificate Issuance to Subscriber

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

Smart-ID App SHALL notify the Subscriber of the new Certificate issuance.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to Clause 4.4.1 of this CP.

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

Refer to Clause 4.4.2 of this CP.

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

Refer to Clause 4.4.3 of this CP.

4.8. Certificate Modification

Not allowed.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances for Certificate revocation SHALL be as laid down in Article 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [7].

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

In addition to the circumstances in the Electronic Identification and Trust Services for Electronic Transactions Act and more precisely, SK has the right to revoke the Q Smart-ID Certificate if one or more of the following occurs:

- the Subscriber requests revocation of the Certificates using the Smart-ID App or Smart-ID Portal or using for identification the RA;
- the Subscriber has blocked the PIN codes;
- SK obtains evidence that Subscriber has lost control over Private Keys or PIN codes;
- the Subscriber notifies SK that the original Certificate request was not authorised and does not retroactively grant authorisation;
- SK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements;
- SK obtains evidence that the Certificate was misused;
- SK obtains evidence from authoritative source that Subscriber's personal details have changed, and Subscriber has not revoked his/her Certificates during a reasonable time;
- SK obtains evidence from authoritative source or authoritative evidence is presented to RA that Subscriber's vital status has changed;
- 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 is made aware that the Certificate was used for unlawful activity (including cyber-attacks and attempt to infringe the Certificate of the Smart-ID System) or there is reasonable doubt for committing unlawful activity;
- SK determines that any of the information appearing in the Certificate is inaccurate or misleading;
- SK ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- SK's right to issue Certificates is revoked or terminated, unless SK has made arrangements to continue maintaining the OCSP repository;
- SK is made aware of a possible compromise of the Private Key of the SK CA used for issuing the Certificate;
- revocation is required by the CP;
- the technical content or format of the Certificate presents an unacceptable risk to Relying Parties.

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

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

4.9.2. Who Can Request Revocation

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

RA MAY request revocation of the Subscriber's Certificates on the basis of Subscriber application or when RA did not conduct Certificate application process in accordance with the CPS and/or CP.

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

4.9.3. Procedure for Revocation Request

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

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

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

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

6. Technical Security Controls

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

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

- Smart-ID Server and Smart-ID App SHALL generate RSA key pairs independently;
- Smart-ID Server's Private Key SHALL be generated on a QSCD;
- Smart-ID App SHALL further divide its Private Key into two parts. The two parts SHALL NOT BE distinguished from random numbers;
- Smart-ID App SHALL send one of these parts to the Smart-ID server over a secure communication channel;
- Smart-ID Application SHALL NOT store the key part sent to the Smart-ID Server, and SHALL store the other part encrypted and protected with activation data.

6.1.2. Private Key Delivery to Subscriber

Not applicable.

6.1.3. Public Key Delivery to Certificate Issuer

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

6.1.4. CA Public Key Delivery to Relying Parties

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

6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [12].

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation 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 [12].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The HSM module used to generate server's Private Keys SHALL be a QSCD.

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

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

The Subscriber SHALL be prompted to enter the PIN code before any single operation done with the Private Key.

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

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

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 [12].

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

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

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

6.4.2. Activation Data Protection

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

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

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

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+.

6.7. Life Cycle Security Controls

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

6.8. Network Security Controls

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

6.9. 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 [3] and ETSI EN 319 411-2 [4].

7.1. Certificate Profile

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

7.2. CRL Profile

Not applicable.

7.3. OCSP Profile

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

8. Compliance Audit and Other Assessments

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

9. Other Business and Legal Matters

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

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No stipulation 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+.

9.3.1. Scope of Confidential Information

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

9.3.2. Information Not Within the Scope of Confidential Information

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

9.3.3. Responsibility to Protect Confidential 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

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

9.6.2. RA Representations and Warranties

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

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

Before giving out Identity Provider status to entity, Smart-ID Provider SHALL evaluate the identity quality level of the entity by verifying that this entity is following Requirements for Identity Providers [13] for qualified certificates.

In case Smart-ID Provider obtains evidence that Identity Provider has not been following Requirements for Identity Providers [13] for qualified certificates it CAN withdraw Identity Provider status of this entity.

Identity Provider SHALL follow the Requirements for Identity Providers [13] for qualified certificates.

Biometric Verification Provider SHALL follow the requirements stipulated in the agreement concluded with SK.

Secondary Subscriber Authentication Provider SHALL follow the Requirements for Secondary Subscriber Authentication Providers [14].

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 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 [6] - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [15];
- Electronic Identification and Trust Services for Electronic Transactions Act [7];
- 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 [3];
  - 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 [4];
  - EN 419 211 Protection profiles for secure signature creation device [8];
- national norms on trust services and electronic identification of countries, where Smart-ID is provided.

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. SK ID Solutions AS - EID-Q SK Certification Practice Statement, published: https://www.skidsolutions.eu/resources/certification-practice-statement/;
2. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt;
3. ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
4. ETSI EN 319 411-2 V2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
5. ETSI Drafting Rules (Verbal forms for the expression of provisions);
6. eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
7. Electronic Identification and Trust Services for Electronic Transactions Act, published: https://www.riigiteataja.ee/en/eli/ee/506032023001/consolide/current;
8. ETSI EN 419 211 Protection profiles for secure signature creation device;
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 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
11. Terms and Conditions for Use of Certificates of Qualified Smart-ID, published: https://www.skidsolutions.eu/resources/conditions-for-use-of-certificates/;
12. Certificate and OCSP Profile for Smart-ID, published: https://www.skidsolutions.eu/resources/profiles/;
13. Requirements for Identity Providers, published: https://www.skidsolutions.eu/resources/requirements-by-sk/;
14. Requirements for Secondary Subscriber Authentication Provider, published: https://www.skidsolutions.eu/resources/requirements-by-sk/;
15. COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.