SK ID Solutions AS - EID-Q SK Certification Practice Statement

Document Information	
Name	EID-Q SK Certification Practice Statement
Version No	10.0
Version History	
Date and Version No	Changes

12.05.2021 10.0	• Description of new SK`s PKI hierarchy has been added to this CPS and removed reference to subordinate CA EID-SK 2011 due to its revocation on October 1st, 2020. Therefore clauses 1.1, 1.3.1 and 4.9.7 have been amended accordingly; • throughout the document removed provisions describing certification service for SEB-card. Clause 1. - removed geographical determination for provision of SK services; • clause 1.1, 1.3.2.1.2, 1.3.2.2.1, 1.3.2.2.2, 2.2.1 - updated SK website hostname; • clause 1.2 - updated document name to reflect distinctly dependencies with new SK's PKI hierarchy; • clause 1.3.1 – removed Mobile-ID reference to Lithuania; • clause 1.3.2.1.1 - added that in case of ABIV the Smart-ID Provider acts as RA; • clause 1.3.2.1.4 - corrected website link for Smart-ID Help Line information; • clause 1.3.5.1.2, 1.6.1 - clarified term 'Identity Provider'; • clause 1.3.5.1.4, 1.6.1, 4.1.2.1.3, 9.6.5.1.4, 10. - added new participant Secondary Subscriber Authentication Provider and Secondary Subscriber Authentication process with respective amendments in CPS; 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, 4.4.2.2, 9.1.2, 9.1.3, 10. - defined Mobile-ID Service Integration API introduction due to Digidoc Services decommission; • clause 3.2.3.1 - replaced 'document validity checking service offered by the eMRTD issuing country' with 'authoritative source'; • clause 4.1.2.1.1, 4.1.2.1.2 - clarified data validation circumstances; • clause 4.1.2.1.3 – added reference to 'Consent for Automated Biometric Identity Verification', and 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 4.2.1.2.4 - removed process for upgrade from non-qualified Smart-ID to Qualified Smart-ID in Customer Service Point;Clause 4.9.4.1 - added conditions about loss of control over Private key(s), or PIN codes; • clause 4.9.9 – specified that OCSP responses for the Certificates issued by EID-SK 2016 are signed by OCSP signer certificate; • clause 6.1.1.1.1, 6.1.2.1.2, 6.1.5.1 – updated key sizes; • clause 9.1.1 - fees are published on SK website; • clause 9.6.1.1 - added possibility for SK to share data with Relying Party; • clause 9.6.3.1 - added Subscriber obligations to revoke Certificates in case of control loss over PIN codes or in case of a change in Subscriber personal details to revoke Certificates during a reasonable time;

	• clause 11. - Annex 1 removed and Requirements of Identity Validation for RA published in SK's public information repository; • throughout the document replaced term 'reliable source' with 'authoritative source'.
10.04.2020 9.0	• Please note: Qualified Electronic Signature and Authentication Certificates for SEB-card were issued until April 2019. Servicing (suspension, termination of suspension, revocation) of the Certificates for SEB-card was carried out until March 2020. As of March 2020 SK no longer provides certification service for SEB-card (except certificate status information that is provided until and beyond expiry of the last Certificate issued according to this Certification Practice Statement) and revokes all Certificates that have been issued for SEB-card. Therefore, as of 10.04.2020, the provisions describing issuance and servicing of the referred Certificates are no longer valid; • however, the provisions on the issuance and servicing of the Certificates for SEB-card have been left in this Certification Practice Statement to facilitate understanding how certification service for SEB-card was performed; • clause 1.3.1 - specified that Certificates are issued and served by intermediate CA EID-SK 2016 and intermediate CA EID-SK 2011 solely provides Certificate status information; • clause 1.5.4 - added that SK performs annual review of this CPS; • clause 4.1.2.3.1 - specified that the Subscriber signs Mobile-ID agreement with MO with their handwritten signature; • clauses 4.4.2 and 4.4.3 - specified that the Certificates are sent to Smart-ID System and not published therein as stated in the previous version of this CPS; • clause 4.9.3.2 - specified that in case of revocation of Q Smart-ID Certificates, OCSP no longer responds with "GOOD"; • clause 9.6.1.2 - added that SK is obligated to ensure that the Smart-ID App includes the component that has been recognised as part of QSCD; • clause 9.6.3.2 - specified that the Subscriber is solely responsible for the maintenance of the part of the Private Key and PIN codes that are in his/her possession; added that the Subscriber ensures that he/she uses the Smart-ID App that is distributed by SK;
21.02.2020 8.0	• Added issuance of Q Smart-ID via Automated Biometric Identity Verification. Therefore, clauses 1.3.5, 1.6.1, 1.6.2, 3.2.3.2, 3.2.5.2, 4.1.2, 4.2.1, 4.2.2, 9.6.3.2 and 9.6.5 have been amended accordingly; • clause 1.3.2.2.4 - removed contact details of Customer Service Point Help Line; • clauses 6.2.8.2.2 and 6.2.8.2.3 - specified how "Server's part of the private key" and 'Server's share of the private key' respectively is activated.

08.11.2018 7.0	• Certification service for Q Smart-ID is provided in accordance with the requirements of the Policy QCP-n-qscd. Therefore, clauses 1.1, 1.6.2, 6.1.2.2 and 9.6.1.2 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 are served in accordance with this Certification Practice Statement until the validity of the last Certificate pair issued under the Policy QCP-n; • additionally, clause 4.1.2.2.3 has been added to this CPS to describe how SK verifies that Q Smart-ID is continually recognised as QSCD.
24.10.2018 6.2	• Clause 1.1 - added new certificate chain and updated figure of PKI hierarchy; • clause 1.6.1 - specified definitions for QSCD and CRL; • clause 2.2.1 – added statement that SK provides capability to allow third parties to check and test Certificates it issues, and that test Certificates clearly indicate that they are for testing purposes; • clause 4.1.2 - specified data included in the Subscriber's Certificate application; amended what is considered acceptance of Q Smart-ID Certificates. Therefore, clauses 4.1.2.2, 4.4.1.2 and 4.7.5 have been amended accordingly; • added clause 4.1.3 to state how SK verifies QSCD status of the devices; • clause 4.9.7 – added statement that CRL is signed by EID-SK 2011; • clause 4.9.9 - added that OCSP contains Certificate status information until the Certificate expires; • clause 9.6.3 - amended the Subscriber's obligations.
06.07.2018 6.1	• clause 4.9.3.2 - added possibility for the Subscriber to request revocation of Q Smart-ID Certificates by deleting his/her Smart-ID Account; • due to adding additional Q Smart-ID key sizes, clauses of 6th Chapter have been amended accordingly; • clauses 6.1.2.2.2 and 6.7.2 - added description of additional security measure (TEK key usage) to protect communication between Smart-ID App and Smart-ID Server; • clause 6.4.2.2 - left out "Smart-ID App generates random activation codes and displays them once to the Subscriber."; • clause 9.15 - replaced General Data Protection Act with General Data Protection Regulation; • minor corrections in wording.

01.03.2018 6.0	• Added issuance and service of Mobile-ID Certificates in Lithuania. Therefore, the CPS has been complemented throughout; • clause 4.9.11 - added how revocation status information of the expired Certificate can be requested; • clause 4.11 - added that maximum validity period of the Certificate is stipulated in certificate profiles; added that subscription ends due to expiration of the Certificate; • clause 9.6.1 - added statements on how SK contributes to making its services accessible to people with disabilities; • clause 9.6.2 - added statements on how RAs assist with making certification services accessible to people with disabilities; • clause 1.6.2 - minor corrections; • minor corrections in wording.
1.11.2017 5.0	• Removed issuance of the Certificates by AS SEB Banka and AB SEB Bankas. Therefore, clauses 1.3.2.1.1, 1.6.2, 4.4.1.1 and 4.9.3.1 of this CPS have been amended accordingly; • added that the Subscriber is entitled to request revocation of Q Smart-ID Certificates via Customer Service Point Help Line. Therefore, clauses 1.3.2.2.4 and 4.9.3.2 of this CPS have been amended accordingly; • clause 6.1.5.1 - left out RSA keys and added new key size of ECC algorithm; • clause 9.6.2.3 - added that Customer Service Point forwards the applications for revocation of Q Smart-ID Certificates to SK; • minor corrections in wording.
1.06.2017 4.0	• Added the procedure of Certificate issuance to minors. Therefore, clauses 3.2.5.2, 4.1.2.2.1, 4.1.2.2.2, 4.2.2.2 and 4.4.1.2 of this CPS have been changed accordingly; • specified formulation and replaced "national population registry" with "reliable source" in clauses 4.1.2.2.1, 4.1.2.2.2 and 4.2.2.2 of this CPS.

1.04.2017 3.0	• Amended and corrected the CPS throughout due to adding issuance of the Certificates in RA office; • amended the wording throughout the CPS; • amended the wording and added specifications and corrections related to issuance of the Certificates on the SEB-card; • clause 1.1 - updated the figure showing the relations between the Root CA, Subordinate CA-s and the CP-s; • clause 1.3.2.2.4 - added Latvian and Lithuanian Help Line numbers; • clause 3.2.3.2 - added statement about verifying physical identification of the Subscriber to assure compliance with art 24 (a) of eIDAS Regulation; • clause 4.2.2.2 - removed the ground that gave SK a right to refuse from issuing Certificates if the Subscriber's signature of the application for Q Smart-ID was not given with his/her existing Q Smart-ID/NQ Smart-ID; • clause 4.4.1.1 – specified the activities the Subscriber has to carry out in order to activate his/her SEB-card certificates. Left out the requirement that the SEB Customer Service Point employee processing the application for activation must be different from the one who handed over the SEB-card; • added that certificate re-key is performed to fix errors during certification of Qualified Smart-ID. Therefore, clauses 4.7.1.2-4.7.4.2 have been supplemented accordingly; • clause 4.7.3.2 - removed the process of certificate re-key, ie. the Subscriber's right to apply for Qualified Smart-ID with his/her existing Qualified Smart-ID or non-qualified Smart-ID.
16.01.2017 2.0	• Chapter 1 – removed paragraph which stated that the current document is a complete redesign of the previous "AS Sertifitseerimiskeskus – Certification Practice Statement" and "SEB-card Certification Policy"; • chapter 1.2 – removed "This is the first version of this document."; • chapter 1.6.1 – added the term Advanced Electronic Signature; • chapter 4.2.2.2 – 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; • chapter 4.7.3.2 – added details of applying Q Smart-ID with existing Q Smart-ID.
1.012017 1.0	• First public version.
Effective from date	12.05.2021

1. Introduction

SK ID Solutions AS (hereinafter referred to as SK) was founded on March 26th 2001. The owners of the limited liability company are AS Swedbank, AS SEB Pank and Telia Eesti AS. The principal activities of SK are offering trust services and related technical solutions. These services guarantee secure and verified electronic communication with public institutions as well as businesses in everyday life.

Inspired by the ETSI EN 319 400 series, SK has divided its documentation into three parts:

- "SK ID Solutions AS Trust Services Practices Statement" [3] (hereinafter referred to as SK PS) describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Practice Statements describe parts that are specific to each Subordinate CA or Time-Stamping Unit;
- Technical Profiles are in separate documents.

Pursuant to the IETF RFC 3647 [2] this CPS is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [2], section headings that do not apply have the statement **"Not applicable"**. References to SK PS [3] and the "Certificate and OCSP Profile for Smart-ID" [9] (hereinafter referred to as Certificate Profile for Smart-ID) and "Certificate and OCSP Profile for Mobile-ID of Lithuania" [13] (hereinafter referred to as Certificate Profile for Mobile-ID) documents are included where applicable.

1.1. Overview

This CPS describes the practices used to comply with "SK ID Solutions AS - Certificate Policy for Qualified Smart-ID" [1] (hereinafter referred to as CP for Q Smart-ID) and "SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania" [14] (hereinafter referred to as CP for Mobile-ID).

These policies are compliant with ETSI EN 319 411-2 Policy: QCP-n-qscd [4] and ETSI EN 319 411-1 Policy: NCP+ [5].

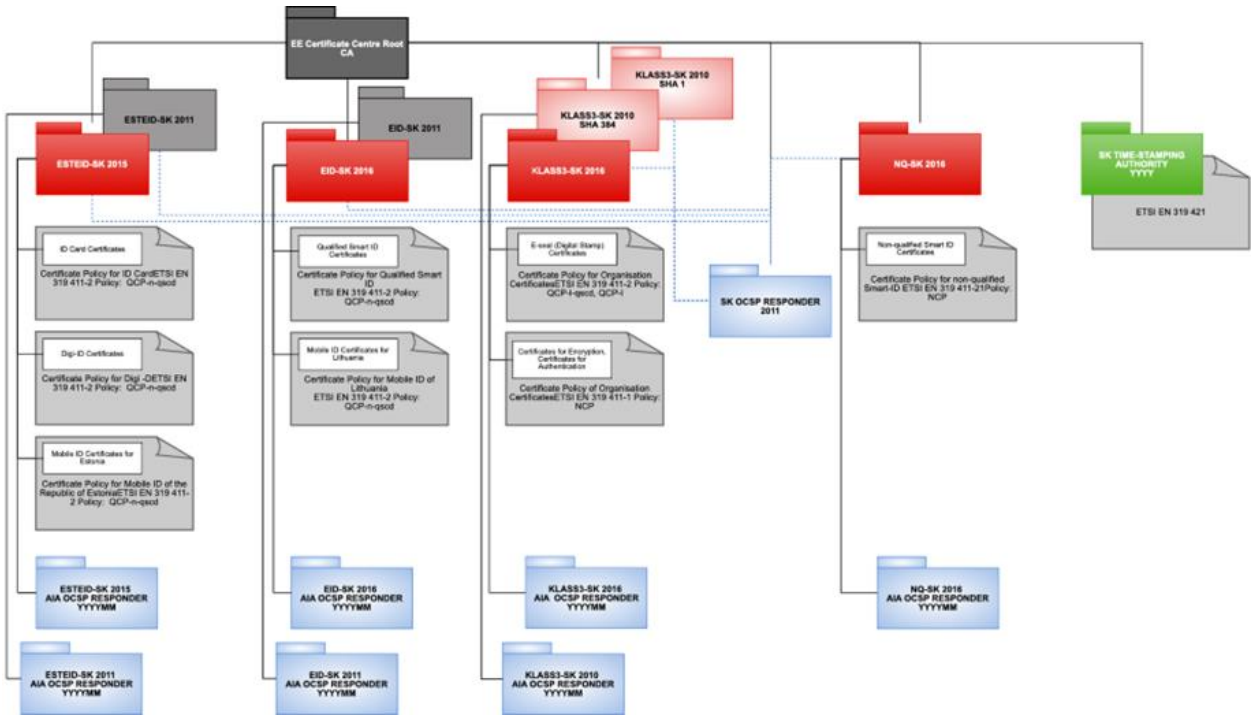
SK always ensures compliance with the latest versions of the referred documents.

SK is currently using following certificate chain:

- EE Certification Centre Root CA chain, valid 2010-2030.

The root "EE Certification Centre Root CA" has certified EID-SK 2016. The Root CA certificates and other certificates necessary for PKI operations are available from SK's website at https://www.skidsolutions.eu/en/repository/certs.

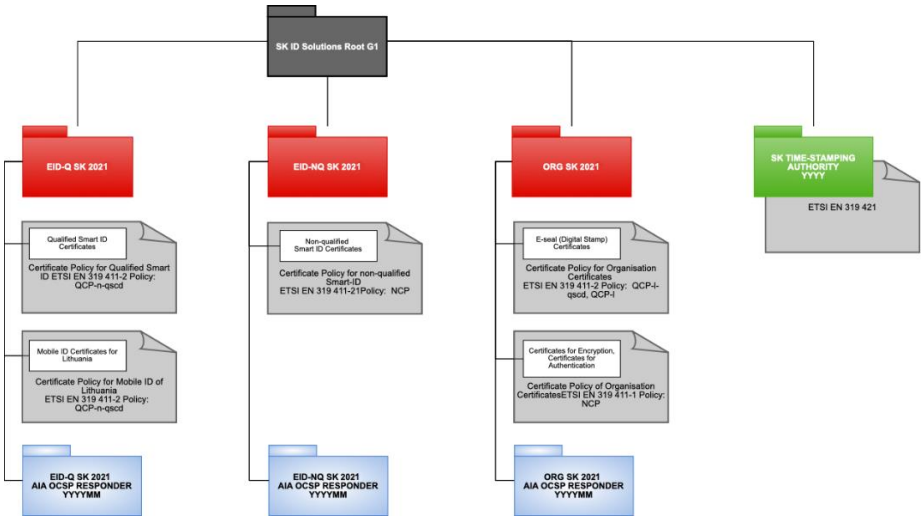
The relations between "EE Certification Centre Root CA", its subordinate CA and the CPs are shown on the following figures:



Provided that all the applicable legal requirements (conformity assessment as well as granted status by the Supervisory Body) are met, Certificates will be issued under the new, SK ID Solutions Root G1 chain. Issuing CA will be EID-Q SK 2021. The Certificates issued by the intermediate CA EID-SK 2016 will be served until expiry of the last Certificate issued by it.

The relations between SK ID Solutions Root G1 and its subordinate CAs and the CPs are shown on the following figure:

SK ID Solutions Root G1 chain, valid 2021-2036



This CPS covers operation of EID-SK 2016, which is the current issuing CA.

The certification service for Qualified Electronic Signature Certificate described in this CPS has qualified status in the Trusted List of Estonia.

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

- QCP-n-qscd;
- NCP+;
- CP for Q Smart-ID [1] and CP for Mobile-ID [14];
- This CPS.

1.2. Document Name and Identification

This document is called "SK ID Solutions AS – EID-Q SK Certification Practice Statement."

1.3. PKI Participants

1.3.1. Certification Authorities

SK operates as a Certificate Authority that issues Certificates for the Qualified Smart-ID (hereinafter referred to as Q Smart-ID) and Certificates for the Mobile-ID (hereinafter referred to as Mobile-ID).

In case of Mobile-ID, SK provides certification service under a contract signed between MO-s and SK.

The certification service provided by SK includes by default all the procedures related to the life cycle of the pairs of keys and Certificates, which are described in this CPS.

The Certificates are issued and served by the intermediate CA EID-SK 2016. Intermediate CA

EID-SK 2016 is identified by the following certificate:

1) EID-SK 2016

```
Certificate: Data: Version: 3 (0x2) Serial Number:
3b:80:3a:6b:69:c1:2a:8c:57:c5:50:05:31:1b:c4:da Signature Algorithm:
sha384WithRSAEncryption Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE
Certification Centre Root CA/emailAddress=pki@sk.ee Validity Not Before: Aug
30 09:21:09 2016 GMT Not After : Dec 17 23:59:59 2030 GMT Subject: C=EE,
O=AS Sertifitseerimiskeskus/2.5.4.97=NTREE-10747013, CN=EID-SK 2016 Subject
Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (4096 bit)
Modulus: 00:af:b5:d6:14:dd:23:d4:21:68:18:8b:95:7b:dc:
51:7b:31:27:03:44:e4:de:f9:af:22:9b:d4:45:7f:
b2:ed:9e:43:26:c7:ee:6f:69:ad:a5:22:ed:6e:15:
e3:01:ec:a7:ab:d4:15:ef:cc:e3:81:0e:f7:a4:d5:
46:87:e1:90:ea:83:c6:ec:71:7c:28:89:59:b8:86:
2c:7f:5f:a0:07:13:f1:36:22:da:d3:eb:02:5b:16:
ba:a7:81:d0:6e:07:60:61:15:46:a1:de:08:41:b8:
9b:f4:a6:ce:92:2d:f0:8c:21:b9:5a:25:a1:d5:23:
fd:a9:cb:93:65:56:3e:f7:36:b0:91:23:1f:eb:93:
f1:fd:8e:02:86:3b:4d:16:d6:3a:e8:c1:2f:b0:f0:
a1:94:71:df:b0:13:62:51:bb:59:eb:c8:c9:35:80:
84:0a:3b:64:9b:4b:f1:cf:68:a2:49:70:76:59:12:
2f:df:f8:53:ad::0c:27:60:8d:33:21:63:45:0a:
06:42:5a:47:d3:5d:3e:7d:c8:ac:39:b2:9e:c8:fc:
00:f2:42:36:d8:eb:68:f4:cc:cb:c3:b2:ac:63:9d:
b8:38:3d:c1:d4:be:4c:13:16:31:1c:3f:75:e9:72:
04:1d:3f:fd:80:13:f6:66:7f:2a:66:ef:c1:96:52:
9d:48:86:a9:38:82:56:f5:91:30:fb:7c:39:50:e5:
3a:2d:3d:ed:4d:26:c0:cd:e4:00:9c:3d:de:08:00:
4f:89:f6:30:1d:80:b4:96:62:ac:3e:94:09:aa:dc:
74:43:72:5b:9b:70:46:45:e6:22:67:d2:ae:2b:7e:
a7:17:f1:bb:f1:88:e1:33:ec:a2:a0:44:6b:d8:1f:
dc:29:fd:f5:8f:45:bf:1a:e1:af:c8:76:a4:6e:89:
30:cb:b9:ec:6c:bd:f4:b1:3b:91:2d:1e:f4:3a:a8:
b9:50:13:32:e1:ef:09:d8:27:6e:47:74:77:34:9c:
```

39:52:aa:52:70:92:1c:86:78:2c:2c:0c:7e:5a:cc:
82:d3:0d:fc:02:63:1e:c0:c0:5c:9e:5a:7f:41:b6:
a4:2a:8e:76:1e:bb:18:45:1d:66:f8:d8:42:54:30:
72:e3:92:f3:97:c2:34:fc:e1:9d:f4:89:1d:83:58:
7b:4f:b4:88:82:e6:55:a7:2c:f2:b3:c1:34:c9:fa:
dc:4b:96:0c:11:df:61:32:a5:4f:af:ba:ec:cd:70:
b3:6f:1c:b0:d2:d5:48:93:c4:0b:33:0f:e5:23:e5:
c4:d4:e8:bb:4a:48:33:03:68:b9:56:96:ba:8b:62:
b4:6a:b7:7a:18:f1:f3:46:a1:8f:4e:48:dc:e5:9e: 03:cd:93 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Authority Key Identifier: keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99 X509v3 Subject Key Identifier: 9C:09:A8:07:87:0C:3D:AC:2E:87:FC:A0:AE:D2:FB:65:49:88:28:FB X509v3 Key Usage: critical Certificate Sign, CRL Sign X509v3 Certificate Policies: Policy: 0.4.0.194112.1.2 CPS: https://www.sk.ee/repositoorium/CPS Policy: 0.4.0.194112.1.0 CPS: https://www.sk.ee/repositoorium/CPS Policy: 0.4.0.2042.1.2 CPS: https://www.sk.ee/repositoorium/CPS X509v3 Basic Constraints: critical CA:TRUE, pathlen:0 X509v3 Extended Key Usage: OCSP Signing, TLS Web Client Authentication, E-mail Protection Authority Information Access: OCSP - URI:http://ocsp.sk.ee/CA CA Issuers - URI:http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt X509v3 Name Constraints: Excluded: DNS:"" IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0 qcStatements: 0.0...+.......0.......I.. X509v3 CRL Distribution Points: Full Name: URI:http://www.sk.ee/repository/crls/eeccrca.crl Signature Algorithm: sha384WithRSAEncryption
a4:88:a2:e7:79:0d:27:e1:0d:4e:b2:a7:e5:6b:5d:82:f8:d3:
08:b9:cc:54:df:d7:d8:5a:fe:43:bf:cf:32:f1:67:58:5f:e3:
95:49:99:2c:ae:90:c5:9a:59:71:2a:85:a2:d6:05:9b:b0:e6:
43:fb:f2:64:34:1f:26:91:51:e9:e7:37:48:68:9b:fa:44:88:
1c:fa:72:ec:fd:a1:cf:b1:96:63:c0:64:cd:b9:66:86:8b:a9:
ae:2e:a4:fd:bf:f8:d0:96:a1:14:f3:62:42:1d:73:d3:04:10:
2b:39:44:c0:54:9b:24:f5:1b:8b:3c:27:a9:fc:2f:63:36:c9:
86:9d:04:cb:cf:18:94:b7:c9:7c:58:75:cf:db:dd:ad:9f:a2:
2c:37:90:a6:bf:ab:5b:57:00:75:d9:0a:cb:b1:15:56:31:5d:
d6:6d:dc:0c:08:9d:81:de:98:25:4a:8d:98:3c:05:a4:69:bc:
81:17:77:70:20:27:0b:7e:f5:ba:55:ff:1d:3f:32:8b:91:3c:
d4:6f:d2:38:d6:23:1d:6c:02:52:fd:e2:13:bb:e1:66:43:30:
56:d9:55:a5:7a:82:91:bb:ed:7d:8f:dd:d3:c7:28:52:11:5b:
38:ed:49:02:57:e0:2e:67:d6:eb:d0:07:13:b8:00:1a:0c:b3: 0a:b4:96:ad

1.3.2. Registration Authorities

1.3.2.1. Qualified Smart-ID

1.3.2.1.1. Smart-ID Provider

In case of electronic authentication and automated biometric identity verification RA duties are performed by Smart-ID Provider.

Refer to clause 1.3.5.1 of this CPS.

1.3.2.1.2. Customer Service Point

Accepting applications for the Certificates of Q Smart-ID, forwarding the request for Q Smart-ID Certificates and accepting applications for revocation of the Certificates takes place in authorised Customer Service Points.

Customer Service Point acts as the representative of SK in the relations between SK and the Subscriber.

The relationship between Customer Service Point and SK is regulated by a bilateral agreement(s).

Information on Customer Service Points and their contact is available on the website of SK https://www.skidsolutions.eu/en/kontakt/customerservice.

1.3.2.1.3. SK Customer Service Point

SK operates a Customer Service Point (hereinafter referred to as SK Customer Service Point).

SK Customer Service Point accepts applications for revocation of the Q Smart-ID Certificates.

Contact information:

Pärnu Ave 141, 11314 Tallinn, Estonia

(Mon-Fri 9.00 a.m. - 6.00 p.m. Eastern European Time)

Tel +372 610 1880

Email: info@skidsolutions.eu

1.3.2.1.4. Help Line

The Help Line acts as the representative of SK in the field of Subscriber telephone servicing. The Help Line provides user support for solving problems related to Q Smart-ID usage.

The Help Line accepts requests for revocation of Certificates of Q Smart-ID from Subscribers.

Information on the Help Line and its contact details is available on Smart-ID's website https://www.smart-id.com/help/customer-service/.

The Help Line may be contacted at:

- from Estonia, at help.ee@smart-id.com or +372 715 1606;
- from Latvia, at help.lv@smart-id.comor +371 6766 5001;
- from Lithuania, at help.lt@smart-id.comor +370 670 41807.

Additionally, Customer Service Point operates the Help Line for the Subscribers who have applied for Q Smart-ID through Customer Service Point.

Customer Service Point Help Line accepts requests for revocation of Q Smart-ID Certificates from the Subscribers.

1.3.2.2. Mobile-ID

1.3.2.2.1. Mobile Operator

Mobile Operator (hereinafter referred to as MO) performs RA duties.

For issuance of the QSCD and servicing of Mobile-ID Certificates there are contracts signed between SK and MO. SK has contractually delegated the responsibilities described in clauses 1.3.2.2.2 and 1.3.2.2.3 to MO.

The contact details of MO can be checked on the website of SK https://www.skidsolutions.eu.

1.3.2.2.2. MO Customer Service Point

Authorised MO Customer Service Points perform Subscriber Authentication, associate the Subscriber to specific QSCD and issue QSCD to the Subscriber, accept applications for the Certificates of Mobile-ID, forward the request for Mobile-ID Certificates to SK and serve Mobile-ID Certificates.

The list and contact details of MO Customer Service Point can be checked on SK's website https://www.skidsolutions.eu/en/kontakt/customerservice and MO's website.

1.3.2.2.3. MO Help Line

MO operates the Help Line in order to assist its Subscribers with the issues related to Mobile-ID usage.

MO Help Line accepts requests from its Subscribers for suspension of the telecommunication service that results in impossibility to use Mobile-ID. MO Help Line may be contacted at:

- 1817 or 8 698 63 333;
- 1501;
- 1575 or 117; +370 6 840 0075 or +370 6 840 0117;1577; +370 6 840 0077.

1.3.3. Subscribers

Refer to clause 1.3.3 of the CP for Q Smart-ID [1] and CP for Mobile-ID [14].

1.3.4. Relying Parties

A Relying Party is a natural or legal person who takes a decision relying on the Certificate issued by SK.

1.3.5. Other Participants

1.3.5.1. Qualified Smart-ID

1.3.5.1.1. Smart-ID Provider

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

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

1.3.5.1.2. Identity Provider

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.

1.3.5.1.3. Biometric Verification Provider

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.

1.3.5.1.4. Secondary Subscriber Authentication Provider

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.

1.3.5.2. Mobile-ID

1.3.5.2.1. SIM-card Manufacturer

SIM-card Manufacturer:

- produces QSCD-s, generates key pairs and loads them on a QSCD.

1.3.5.2.2. Telecommunication Service Provider

Telecommunication Service Provider:

- facilitates communication between the Subscriber's device and QSCD;
- provides SMS service API that enables Mobile-ID usage;
- manages QSCD distribution to the Subscribers.

The role of Telecommunication Service Provider is fulfilled by MO (hereinafter Telecommunication Service Provider is referred to as MO).

1.4. Certificate Usage

Refer to clause 1.4 of the CP for Q Smart-ID [1] and CP for Mobile-ID [14].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS 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

Not applicable.

1.5.4. CPS Approval Procedures

Amendments which do not change the meaning of this CPS, 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 is enlarged.

In case the CP for Q Smart-ID [1] and CP for Mobile-ID [14] is amended, the CPS is reviewed as well in order to verify the need for its amendments.

In case of substantial changes, the new CPS version is clearly distinguishable from the previous ones and the serial number is enlarged by one. The amended CPS along with the enforcement date, which cannot be earlier than 30 days after publication, is published electronically on SK website.

Amendments which are relevant to Customer Service Point are coordinated with Customer Service Point.

Amendments which are relevant to MO are coordinated with MO.

SK performs annual review of this CPS to ensure compliance of the present document and services provided based on this CPS with the applicable requirements.

All amendments are approved by the head of trust services and amended CPS is enforced by the CEO.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CPS 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.

Term	Definition
Advanced Electronic Signature Certificate	Advanced Electronic Signature Certificate according to eIDAS Regulation [6].
Advanced Electronic Signature	Electronic Signature which meets the requirements provided in Article 26 of eIDAS Regulation [6].
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 Automated Biometric Identity Verification and liveness detection of Subscriber during remote on-boarding process for Q Smart-ID.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile for Smart-ID [8] and Certificate Profile for Mobile-ID [12] rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.
Certification Service	In the context of this document, service related to issuing Certificates, managing revocation, modification and re-key of the Certificates.
Distinguished name	Subject name in the infrastructure of Certificates that is unique for every Subscriber.
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
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.

Term	Definition
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 [10] for qualified certificates.
Integrity	A characteristic of an array: information has not been changed after the array was created.
Mobile Device	A tablet computer or smartphone that runs a mobile device operating system (Apple iOS, Google Android).
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 [14] that can be used to add Mobile-ID authentication, digital signing and pulling Subscriber certificate functionality to an e-service or application.
NQ Smart-ID	Smart-ID which contains one pair of Certificates consisting of the Authentication Certificate and the Advanced Electronic Signature Certificate and their corresponding Private Keys. NQ Smart-ID is issued under the "SK ID Solutions AS - NQ SK Certification Practice Statement." [11]
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. 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 and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
PUK code	The unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
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 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 eIDAS Regulation [6].
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.

Term	Definition
Qualified Electronic Signature Certificate	Qualified Electronic Signature Certificate according to eIDAS Regulation [6].
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation [6]. In the context of Mobile-ID, QSCD compliant SIM-card is a QSCD.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Relying Party	Entity that relies on the information contained within a Certificate or Certificate status information provided by SK.
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 [16].
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.
SK ID Solutions AS Trust Services Practice Statement	A statement of practices that SK employs in providing Trust Services.
Smart-ID	Smart-ID is the new generation electronic ID which provides the Subscriber with means for Electronic Authentication and Electronic Signature.
Smart-ID Account	The 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 instance installed on a Subscriber's Mobile Device that provides access to qualified Smart-ID service.

Term	Definition
Smart-ID HSM module	The hardware security module used in the Smart-ID system. FIPS 140-2 Level 3 certified cryptographic 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 organization that is legally responsible for the Smart-ID system. SK is the Smart-ID provider.
Smart-ID Server	A technical component of the Smart-ID system, handles back-end operations.
Smart-ID System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The Smart-ID system provides services that allow Subscribers (Account owners) to authenticate themselves to services, to give Electronic Signatures requested by E-Service Providers, 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 Certificates of Q Smart-ID or Mobile-ID 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 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 [10] for qualified certificates.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement.
CRL	Certificate Revocation List
CSR	Certificate Signing Request
eIDAS	Regulation (EU) No 910/2014 [6] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
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 crypto processing.

Acronym	Definition
MO	Mobile Operator
MRZ	Machine Readable Zone
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [5]
NFC	Near-Field Communication
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
SCM	SIM-card Manufacturer
SK	SK ID Solutions AS
SK PS	SK ID Solutions AS Trust Services Practice Statement [3]

2. Publication and Repository Responsibilities

2.1. Repositories

Refer to clause 2.1 of SK PS [3].

2.1. Publication of Certification Information

Refer to clause 2.2 of SK PS [3].

2.1.1. Publication and Notification Policies

This CPS is published on SK's website: https://www.skidsolutions.eu/en/repository/CPS.

This CPS and referred documents - the CP for Q Smart-ID [1] and the CP for Mobile-ID [13], the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12], "Terms and Conditions for Use of Certificates of Qualified Smart-ID" [9] (hereinafter referred to as Terms and Conditions of Q Smart-ID) as well as the "Terms and Conditions for Use of Certificates of Mobile-ID of Lithuania" [15] (hereinafter referred to as Terms and Conditions of Mobile-ID) together with the enforcement dates are published on SK's website https://www.skidsolutions.eu/en/repository no less than 30 days prior to taking effect.

SK provides the capability to allow third parties to check and test Certificates it issues.

Test Certificates clearly indicate that they are for testing purposes.

2.1.2. Items not Published in the Certification Practice Statement

Refer to clause 2.2.2 of the CP for Q Smart-ID [1] and the CP for Mobile-ID [13].

Refer to clause 9.3.1 of SK PS [3].

2.2. Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.3. Access Controls on Repositories

Refer to clause 2.4 of SK PS [3].

3. Identification and Authentication

3.1. Naming

3.1.1. Type of Names

Type of names assigned to the Subscriber is described in the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12].

3.1.2. Need for Names to be Meaningful

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

Meaning of names in different fields of the Certificates is described in the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12].

3.1.3. Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4. Rules for Interpreting Various Name Forms

Subscriber names are encoded in UTF-8 and transcribed to Latin letters according to ICAO rules.

3.1.5. Uniqueness of Names

3.1.5.1. Qualified Smart-ID

Subscriber's distinguished name is compiled according to the certificate profile described in the Certificate Profile for Smart-ID [8]. SK does not issue Certificates with an identical Common Name (CN) and Serial Number (S) fields to different Subscribers.

3.1.5.2. Mobile-ID

Subscriber's distinguished name is compiled according to the certificate profile described in the Certificate Profile for Mobile-ID [12]. SK does not issue Certificates with an identical Common Name (CN) and Serial Number (S) fields to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Trademarks are not allowed.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

3.2.1.1. Qualified Smart-ID

There is a single process flow that includes key generation, Certificate Request and issuance. Both the Subscriber and Smart-ID Provider have to participate in the key generation procedure. The Certificate Request sent to CA includes a cryptographic signature created by the newly generated keys.

3.2.1.2. Mobile-ID

MO performs Subscriber Authentication and issues unpersonalised QSCD with pre-generated keys to the Subscriber. The Subscriber signs the corresponding application form and confirms the ownership of the issued QSCD.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

3.2.3.1. Qualified Smart-I

The Subscriber can be identified electronically, via biometric verification or face to face in a Customer Service Point.

Electronic identification is possible when the application is signed with a Qualified Electronic Signature compliant with eIDAS Regulation [6]. In that case, SK relies on identification data provided in the signature of the application, which in turn has to be previously verified by the CA that has issued the Certificate used for signature. SK also verifies that the CA that issued the Certificate used for signature, has identified the Subscriber by physical presence before issuing the Certificate to him/her. The requirement for Qualified Electronic Signature implies acceptable identification and authentication level required to issue Qualified Certificates.

Biometric verification consists of the following steps. The Subscriber's identity is verified based on his/her personal information read from the chip on eMRTD presented by the Subscriber for identity validation. Authenticity of the eMRTD chip is verified based on authentication mechanism supported by the chip and by verifying data read from the MRZ. Validity check of eMRTD is performed based on authoritative source. Biometric verification of the Subscriber is based on the facial image retrieved from data on eMRTD chip with NFC technology and the facial image captured in the liveness session during registration via Smart-ID App. During the liveness session, liveness of the Subscriber's facial image is verified.Physical identity validation is carried out by an employee of Customer Service Point in accordance with the Requirements of Identity Validation for RA [17].

3.2.3.2. Mobile-ID

The Subscriber is identified either electronically or physically in a MO Customer Service Point.

MO electronically verifies the Subscriber's identity and validates that the application for the Certificates is signed with a Qualified Electronic Signature compliant with eIDAS Regulation [6]. MO additionally verifies that the Subscriber's personal data in the application matches with the data provided in his/her signature for the application.

Physical identity validation is carried out by an employee of MO Customer Service Point in accordance with the Requirements of Identity Validation for RA [17].

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information is not allowed in the Certificate.

3.2.5. Validation of Authority

3.2.5.1. Qualified Smart-ID

The Subscriber can apply for Q Smart-ID only personally. SK checks whether the Subscriber has legal capacity.

If the minor applies for Q Smart-ID, SK verifies the right of representation of the minor's legal representative.

3.2.5.2. Mobile-ID

The Subscriber can apply for Mobile-ID only personally. MO checks that the applicant has legal capacity.

3.2.6. Criteria for Interoperation

Not applicable.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Refer to clause 3.2 of this CPS.

3.3.2. Identification and Authentication for Re-Key After Revocation

Refer to clause 3.2 of this CPS.

3.4. Identification and Authentication for Revocation Request

Refer to clause 4.9.3 of this CPS.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

4.1.1.1. Qualified Smart-ID

The Subscriber can enrol herself using the functionality provided by the Smart-ID System.

SK accepts only applications coming from the Smart-ID System.

4.1.1.2. Mobile-ID

Certificate application can be submitted by the Subscriber via MO.

4.1.2. Enrolment Process and Responsibilities

4.1.2.1. Qualified Smart-ID

4.1.2.1.1. Electronic Application

The Subscriber opens the Smart-ID App that starts generating keys for the Certificates. After the Subscriber's Private Key is generated, the Smart-ID App generates a registration token for the Subscriber.

The Subscriber fills an application for Q Smart-ID in the Smart-ID App. The application for Q Smart-ID includes the Subscriber's identification data, email address and/or mobile phone number.

Upon submitting an application for Q Smart-ID, the Subscriber confirms familiarisation and agreement to the Terms and Conditions of Q Smart-ID [9].

In case of a minor, both the minor and his/her legal representative confirm familiarisation and agreement to the Terms and Conditions of Q Smart-ID [9] upon submitting an application for Q Smart-ID.

SK associates the Subscriber and his/her Private Key by using the Subscriber's registration token. The Subscriber signs the application for Q Smart-ID with a Qualified Electronic Signature compliant with eIDAS Regulation [6] and confirms the correctness and integrity of the information presented to SK.

Alternatively, the Subscriber fills an application for Q Smart-ID in the Smart-ID Portal and enters there his/her registration token. The Subscriber signs the application for Q Smart-ID with a Qualified Electronic Signature compliant with eIDAS Regulation [6] and confirms the correctness and integrity of the information presented to SK. SK associates the Subscriber and his/her Private Key by using the Subscriber's registration token.

SK validates the data presented in the application about Subscriber and his/her legal representative against authoritative source. The Subscriber's legal representative signs the application for Q Smart-ID with a Qualified Electronic Signature compliant with eIDAS Regulation [6] and confirms the correctness and integrity of the information presented to SK.

Smart-ID System validates the Subscriber's or his/her legal representative's Qualified Electronic Signature and forwards the application to SK.

SK archives the Subscriber's electronically signed application or the Subscriber's application electronically signed by his/her legal representative.

The Subscriber signs CSR in the Smart-ID App that submits it automatically to SK.

SK checks the data in the CSR against the Subscriber's identification data in the signed application and whether the Subscriber has legal capacity. If there is a match, SK generates Certificates.

SK sends Certificates to Smart-ID System.

4.1.2.1.2. Paper Application

The Subscriber opens the Smart-ID App that starts generating keys for the Certificates. After the Subscriber's Private Key is generated, the Smart-ID App generates a registration token for the Subscriber.

An employee of the Customer Service Point fills an application for Q Smart-ID in the Smart-ID System on behalf of the Subscriber and based on the Subscriber's identification data.

The application for Q Smart-ID includes the Subscriber's identification data, email address and/or mobile phone number.

Upon submitting an application for Q Smart-ID, the Subscriber confirms familiarisation and agreement to the Terms and Conditions of Q Smart-ID [9].

In case of a minor, both the minor and his/her legal representative confirm familiarisation and agreement to the Terms and Conditions of Q Smart-ID [9] upon submitting an application for Q Smart-ID.

In case of a minor, an employee of the Customer Service Point fills an application for Q Smart-ID in the Smart-ID System on behalf of the Subscriber and based on the Subscriber's and his/her legal representative's identification data. SK validates the data presented in the application and during registration about Subscriber and his/her legal representative against authoritative source.

The Subscriber shows his/her registration token to an employee of the Customer Service Point, who enters it to the Smart-ID System. SK associates the Subscriber and his/her Private Key by using the Subscriber's registration token.

The Subscriber or his/her legal representative signs the application for Q Smart-ID and upon signing the application, the Subscriber or his/her legal representative confirms the correctness and integrity of the information presented to SK.

Customer Service Point archives the Subscriber's signed application or the Subscriber's application signed by his/her legal representative and requests the Certificates from SK.

The Subscriber signs CSR in the Smart-ID App that submits it automatically to SK.

SK checks the data in the CSR against the Subscriber's identification data in the signed application and whether the Subscriber has legal capacity. If there is a match, SK generates Certificates.

SK sends Certificates to Smart-ID System.

4.1.2.1.3. Automated Biometric Identity Verification

In order to apply for Q Smart-ID, the Subscriber opens the Smart-ID App and chooses biometric verification for an authentication method. The Subscriber confirms that he/she agrees with the processing of his/her biometric data as stipulated in Consent for Automated Biometric Identity Verification [18].

The Subscriber fills an application for Q Smart-ID in the Smart-ID App. The application for Q Smart-ID includes the Subscriber's identification data, email address and/or mobile phone number. Upon submitting an application for Q Smart-ID, the Subscriber confirms familiarisation and agreement to the Terms and Conditions of Q Smart-ID [9]. The application for Q Smart-ID is electronically signed.

SK validates the data presented in the application and during registration about Subscriber against authoritative source.

During registration process Secondary Subscriber Authentication is performed in order to ensure Subscriber awareness about ongoing Q Smart-ID registration. The Secondary Subscriber Authentication is facilitated or performed by Secondary Subscriber Authentication Provider using with following method:

- delivering authentication message to Subscriber with unique secret generated by Smart-ID System, that Subscriber has to represent through Smart-ID app to Smart-ID System during registration process and Smart-ID system will verify the unique secret’s correctness; or
- authenticating Subscriber with electronic identification mean that corresponds minimal to assurance level substantial.

The Smart-ID App starts generating keys for the Certificates. After the Subscriber's Private Key is generated, the Smart-ID System generates a CSR.

The Subscriber signs CSR in the Smart-ID App that submits it automatically to SK.

Smart-ID System validates the signature for the application for Q Smart-ID and forwards the application to SK.

SK checks the data in the CSR against the Subscriber’s identification data in the signed application. If there is a match, SK generates Certificates. If application for Q Smart-ID is signed with Certificate issued during ongoing registration, the data in the CSR against the Subscriber’s data in the signed application is verified after issuance of the Certificates. If there is no match, SK revokes the Certificates.

SK sends Certificates to Smart-ID System.

Upon signing an application for Q Smart-ID the Subscriber confirms the correctness and integrity of the information presented to SK.

SK always archives the Subscriber's electronically signed application.

4.1.2.2. Mobile-ID

4.1.2.2.1. Paper Application

MO performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS.

MO issues the QSCD to the Subscriber. The Subscriber confirms that the QSCD with PIN codes have been handed over to him/her in untampered condition.

MO performs additional checks related to the Subscriber's identity validation in one of the following way:

- via micropayment - MO's information system verifies if the micropayment was made with the bank card held by the same person who was initially identified (i.e. the Subscriber);
- via automatic technical control to verify from authoritative source validity and issuance of the identification document that the Subscriber initially presented for identity validation;
- second employee of MO Customer Service Point verifies the Subscriber's identity or employee of MO Customer Service Point verifies that the data on the copy of the Subscriber's identification document matches with the data in the Subscriber's application.

The Subscriber's application includes his/her identification data, email address or mobile phone number.

In case of positive decision, the Subscriber signs a Mobile-ID agreement with their handwritten signature with MO. Upon signing an agreement with MO, the Subscriber confirms:

- he/she has read and agrees with the Terms and Conditions of Mobile-ID [15];
- QSCD has been issued to him/her;
- correctness of the information presented to MO.

MO forwards the information that associates the Subscriber with the Private Keys on the issued QSCD to SK. SK uses corresponding Public Keys for Certification.

MO forwards the Certificate request over secure communication channel to SK.

MO archives the Subscriber's signed agreement.

SK verifies that issued QSCD has been previously registered in its database and can check the data in the request against the data in authoritative source using an automatic procedure.

In case of positive decision, Certificates are issued by SK.

4.1.2.2.2. Electronic Application

MO sends the QSCD to the Subscriber.

MO performs Subscriber Authentication pursuant to clause 3.2.3.2 of this CPS. Upon successful Authentication, the Subscriber signs a Mobile-ID agreement with MO with a Qualified Electronic Signature. Mobile-ID agreement includes the Subscriber's identification data, email address or mobile phone number.

Upon signing an agreement with MO, the Subscriber confirms:

- he/she has read and agrees with the Terms and Conditions of Mobile-ID [15];
- QSCD has been issued to him/her;
- correctness of the information presented to MO.

MO verifies that the Subscriber has signed an agreement with a Qualified Electronic Signature compliant with eIDAS Regulation [6], and that the Subscriber's personal data therein matches with the data provided in his/her signature for the agreement.

MO archives the Subscriber's electronically signed agreement.

MO forwards the information that associates the Subscriber with the Private Keys on the issued QSCD to SK. SK uses corresponding Public Keys for Certification.

MO forwards the Certificate request over secure communication channel to SK. SK verifies that issued QSCD has been previously registered in its database and can check the data in the request against the data in authoritative source using an automatic procedure.

In case of positive decision, Certificates are issued by SK.

4.1.3. Annual Control of QSCD

Refer to clause 4.1.3 of SK PS [3].

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. Qualified Smart-ID

4.2.1.1.1. Electronic Application

The Subscriber is identified and authenticated by the data in the Qualified Electronic Signature of the application.

The signature is verified by both the Smart-ID System and SK.

4.2.1.1.2. Paper Application

The Subscriber is identified at least by two employees of the Customer Service Point in accordance with the clause 3.2.3.1 of this CPS.

4.2.1.1.3. Automated Biometric Identity Verification

Biometric Verification Provider verifies the Subscriber's identity in accordance with the clause 3.2.3.1 of this CPS.

The signature for the application for Q Smart-ID is verified by both the Smart-ID System and SK.

4.2.1.2. Mobile-ID

4.2.1.2.1. Paper Application

The Subscriber is identified by an employee of MO Customer Service Point in accordance with the clause 3.2.3.2 of this CPS.

MO performs additional checks related to the Subscriber's identity validation pursuant to clause 4.1.2.2.1 of this CPS.

4.2.1.2.2. Electronic Application

The Subscriber is identified by MO in accordance with the clause 3.2.3.2 of this CPS.

4.2.2. Approval or Rejection of Certificate Applications

4.2.2.1. Qualified Smart-ID

Refer to clause 4.2.2 of the CP for Q Smart-ID [1].

4.2.2.2. Mobile-ID

The acceptance or rejection of an application for Mobile-ID is decided by SK.

SK refuses 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, SK coordinates corresponding amendment with MO.

SK notifies MO of the refusal to issue a Certificate.

4.2.3. Time to Process Certificate Applications

Refer to clause 4.2.3 of the CP for Q Smart-ID [1] and the CP for Mobile-ID [13].

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

4.3.1.1. Qualified Smart-ID

After verifying the data contained in the CSR, SK automatically issues Certificates corresponding to the application.

4.3.1.2. Mobile-ID

After SK has verified that issued QSCD has been previously registered in SK's database, and if having performed query to authoritative source, verified that the data in the request matches with the data in authoritative source, SK automatically issues corresponding Certificates.

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

4.3.2.1. Qualified Smart-ID

The Subscriber is immediately notified of the results by the Smart-ID App as the whole process is done online in real time.

4.3.2.2. Mobile-ID

SK notifies MO of the new Certificate issuance to the Subscriber.

MO notifies the Subscriber of the new Certificate issuance.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

4.4.1.1. Qualified Smart-ID

After SK has issued the Certificates, the Subscriber verifies correctness of the data in the Certificates. If the Subscriber has verified that the data in the Certificates is correct, the Subscriber confirms correctness of the information.

Corresponding confirmation is deemed Certificate acceptance.

If the Subscriber verifies that the data in the Certificates is incorrect, the Subscriber refuses from accepting the Certificates and SK revokes the Certificates.

4.4.1.2. Mobile-ID

Upon signing a Mobile-ID agreement with MO, the Subscriber confirms familiarisation and agreement to the Terms and Conditions of Mobile-ID [15].

Corresponding confirmation is deemed Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

4.4.2.1. Qualified Smart-ID

SK sends the Certificates to Smart-ID System. Certificate validity can be checked through OCSP service.

4.4.2.2. Mobile-ID

Certificates are made available via Mobile-ID Service Integration API [14] after issuance of the Certificates by SK. OCSP starts responding with "GOOD".

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

4.4.3.1. Qualified Smart-ID

The Certificates are automatically sent to Smart-ID System by SK.

4.4.3.2. Mobile-ID

SK notifies MO about issued Mobile-ID Certificates.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

The Subscriber is required to use the Private Key and Certificate lawfully and in accordance with:

- the CP for Q Smart-ID [1] and the CP for Mobile-ID [13];
- this CPS;the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15].

4.5.2. Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber's Public Key and Certificate lawfully and in accordance with:

- the CP for Q Smart-ID [1] and the CP for Mobile-ID [13];
- this CPS;
- the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15].

4.6. Certificate Renewal

Renewal of Certificates is not allowed.

4.7. Certificate Re-Key

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 CPS.

4.7.1. Circumstances for Certificate Re-Key

4.7.1.1. Qualified Smart-ID

Certificate re-key is allowed to:

- fix errors during certification.

4.7.1.2. Mobile-ID

Certificate re-key is allowed only if the QSCD has to be replaced.

4.7.2. Who May Request Certification of a New Public Key

4.7.2.1. Qualified Smart-ID

Certificate re-key process to fix errors during certification can only be initiated by SK.

4.7.2.2. Mobile-ID

Certificate re-key process can only be initiated by the Subscriber.

All the Certification requests are delivered to SK through MO.

4.7.3. Processing Certificate Re-Keying Requests

4.7.3.1. Qualified Smart-ID

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

If the Certificate re-key is performed to fix production errors, the erroneous Certificate are revoked.

If the Certificate re-key is performed to fix production errors only Smart-ID Server's Private Key is generated pursuant to clause 6.1.1 of this CPS.

4.7.3.2. Mobile-ID

The application for recurring Mobile-ID is processed as an application for a new Mobile-ID.

SK immediately revokes the Certificates that have been replaced.

4.7.4. Notification of New Certificate Issuance to Subscriber

4.7.4.1. Qualified Smart-ID

CA notifies RA of the new Certificate issuance to the Subscriber.

RA notifies the Subscriber of the new Certificate issuance.

4.7.4.2. Mobile-ID

The Subscriber notification is similar to initial notification pursuant to clause 4.3.2.2 of this CPS.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

If the Certificate re-key is performed for Mobile-ID, the Subscriber confirms that he/she has read and agrees to the Terms and Conditions of Mobile-ID [15] as stated in clause 4.4.1.2 of this CPS.

If the Certificate re-key is performed for Q Smart-ID, the Subscriber verifies correctness of the data in the Certificates as stated in clause 4.4.1.1 of this CPS.

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

Refer to clause 4.4.2 of this CPS.

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

Refer to clause 4.4.3 of this CPS.

4.8. Certificate Modification

For Certificate modification of Q Smart-ID see clause 4.7 of this CPS.

4.8.1. Circumstances for Certificate Modification

4.8.1.1. Mobile-ID

Certificate modification is allowed to:

- fix invalid Certificates that do not comply with the Certificate Profile for Mobile-ID [12].

4.8.2. Who May Request Certificate Modification

4.8.2.1. Mobile-ID

Certificate modification process can only be initiated by SK.

4.8.3. Processing Certificate Modification Requests

4.8.3.1. Mobile-ID

SK processes Certificate modification requests and is not required to coordinate it with the Subscriber.

During Certificate modification, all the erroneous or unusable Certificates to be replaced are revoked.

The validity period of the newly issued Certificates does not exceed the validity period of the underlying Mobile-ID.

4.8.4. Notification of New Certificate Issuance to Subscriber

4.8.4.1. Mobile-ID

SK notifies the Subscriber of new Certificate issuance.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

4.8.5.1. Mobile-ID

Refer to clause 4.7.5 of this CPS.

4.8.6. Publication of Modified Certificate by the CA

4.8.6.1. Mobile-ID

Refer to clause 4.7.6 of this CPS.

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

4.8.7.1. Mobile-ID

Refer to clause 4.7.7 of this CPS.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Refer to clause 4.9.1 of the CP for Q Smart-ID [1] and the CP for Mobile-ID [13].

4.9.2. Who Can Request Revocation

4.9.2.1. Qualified Smart-ID

The Subscriber can request revocation of the Subscriber's Certificates any time.

4.9.2.2. Mobile-ID

Refer to clause 4.9.2 of the CP for Mobile-ID [13].

4.9.3. Procedure for Revocation Request

4.9.3.1. Qualified Smart-ID

The Subscriber can request revocation of Q Smart-ID Certificates as follows.

The Subscriber can request revocation of Q Smart-ID Certificates via the Help Line or Customer Service Point Help Line.

The operator of the Help Line verifies the Subscriber by using the identification data in the Subscriber's application. After the Subscriber's identity and legality to request revocation is verified, the operator of the Help Line revokes the Q Smart-ID Certificates.

If the operator of the Customer Service Point Help Line is unable to verify the Subscriber's identity, the Subscriber can be directed to request revocation via the Help Line.

Revocation request submitted via the Help Line or the Customer Service Point Help Line is recorded.

Alternatively, the Subscriber can request revocation of Q Smart-ID via Smart-ID Portal, where the Subscriber is authenticated using Verified Electronic Authentication. The Subscriber has to confirm the application there.

The Subscriber can also request revocation of Q Smart-ID Certificates by deleting his/her Smart-ID Account in Smart-ID App. In this case, revocation of the Certificates is possible only from the Smart-ID App instance that the Subscriber used for registering his/her Smart-ID Account.

The Smart-ID Portal or Smart-ID App sends the request for revocation to SK.

The Subscriber can also submit a signed application for revocation of the Certificates to Customer Service Point or SK Customer Service Point.

In case of a signed application, the identity of the person is verified based on the identity document by an employee of Customer Service Point or SK Customer Service Point. After SK has received an application for revocation of the Certificate, the procedure for processing the request is the following:

- the revocation application is registered by an employee of Customer Service Point or SK Customer Service Point;
- the person filing an application for revocation is verified;
- the compliance of the application for revocation with the CP for Q Smart-ID [1] is verified in SK's information system;
- OCSP no longer responds with "GOOD";
- the documentation on which the application for revocation was based is archived;
- the Subscriber is notified of revocation of the Certificates.

After SK has received an application for revocation, SK processes it immediately.

The revocation of the Certificate is recorded in the certificate database of SK. The Subscriber has a possibility to verify from the Smart-ID System that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

4.9.3.2. Mobile-ID

The Subscriber submits a signed application for revocation to an employee of MO Customer Service Point. The revocation application is registered by an employee of MO Customer Service Point.

An employee of MO Customer Service Point verifies the person filing an application for revocation in accordance with the Requirements of Identity Validation for RA [17] and establishes the legality to request revocation.

An employee of MO Customer Service Point archives the application for revocation and forwards the revocation request to SK.

If competent authority requests revocation of the Certificates, SK processes it according to the procedure listed below (except verifying the identity of the person requesting revocation).

After SK has received a request for revocation of the Certificates, the procedure for processing the request is the following:

- the revocation request is registered by SK;
- the legality to request revocation is verified by SK if the revocation is requested by competent authority;
- the compliance of the request with the CP for Mobile-ID [13] is verified in SK's information system;
- the Certificate is marked as revoked in the certificate database and if revocation is requested by competent authority, the Certificate is tagged accordingly in SK's internal database to distinguish it later from other revoked Certificates;
- OCSP stops responding with status "GOOD";
- the documentation on which the application for revocation was based is archived if the revocation is requested by competent authority;
- the Subscriber is notified of revocation of the Certificate.

After SK has received the request for revocation, SK processes it immediately.

If revocation is requested by competent authority, the Certificates are revoked given all the reasonable circumstances, no later than on the date indicated in the revocation request or 24 hours after receipt of the request.

The revocation of the Certificate is recorded in the certificate database of SK. The Subscriber has a possibility to verify via OCSP that the Certificate has been revoked.

Certificate revocation applies to Certificate Pairs only.

If one of the Certificates in a Certificate Pair is revoked, all the Certificate Pairs of the same Mobile-ID are revoked. 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 only revokes the corresponding Certificate Pair and the other Certificate Pair remains valid.

Revoked Certificates can not be reinstated.

The Subscriber can request suspension of the telecommunication service via MO Help Line 24 hours a day, 7 days a week. The operator of MO Help Line verifies the Subscriber by asking the Subscriber his/her safeword or check-up questions about the Subscriber's personal details (e.g. name, personal identification code, address).

Alternatively, the Subscriber can request suspension of the telecommunication service by submitting an application at MO Customer Service Point. An employee of MO Customer Service Point verifies the Subscriber in accordance with internal verification procedures.

Suspension of the telecommunication service results in impossibility to use Mobile-ID.

Suspension of the telecommunication service does not automatically result in revocation of the Certificates, the Subscriber is required to request revocation in case he/she is convinced that his/her device is lost or stolen. Otherwise the Certificates remain valid, but the usage of Mobile-ID is disabled. In case the Subscriber requests revocation of the Mobile-ID Certificates, the request is processed pursuant to the procedure described herein.

MO can request revocation of the Certificates if any of the circumstances applicable to her and stipulated in clause 4.9.1 of the CP for Mobile-ID [13] occur or if she terminates telecommunication service provided to the Subscriber.

In these cases, an employee of MO sends a revocation request to SK. After checking authenticity and integrity of the request, SK revokes the Certificates.

MO and the Subscriber are notified of revocation of the Certificate.

4.9.4. Revocation Request Grace Period

4.9.4.1. Qualified Smart-ID

The Subscriber is required to request revocation immediately after verifying the loss or theft of the device, or loss of control over one or both Private keys, or PIN codes.

4.9.4.2. Mobile-ID

The Subscriber is required to request revocation immediately after verifying the loss or theft of the device.

4.9.5. Time Within Which CA Must Process the Revocation Request

4.9.5.1. Qualified Smart-ID

After an application for revocation has been submitted, SK immediately processes an application for revocation.

4.9.5.2. Mobile-ID

After MO has forwarded the request for revocation to SK, SK immediately processes the request for revocation.

SK processes competent authority's application for revocation immediately after it has verified the correctness and completeness of the corresponding application as well as applicant's authority to request revocation.

4.9.6. Revocation Checking Requirements for Relying Parties

The mechanisms available to a Relying Party in order to check the status of certificates on which it wishes to rely have been established in the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15].

4.9.7. CRL Issuance Frequency

CRL for EID-SK 2016 is not issued.

4.9.8. Maximum Latency for CRLs

SK monitors of the expiry time of the CRL that is published on SK's website. If a new CRL is not published 120 minutes before expiry of the previous one, an alarm is raised.

4.9.9. On-Line Revocation/Status Checking Availability

OCSP service is free of charge and publicly accessible.

OCSP service serves as a primary source for the Certificate status information and contains Certificate status information until the Certificate expires.

Certificate status information for the Certificates issued by EID-SK 2016 is signed by EID-SK 2016 AIA OCSP RESPONDER YYYYMM certificate (naming convention in [8] and [12]).

4.9.10. On-Line Revocation Checking Requirements

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been established in the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15].

4.9.11. Other Forms of Revocation Advertisements Available

SK offers OCSP service with better SLA under agreement and price list.

Revocation status information of the expired Certificate can be requested at the email address info@skidsolutions.eu

4.9.12. Special Requirements Related to Key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

Not applicable.

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

SK offers OCSP service for checking certificate status. Services are accessible over HTTP protocol.

The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12].

4.10.2. Service Availability

SK ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.44% availability overall per year with a scheduled downtime that does not exceed 0.28% annually.

4.10.3. Operational Features

None.

4.11. End of Subscription

The maximum validity period of the Certificate is described inthe Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12].

Subscription ends if the Certificate expires.

The Subscriber may end a subscription for the Certificate by revoking the Certificate without replacing it.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

SK does not provide the Subscriber with key escrow and recovery services.

Storing the components of the split private key of Q Smart-ID in the Smart-ID Server is not considered a key escrow service.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

Refer to clause 5.1 of SK PS [3].

5.2. Procedural Controls

Refer to clause 5.2 of SK PS [3].

5.3. Personnel Controls

Refer to clause 5.3 of SK PS [3].

5.4. Audit Logging Procedures

Refer to clause 5.4 of SK PS [3].

Audit log of events relation to preparation of QSCD is kept.

5.5. Records Archival

5.5.1. Types of Records Archived

Refer to clause 5.5.1 of SK PS [3].

All physical records from issuance process and from applications for suspension, termination of suspension and revocation are retained by RA-s and archived in accordance with relevant regulations.

5.5.2. Retention Period for Archive

Refer to clause 5.5.2 of SK PS [3].

5.5.3. Protection of Archive

Refer to clause 5.5.3 of SK PS [3].

5.5.4. Archive Backup Procedures

Refer to clause 5.5.4 of SK PS [3].

5.5.5. Requirements for Time-Stamping of Records

Refer to clause 5.5.5 of SK PS [3].

5.5.6. Archive Collection System (Internal or External)

Refer to clause 5.5.6 of SK PS [3].

RA-s may use external archive collection system for physical archive records.

5.5.7. Procedures to Obtain and Verify Archive Information

Refer to clause 5.5.7 of SK PS [3].

5.6. Key Changeover

The Public Key of the CA does not change. The Public Key for the OCSP responder is sent inside the OCSP response, through which a change of key is known.

If necessary, details of a key changeover are considered each time. Common name of the CA always contains the number of the year which it was issued (e.g. EID-SK 2016).

5.7. Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [3].

5.8. CA or RA Termination

Refer to clause 5.8 of SK PS [3].

6. Technical Security Controls

6.1. Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [3].

6.1.1. Key Pair Generation

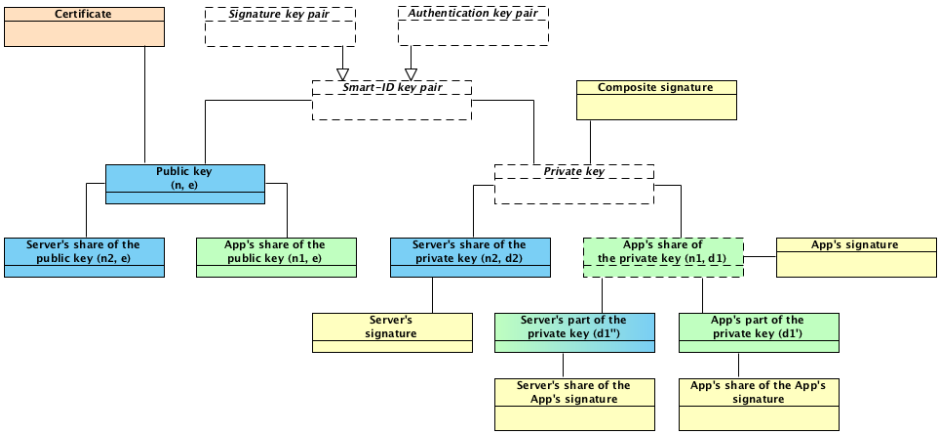
Refer to clause 6.1.1 of SK PS [3].

6.1.1.1. Qualified Smart-ID

Qualified Smart-ID Key Pair Terminology

Q Smart-ID Key Pair is generated with multiple components for additional protection and cryptographic properties. The following terminology is used to describe the technical security controls:

1. 'Public key' - is the public verification key in the public-key cryptography. This corresponds to the regular RSA public key. The relation between the 'Public key' and a 'Subscriber's Identity' is attested by a Certificate. Public key has the following components: 'App's share of the public key' and 'Server's share of the public key';
2. 'App's share of the public key' - is generated in the Smart-ID App, along with the generation of the 'App's share of the private key';
3. 'Server's share of the public key' - is generated in the Smart-ID server, along with the generation of the 'Server's share of the private key';
4. 'Private key' - is the confidential component of the key pair in the public-key cryptography. 'Private key' is used for creating 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. 'Private key' has the following components:
    1. 'App's share of the private key', which is a regular RSA private key. It is further divided to the following components:
        1. 'App's part of the private key';
        2. 'Server's part of the private key'.
    2. 'Server's share of the private key', which is a regular RSA private key.
5. 'App's share of the private key' - is the component of the private key that is generated in the Smart-ID App. The share is divided into two parts immediately after generation and the share itself is deleted;
6. 'App's part of the private key' - is the component of the private key, which is generated in the Smart-ID App and stored in the Smart-ID App and is protected with the Subscriber's PIN-code;
7. 'Server's part of the private key' - is the component of the private key, which is generated in the Smart-ID App and securely transmitted to the server. 'Server's part of the private key' is stored in the server's database and protected with Key-Wrapping-Key, which in turn, is protected by the HSM;
8. 'Server's share of the private key' - is the component of the private key, which is generated in the HSM and protected by the HSM.



6.1.1.1.1. Smart-ID Key Pair Generation

Subscriber Key Pair is generated during the Smart-ID registration process in the Smart-ID App and in the Smart-ID server. The following components are generated.

Generation of 'App's share of the private key' and 'App's share of the public key'

'App's share of the private key' and 'App's share of the public key' is a 3072-bit RSA key pair. Smart-ID App generates the key pair according to FIPS 186-4 with the PRNG, which corresponds to NIST SP 800-90A Rev. 1. After dividing the 'App's share of the private key' to components, the private key of the RSA key pair is deleted.

Generation of 'App's part of the private key'

The 'App's part of the private key' is a 3072-bit random number. Smart-ID App generates the 'App's part of the private key' randomly with the PRNG, which corresponds to NIST SP 800-90A Rev. 1.

Generation of 'Server's part of the private key'

The 'Server's part of the private key' is a 3072-bit number, which is computed from the private exponent of the 'App's share of the private key' and 'App's part of the private key'. Smart-ID App computes the 'Server's part of the private key' and transmits the 'Server's part of the private key' securely to the Smart-ID server.

Generation of 'Server's share of the private key' and 'Server's share of the public key'

'Server's share of the private key' and 'Server's share of the public key' is a 3072-bit RSA keypair. Smart-ID server generates the keypair inside the Smart-ID HSM module.

Generation of Subscriber's 'Public key'

Subscriber's 'Public key' is a 6144-bit RSA public key. The public key is computed by the Smart-ID server from the 'App's share of the public key' and 'Server's share of the public key'. This way all the Smart-ID keypair components are tied together with the 'Public key'.

6.1.1.2. Mobile-ID

The Private Keys are pre-generated by the SCM in a FIPS 140-2 Level 3 certified cryptographic device or higher certified security module. The keys are loaded onto the QSCD in a secure manner. The Subscriber keys are protected by the activation PIN codes handed over and known only to the Subscriber. The SCM deletes private keys from her information system promptly after transferring them on the QSCD. Private Keys are not saved outside of the QSCD in the course of this transfer.

6.1.2. Private Key Delivery to Subscriber

6.1.2.1. Qualified Smart-ID

Subscriber's 'Private key' is composed of multiple components.

6.1.2.1.1. Delivery of 'App's part of the private key'

The 'App's part of the private key' is generated inside the Subscriber's mobile device and is never transmitted outside of this device.

6.1.2.1.2. Delivery of 'Server's part of the private key'

The 'Server's part of the private key' is generated inside the Subscriber's mobile device and is securely transmitted to the Smart-ID server. The transmission is handled in the following way:

1. The key-transmission-key (KTK) key pair is generated inside the Smart-ID HSM module. The KTK is a 3072-bit RSA key pair;
2. The public key of the KTK is embedded in the binary distribution of the Smart-ID App;
3. During the registration procedure, the Smart-ID App and Smart-ID server generate Diffie-Hellman key pairs and perform the Diffie-Hellman key exchange protocol to derive the transmission-encryption-key (TEK). The length of TEK key is 256 bits, it consists of 128-bit AES key and 128-bit HMAC key, concatenated;
4. The 'Server's part of the private key' is sent to the Smart-ID server with the following protection:
    1. The key is encoded and encrypted with the public key of the KTK (according to the RFC 7516), so that it can only be decrypted by the Smart-ID server;
    2. The submission request is encrypted and integrity protected with the shared TEK key;
    3. The communication is performed within the TLS channel, for additional confidentiality and authenticity.
5. The Smart-ID server uses the established TEK key to decrypt the request and HSM to decrypt the 'Server's part of the private key' and stores it securely in the database, wrapped with another long-term key-wrap-keypair (KWK). The KWK is generated and protected by the Smart-ID HSM module.

6.1.2.1.3. Delivery of 'Server's share of the private key'

The 'Server's share of the private key' is generated inside the Smart-ID HSM module and is always protected by the HSM module.

6.1.2.2. Mobile-ID

The Subscriber Private Keys are delivered in the chip of the card. The confidentiality and non-usage of the generated Private Keys and PIN codes is warranted by not handing over personalised QSCD to the Subscriber, i.e. QSCD is non-personalised before it is handed over to the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

6.1.3.1. Qualified Smart-ID

The Subscriber's 'Public key' is computed inside the Smart-ID server from the 'App's share of the public key' and 'Server's share of the public key' and then transmitted to Certificate Issuer inside the PKCS#10 Certificate Signing Request (CSR). The CSR is signed by the Subscriber for authenticity. The transmission is protected by TLS communication channel for additional confidentiality and authenticity.

Subscriber's 'Public key' is composed of multiple components. The delivery of individual components is as follows:

6.1.3.1.1. Delivery of 'App's share of the public key' from Smart-ID App to Smart-ID server

The 'App's share of the public key' is generated in the Smart-ID App and then transmitted to the Smart-ID server during the Subscriber's registration process. The public key is transmitted over the TLS communication channel for confidentiality and authenticity.

6.1.3.1.2. Delivery of 'Server's share of the public key' from Smart-ID HSM to Smart-ID server

The 'Server's share of the public key' is generated inside the Smart-ID HSM module and then transmitted to Smart-ID server. The public key is transmitted over the secured communication channel for confidentiality and authenticity.

6.1.3.2. Mobile-ID

The pre-generated Public Keys are delivered in batches from the SCM to MO. An authorized representative of the MO electronically signs the batch and requests loading the keys to a database in SK. When issuing a Certificate, SK finds the correct Public Key from the database of previously loaded keys based on the serial number of the QSCD.

6.1.4. CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [3].

6.1.5. Key Sizes

6.1.5.1. Qualified Smart-ID

1. 'App's share of the private key' is a 3071 or 3072 bit RSA private key;
2. 'App's part of the private key' is a 3071 or 3072 bit number;
3. 'Server's part of the private key' is a 3071 or 3072 bit number;
4. 'Server's share of the private key' is a 3071 or 3072 bit RSA private key;
5. 'App's share of the public key' is a 3071 or 3072 bit RSA public key;
6. 'Server's share of the public key' is a 3071 or 3072 bit RSA public key;
7. 'Public key' is a 6142, 6143 or 6144 bit RSA public key;

6.1.5.2. Mobile-ID

Subscriber keys are 2048 bits when RSA and 256 bits when ECC algorithm is used.

6.1.6. Public Key Parameters Generation and Quality Checking

6.1.6.1. Qualified Smart-ID

Quality of public keys is guaranteed by using secure random number generators by the Smart-ID App and Smart-ID HSM module and following the specified algorithms in the FIPS 186-4. Before issuing a Certificate, key is checked for duplicates and some basic analytic checks are applied (e.g. e > 1 for RSA). More thorough checks are run over database of issued Certificates regularly.

6.1.6.2. Mobile-ID

The quality of Public Keys is guaranteed by using secure random number generators built into the card or HSM-s. User-generated keys are not accepted.

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

Refer to clause 6.1.7 of SK PS [3].

Key usage purposes are described in clause 7.1 of this CPS.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

6.2.1.1. Qualified Smart-ID

Refer to clause 6.2.1 of SK PS [3].

Qualified Smart-ID App cryptographic library standards

The Smart-ID App on the Android and iOS platforms are corresponding to FIPS 186-4.

Qualified Smart-ID server cryptographic library standards

The Smart-ID server is using Smart-ID HSM module for the cryptographic operations. HSM module is corresponding to FIPS 140-2 Level 3. HSM is certified to be compliant with the QSCD requirements according to eIDAS Regulation [6].

6.2.1.2. Mobile-ID

Refer to clause 6.2.1 of SK PS [3].

The chips used to store Subscriber Private keys are QSCD according to eIDAS Regulation [6].

Keys are generated by a FIPS 140-2 (Level 3) certified device or higher certified security module.

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

6.2.2.1. Qualified Smart-ID

Multi-Person Control of 'App's part of the private key'

No Multi-Person control is applied to 'App's part of the private key'.

Multi-Person Control of 'Server's part of the private key'

The access means to the KWK key, which is used to protect the 'Server's part of the private key', is divided into two parts that are secured by different persons in Trusted Roles. For activation of the KWK key the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [3].

Multi-Person Control of 'Server's share of the private key'

The access means to the 'Server's share of the private key' is divided into two parts that are secured by different persons in Trusted Roles. For activation of such keys, after the reboot of the Smart-ID system, the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [3].

6.2.2.2. Mobile-ID

Refer to clause 6.2.2 of SK PS [3].

No Multi-Person control is applied to Subscriber Private keys.

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [3].

SK does not offer Key Escrow services to Subscribers.

6.2.4. Private Key Backup

6.2.4.1. Qualified Smart-ID

Refer to clause 6.2.4 of SK PS [3].

In general, Smart-ID System doesn't provide the private key backup services. SK makes the following exceptions to the following components of the Subscriber's private key in order to support high availability of the Smart-ID system.

6.2.4.1.1. No backup of 'App's part of the private key'

The encrypted value of 'App's part of the private key' is stored inside the Smart-ID App private storage area. It is not backed up and not copied from the storage area.

In case Subscriber needs to recover from the malfunctioning mobile device or user error, Subscriber needs to complete the registration process again.

6.2.4.1.2. Backing up of encrypted value of 'Server's part of the private key'

The encrypted value of 'Server's part of the private key', protected with the KWK, is stored inside the Smart-ID database.

The Smart-ID database is regularly synchronised to another data center and regularly copied to the backup storage.

6.2.4.1.3. Backing up of KWK of 'Server's part of the private key'

The 'Server's part of the private key' is encrypted with the KWK, which is protected by the Smart-ID HSM module.

The HSM module is regularly synchronized to another data center and regularly backed up to backup storage.

6.2.4.1.4. Backing up 'Server's share of the private key'

The 'Server's share of the private key' is protected by the Smart-ID HSM module.

The Smart-ID HSM module is regularly synchronised to another data center and regularly backed up to backup storage.

6.2.4.2. Mobile-ID

Refer to clause 6.2.4 of SK PS [3].

The Subscriber Private Keys cannot be extracted or restored from the chip and are not backed up.

6.2.5. Private Key Archival

6.2.5.1. Qualified Smart-ID

Refer to clause 6.2.5 of SK PS [3].

Components of Subscriber's 'Private key' are not archived.

6.2.5.2. Mobile-ID

Refer to clause 6.2.5 of SK PS [3].

The Subscriber Private Keys cannot be extracted or restored from the chip and are not archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

6.2.6.1. Qualified Smart-ID

Refer to clause 6.2.6 of SK PS [3].

Private key transfer into or from the cryptographic module is not done, otherwise than described in the clause 6.1.2 of this CPS.

6.2.6.2. Mobile-ID

Refer to clause 6.2.6 of SK PS [3].

The Subscriber Private Keys for Mobile-ID are transferred from the HSM to QSCD in a protected environment using a secure electronic channel.

6.2.7. Private Key Storage on Cryptographic Module

6.2.7.1. Qualified Smart-ID

Refer to clause 6.2.7 of SK PS [3].

6.2.7.1.1. Storage of 'App's part of the private key'

'App's part of the private key' is a random large integer number. For storage, it is encrypted with the 128-bit AES key, derived from the Subscriber's PIN. The encrypted 'App's part of the private key' is then stored on the private area of the Smart-ID App on the mobile device storage.

The AES key is generated from the Subscriber's PIN with the PBKDF2 function (according to RFC 2989). The AES key and the Subscriber's PIN is never stored by the Smart-ID App. The AES encryption algorithm is used in the CBC mode and without any padding.

6.2.7.1.2. Storage of 'Server's part of the private key'

'Server's part of the private key' is a random large integer number. For storage in the Smart-ID database, it is encrypted with the 128-bit key-wrapping-key (KWK). The KWK is a 128-bit AES key, which is protected by the Smart-ID HSM module.

6.2.7.1.3. Storage of 'Server's share of the private key'

'Server's share of the private key' is a private key of the RSA key pair. It is generated inside the Smart-ID HSM module and protected by the HSM module.

6.2.7.2. Mobile-ID

Refer to clause 6.2.7 of SK PS [3].

Private keys of the Subscriber's are stored on the chip of the Mobile-ID.

6.2.8. Method of Activating Private Key

6.2.8.1. Qualified Smart-ID

Refer to clause 6.2.8 of SK PS [3].

In order to give signatures with Subscriber's 'Private Key', all components of the Private Key must be activated.

6.2.8.1.1. Activating 'App's part of the private key'

'App's part of the private key' is protected by Subscriber's PIN and Subscriber needs to enter the PIN to the Smart-ID App for each transaction. The value of PIN is never stored by the Smart-ID App.

Subscriber's PIN is chosen by the Subscriber during the registration process of Smart-ID.

The following rules apply:

1. PIN1 to protect the authentication key pair has to be 4 to 12 digit long;
2. PIN2 to protect the signature key pair has to be 5 to 12 digit long;
3. In case the Subscriber enters the wrong PIN 3 times in a row, the keypair is locked from usage for next three hours;
4. In case the Subscriber enters the wrong PIN 6 times in a row, the keypair is locked from usage for next 24 hours;
5. In case the Subscriber enters the wrong PIN 9 times in a row, the keypair is blocked and the certificate is revoked.

6.2.8.1.2. Activating 'Server's part of the private key'

'Server's part of the private key' is protected by KWK, which in turn, is protected by the Smart-ID HSM module. To activate the KWK, the operator needs to enter the operator keycard into the HSM and enter the operator password to the HSM. Once activated by the operator, the KWK is activated until the Smart-ID system is stopped.

Further, the activation of the 'Server's part of the private key' for completing the signature with the Subscriber's 'Private Key' is the subject of authentication and access control procedure performed on the Smart-ID server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the Smart-ID App over the secure channel) and successful validation of the knowledge-based authentication factor (signature share computed from the data to be signed, Subscriber's PIN and the 'App's part of the private key', presented by the Subscriber and Smart-ID App over the secure channel). So this means that activation of 'Server's part of the private key' requires that Subscriber has activated the 'App's part of the private key' by entering correct PIN code according to clause 6.2.8.2.1 of this CPS.

The authentication factors are only usable for specific data to be signed and they would need to be re-submitted for next operation with Subscriber's 'Private Key'.

6.2.8.1.3. Activating 'Server's share of the private key'

'Server's share of the private key' is a RSA private key, which is generated and protected by the Smart-ID HSM module. To allow Smart-ID system to access the HSM,the operator needs to enter the operator keycard into the HSM and enter the operator password to the HSM. HSM connection is active until the Smart-ID system is stopped.

The activation of the 'Server's share of the private key' for completing the signature with the Subscriber's 'Private Key' is the subject of authentication and access control procedure performed on the Smart-ID server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the Smart-ID App over the secure channel) and successful validation of the knowledge-based authentication factor (App's signature computed from the data to be signed, Subscriber's PIN (presented by the Subscriber), the 'App's part of the private key' and 'Server's part of the private key'). So this means that activation of 'Server's share of the private key' requires that Subscriber has activated the 'App's part of the private key' by entering correct PIN code according to clause 6.2.8.2.1 of this CPS.

The authentication factors are only usable for specific data to be signed and they would need to be re-submitted for next operation with Subscriber's 'Private Key'.

6.2.8.2. Mobile-ID

Refer to clause 6.2.8 of SK PS [3].

The Subscriber Private Keys are protected by PIN codes. The following rules apply:

- There is a separate PIN for each Private Key or group of Private Keys corresponding to a Certificate with unique Distinguished Name (i.e. there are separate PIN-s for Authentication Key and Signature Key, but RSA key for Authentication and ECC key for Authentication can be protected with the same PIN);
- The Subscriber must enter the activation code of the Authentication Certificate (PIN1) at least once after the mobile handset has booted;
- The Subscriber must enter the activation code of the Qualified Electronic Signature Certificate (PIN2) before every single operation done with the corresponding Private Key;
- the usage of all Private Keys protected by a single PIN will be blocked after 3 consecutive incorrect tries;
- PIN can be unblocked using a PUK code;
- the usage of PUK code will be blocked after 3 consecutive incorrect tries;
- tser can change the PIN and PUK codes.

The length of the activation codes is limited to:

- 4 numbers for the Authentication Key (PIN1);
- 5 numbers for the Signature Key (PIN2);
- 8 numbers for the The Unlock (PUK) code.

PIN and PUK codes for activating Private Keys of Mobile-ID are different from PIN and PUK codes of the SIM-card.

6.2.9. Method of Deactivating Private Key

6.2.9.1. Qualified Smart-ID

Refer to clause 6.2.9 of SK PS [3].

Deactivation of any component of the Subscriber's 'Private Key' also means that the Subscriber cannot give signatures anymore and needs to activate that component again.

6.2.9.1.1. Deactivating 'App's part of the private key'

The user entered PIN-code is only used for a single key pair operation. The PIN and derived AES key is deleted from the Smart-ID App memory after the operation is completed or when the Smart-ID server responds with 'Wrong PIN' error message.

6.2.9.1.2. Deactivating 'Server's part of the private key'

The 'Server's part of the private key' is only decrypted for a single key pair operation by the server and the clear-text value is immediately deleted from the Smart-ID server memory after the operation is completed or when the Smart-ID server responds with 'Wrong PIN' error message.

6.2.9.1.3. Deactivating 'Server's share of the private key'

'Server's share of the private key' is protected by the Smart-ID HSM module. Access to the keys is lost after the Smart-ID HSM or Smart-ID server is stopped.

6.2.9.2. Mobile-ID

Refer to clause 6.2.9 of SK PS [3].

The Private Key is deactivated by disconnecting power or resetting the card.

The Subscriber can deactivate a Private Key by entering all the PIN and PUK codes incorrectly 3 consecutive times.

6.2.10. Method of Destroying Private Key

6.2.10.1. Qualified Smart-ID

Refer to clause 6.2.10 of SK PS [3].

Destroying of any component of the Subscriber's 'Private key' also means that the Subscriber cannot give signatures anymore and needs to complete the registration process again.

6.2.10.1.1. Destroying 'App's part of the private key'

Subscriber can destroy the 'App's part of the private key' from the Smart-ID App during the Smart-ID Account closing (for example, by closing the Smart-ID Account n the Smart-ID App or in the Smart-ID Portal, by uninstalling the Smart-ID App, by destroying the mobile device, etc).

6.2.10.1.2. Destroying 'Server's part of the private key'

'Server's part of the private key' is deleted in the Smart-ID server during the Smart-ID Account closing (for example, by closing the Smart-ID Account in Smart-ID App or in the Smart-ID Portal, after multiple wrong PIN codes entered, detection of cloned device, etc).

6.2.10.1.3. Destroying 'Server's share of the private key'

'Server's share of the private key' is deleted in the Smart-ID HSM module during the account closing (for example, by closing the Smart-ID Account in Smart-ID App or in the Smart-ID Portal, after multiple wrong PIN codes entered, detection of cloned device, etc).

6.2.10.2. Mobile-ID

Refer to clause 6.2.9 of SK PS [3].

The Subscriber Private Keys can be destroyed by physically destroying or damaging the chip of the card.

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS.

Mobile-ID SIM-cards are QSCD according to eIDAS Regulation [6].

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to clause 6.3.1 of SK PS [3].

All the Subscriber Public Keys are kept in database of SK and may be archived after expiration of the CA that has issued the certificates.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Refer to clause 6.3.2 of SK PS [3].

For Subscriber Certificates, the validity period is defined in clause 7.1 of this CPS.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

6.4.1.1. Qualified Smart-ID

Refer to clause 6.4.1 of SK PS [3].

Smart-ID App generates random activation codes and provides the Subscriber option to choose his own activation codes as well.

Activation data is used as the input seed to the encryption key derivation function (PBKDF2) and the resulting key is used to encrypt the locally stored 'App's part of the private key'. The activation codes themselves are never stored in the Smart-ID App nor in the Smart-ID Service Provider.

6.4.1.2. Mobile-ID

Refer to clause 6.4.1 of SK PS [3].

Activation codes are pre-generated by the SCM printed on the plastic of the QSCD containment under the secure layer. Activation codes are protected in such way that it is impossible to read them without breaking security element. The Subscriber has prerogative to refuse from accepting of activation codes with altered security element.

6.4.2. Activation Data Protection

6.4.2.1. Qualified Smart-ID

Refer to clause 6.4.2 of SK PS [3].

The initial activation data is generated by the Smart-ID App or chosen by the Subscriber.

After that, activation codes themselves are never stored in the Smart-ID App nor in the Smart-ID Service Provider.

Subscriber has to memorise the activation codes and never share them with anyone.

6.4.2.2. Mobile-ID

Refer to clause 6.4.2 of SK PS [3] and 6.4.1.2 of this CPS.

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Refer to clause 6.5.1 of SK PS [3].

Subscriber is responsible for applying reasonable protections on her device.

6.5.2. Computer Security Rating

Refer to clause 6.5.2 of SK PS [3].

Subscriber is responsible for applying reasonable protections on her device.

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [3].

Subscriber is responsible for applying reasonable protections on her device.

6.7. Network Security Controls

6.7.1. Qualified Smart-ID

Refer to clause 6.7 of SK PS [3].

Smart-ID App and Smart-ID server communicates with each other over the TLS channel. Server enforces known good encryption cipher-suites on the TLS channel. Smart-ID App implements the certificate pinning to verify the authenticity of channel endpoint. Server implements the Smart-ID App authentication to verify the authenticity of channel endpoint.

Smart-ID App and Smart-ID server further use the established transmission-encryption-key (TEK) to secure the network requests and responses. Smart-ID App and server generate Diffie-Hellman key pairs and perform the Diffie-Hellman key exchange protocol, to derive the TEK. The length of TEK key is 256 bits, it consists of 128-bit AES key and 128-bit HMAC key, concatenated.

The Subscriber is responsible for applying reasonable protections on her device.

6.7.2. Mobile-ID

Refer to clause 6.7 of SK PS [3].

Subscriber is responsible for applying reasonable protections on her device.

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [3].

Not applicable to Subscribers.

7. Certificate, CRL, and OCSP Profiles

7.1. Certificate Profile

Certificate profile is described in the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/.

7.2. CRL Profile

Not applicable.

7.3. OCSP Profile

The OCSP profile is described in the Certificate Profile for Smart-ID [8] and the Certificate Profile for Mobile-ID [12], published in SK's public information repository https://www.skidsolutions.eu/en/repository/profiles/.

8. Compliance Audit and Other Assessments

Refer to chapter 8 of SK PS [3].

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

9.1.1.1. Qualified Smart-ID

Fee for issuance of certificate is published on SK website: https://www.skidsolutions.eu/en/repository/certificates-fees/.

Certificate renewal is not performed.

9.1.1.2. Mobile-ID

Fee for issuance of certificate is published on SK website: https://www.skidsolutions.eu/en/repository/certificates-fees/.

Certificate renewal is not performed.

9.1.2. Certificate Access Fees

Valid and activated Certificates are available via OCSP service.

Mobile-ID Certificates are also available in Mobile-ID Service Integration API [14].

There are no public records about the Certificates.

9.1.3. Revocation or Status Information Access Fees

Revocation of the Certificate of Q SID and Mobile-ID is free of charge.

An OCSP service for online verification is free of charge and publicly accessible.

The fee for Mobile-ID Service Integration API [14] is specified in the Subscriber or Relying Party agreement.

In case of other manners of publication information on certificate status, SK may fix a fee in a price list or require corresponding agreement.

9.1.4. Fees for Other Services

Fees for other services are specified in SK's price list or in the Subscriber's or Relying Party's agreement.

9.1.5. Refund Policy

Refer to clause 9.1.5 of SK PS [3].

Financial settlements are considered business secret of agreement parties.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Refer to clause 9.2.1 of SK PS [3].

9.2.2. Other Assets

Not applicable.

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of SK PS [3].

9.3. Confidentiality of Business Information

Refer to clause 9.3 of SK PS [3].

9.4. Privacy of Personal Information

Refer to clause 9.4 of SK PS [3].

9.5. Intellectual Property rights

SK obtains intellectual property rights to this CPS.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

9.6.1.1. Qualified Smart-ID

Refer to clause 9.6.1 of SK PS [3].

SK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- the supply of the certification service is in accordance with this CPS and the CP for Q Smart-ID [1];
- Q Smart-ID is recognised as QSCD;
- the Smart-ID App includes the component that has been recognised as part of QSCD;
- it keeps account of the certificates issued by it and of their validity;
- it provides the possibility to check the validity of certificates 24 hours a day;
- the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
- the certification keys used in the supply of the certification service are activated on the basis of shared control;
- it provides security with its internal security procedures.

As the Smart-ID App is used for applying for Q Smart-ID Certificates, application process by default implies the Subscriber's capability to visually see the Smart-ID App and generated PIN-codes as well as memorise them. While developing the Smart-ID App, SK always takes into account usability so that the application could be used by possibly wide range of users.

The application process initiated by minor, in any case assumes participation of minor's legal representative with legal capacity. Legal representative assists minor with applying for Q Smart-ID Certificates.

If the Subscriber has some sort of disability, the Customer Service Point assists with applying for the Certificates.

SK has right to share relevant data with Relying Party for the purpose of ensuring certificate usage security.

9.6.1.2. Mobile-ID

Refer to clause 9.6.1 of SK PS [3].

SK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- the supply of the certification service is in accordance with this CPS and the CP for Mobile-ID [13];
- it keeps account of the Certificates issued by it and of their validity;
- it provides the possibility to check the validity of Certificates 24 hours a day;
- it accepts and registers batches of Public Keys presented by MO;
- it accepts and registers the issuance of QSCD-s and corresponding Public Keys presented by MO;

- it accepts and registers the requests of the Certificates presented by MO and decides the issuance of the Certificates;
- it accepts, registers and processes the applications for revocation of Mobile-ID Certificates presented by the Subscriber, MO and competent authority;
- the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of SK;
- the certification keys used in the supply of the certification service are activated on the basis of shared control;
- it provides security with its internal security procedures.

Due to Mobile-ID Certificates being used for electronic identification and creating electronic signatures, usage of the Certificates imply legal capability of the Subscriber.

If the Subscriber has some sort of disability, MO Customer Service Point and MO Help Line assist with applying for and usage of the Certificates.

9.6.2. RA Representations and Warranties

9.6.2.1. Qualified Smart-ID

9.6.2.1.1. Smart-ID Provider

Smart-ID Provider ensures that:

- it accepts Subscriber applications for issuance of Q Smart-ID Certificates;
- provides Smart-ID Portal in accordance with the technical requirements set in applicable agreements.

9.6.2.1.2. Customer Service Point

Refer to clause 9.6.2 of SK PS [3].

The Customer Service Point ensures that:

- it accepts applications for the Certificates of Q Smart-ID and forwards the request for Q Smart-ID Certificates to SK;
- it accepts applications for the Certificate revocation and forwards the applications to SK;
- it checks the correctness and completeness of the revocation applications;
- it identifies and verifies the Subscriber submitting application for revocation;
- it keeps records to prove legitimacy of the Subscriber's actions;
- it provides security with its internal security procedures.

If the Subscriber has some sort of disability, the Customer Service Point assists with applying for the Certificates.

9.6.2.1.3. SK Customer Service Point

Refer to clause 9.6.2 of SK PS [3].

SK Customer Service Point ensures that:

- it accepts applications for the Certificate revocation;
- it checks the correctness and completeness of the revocation applications;
- it identifies and verifies the Subscriber submitting application for revocation;
- it keeps records to prove legitimacy of the Subscriber's actions;
- it provides security with its internal security procedures.

9.6.2.1.4. Help Line

Refer to clause 9.6.2 of SK PS [3].

The Help Line ensures that:

- it accepts requests for revocation of Certificates of Q Smart-ID from Subscribers;
- it provides security with its internal security procedures.

The Help Line takes calls from Subscribers and other parties 24 hours a day 7 days a week.

The Help Line immediately notifies SK about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

9.6.2.2. Mobile-ID

9.6.2.2.1. Mobile Operator

Refer to clause 9.6.2 of SK PS [3].

MO ensures that:

- it accepts applications from the Subscribers for the issuance and revocation of the Certificates and forwards them to SK;
- it checks the correctness and completeness of the applications submitted by the Subscribers;
- it identifies and verifies the Subscriber submitting an application for the issuance and revocation of the Certificates;
- it preserves Mobile-ID agreements signed by the Subscriber;
- it forwards batches of Public Keys to SK;
- it validates QSCD ownership and ensures the validity of the Public Keys presented for Certification;
- it accepts notifications from SK about Certificates issued by SK;
- the employees, who are involved with information related to certification service, are not punished for intentional crime;
- it provides security with its internal security procedures.

MO forwards true and complete data to SK.

MO immediately notifies SK about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

9.6.2.2.2. MO Customer Service Point

MO ensures that:

- it follows availability and security requirements on the information system related to Mobile-ID service at least to the level of the requirements described in this CPS;
- the employees, who accept applications regarding QSCD and Certificates and/or are involved with information related to certification service, are not punished for intentional crime;
- it provides security with its internal security procedures.

If the Subscriber has some sort of disability, MO Customer Service Point assists with applying for and usage of the Certificates.

9.6.2.2.3. MO Help Line

Refer to clause 9.6.2 of SK PS [3].

MO Help Line ensures that:

- it accepts requests for suspension of the telecommunication service from its Subscribers;
- it provides security with its internal security procedures.

MO Help Line takes calls from Subscribers 24 hours a day, 7 days a week.

MO Help Line immediately notifies SK about any technical failure hindering the supply of the service and uses all reasonable endeavours to repair the failure as soon as possible.

If the Subscriber has some sort of disability, MO Help Line assists with applying for and usage of the Certificates.

9.6.3. Subscriber Representations and Warranties

9.6.3.1. Qualified Smart-ID

Refer to clause 9.6.3 of SK PS [3].

The Subscriber ensures that:

- he/she adheres to the requirements provided by SK in this CPS;
- he/she presents true and correct information to Smart-ID System;
- in case of a change in his/her personal details, he/she notifies Smart-ID Provider of the correct details and revokes his/her Certificates during a reasonable time;
- he/she uses the Smart-ID App that is distributed by SK;
- he/she uses his/her Private Keys solely for creating Qualified Electronic Signatures;
- he/she uses his/her Private Keys and corresponding Certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her Private Key in accordance with this CPS;
- he/she immediately informs SK of a possibility of unauthorised use of his/her Private Key and revokes his/her Certificates;
- he/she immediately revokes his/her Certificates if his/her PIN codes have gone out of his/her control;
- he/she immediately revokes his/her Certificates if his/her Private Key has gone out of his/her possession;
- he/she no longer uses his/her Private Key, in the case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised;
- he/she is aware that Qualified Electronic Signatures given on the basis of expired or revoked Certificates are invalid.

The Subscriber is solely responsible for the maintenance of the part of the Private Key and PIN codes that are in his/her possession.

The Subscriber is obliged to agree with the processing of his/her biometric data for his/her identity validation purposes during Automated Biometric Identity Verification.

The Subscriber has to accept the Terms and Conditions of Q Smart-ID [9].

9.6.3.2. Mobile-ID

Refer to clause 9.6.3 of SK PS [3].

The Subscriber ensures that:

- he/she adheres to the requirements provided by SK in this CPS;
- he/she presents true and correct personal data to MO while submitting an application for QSCD or for change of QSCD;
- he/she notifies MO in case of Mobile-ID becoming unusable, lost or destroyed in accordance with the effective legislation;
- he/she uses his/her Private Keys solely for creating Qualified Electronic Signatures;
- he/she uses his/her Private Keys and corresponding Certificates pursuant to the procedure and in the manner prescribed by SK;
- he/she uses his/her Private Key in accordance with this CPS;
- in case of a change in his/her personal details stored in the Certificate he/she applies for a new QSCD and Mobile-ID Certificates in order to continue usage of the Mobile-ID service;
- he/she immediately informs SK of a possibility of unauthorised use of his/her Private Key and revokes his/her Certificates;
- he/she immediately revokes his/her Certificates if his/her Private Key has gone out of his/her possession or the device has been stolen;
- he/she no longer uses his/her Private Key, in case of being informed that his/her Certificate has been revoked or that the issuing CA has been compromised;
- he/she is aware that Qualified Electronic Signatures given on the basis of expired or revoked Certificates are invalid.

If the Subscriber has a suspicion that Mobile-ID has gone out of control of him/her at the time of suspension of the telecommunication service, the Subscriber is obliged to revoke the Certificates.

The Subscriber is solely responsible for the maintenance of his/her Private Key.

The Subscriber has to accept the Terms and Conditions of Mobile-ID [15].

9.6.4. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [3].

A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in this CPS, the CP for Q Smart-ID [1] and the CP for Mobile-ID [13].

If not enough evidence is enclosed to the Certificate or Electronic Signature with regard to the validity of the Certificate, a Relying Party verifies the validity of the Certificate on the basis of certificate validation services offered by SK at the time of using the Certificate or affixing a Qualified Electronic Signature.

A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CP for Q Smart-ID [1] and the CP for Mobile-ID [13].

A Relying Party uses CRL service on its own responsibility.

9.6.5. Representations and Warranties of Other Participants

9.6.5.1. Qualified Smart-ID

9.6.5.2. Smart-ID Provider

Smart-ID Provider ensures that:

- it adheres to the key generation and storage procedures under its control and described in this CPS;
- it adheres to provisions of fees described in this CPS;
- it transfers the correct Certificate and correct Certificate status information.

Smart-ID Provider is entitled to withdraw Identity Provider status if it obtains evidence that Identity Provider has not been following Requirements for Identity Providers [10] for qualified certificates.

9.6.5.2.1. Identity Provider

Identity Provider follows Requirements for Identity Providers [10] for qualified certificates.

9.6.5.2.2. Biometric Verification Provider

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

9.6.5.2.3. Secondary Subscriber Authentication Provider

Secondary Subscriber Authentication Provider SHALL follow the Requirements for Secondary Subscriber Authentication Providers [16].

9.6.5.3. Mobile-ID

9.6.5.3.1. 9.6.5.2.1. SIM-card Manufacturer

SCM is responsible for all operations and procedures regarding the production of QSCD, including secure key generation and loading as well as Public Key delivery to SK.

9.6.5.3.2. Mobile Operator

MO ensures that:

- it requests revocation of the Certificates from SK if she terminates telecommunication service provided to the Subscriber.

9.7. Disclaimers of Warranties

Refer to clause 9.7 of SK PS [3].

9.8. Limitations of Liability

Refer to clause 9.8 of SK PS [3].

9.9. Indemnities

Indemnities between the Subscriber and SK are regulated in the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15].

9.10. Term and Termination

9.10.1. Term

Refer to clause 2.2.1 of this CPS.

9.10.2. Termination

Refer to clause 9.10.2 of SK PS [3].

9.10.3. Effect of Termination and Survival

SK communicates the conditions and effect of this CPS's termination via its public repository. The communication specifies which provisions survive termination.

At a minimum, all responsibilities related to protecting personal and confidential information, also maintenance of SK archives for determined period and logs survive termination. All Subscriber agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

Termination of this CPS cannot be done before termination actions described in clause 5.8 of this CPS.

9.11. Individual Notices and Communications with Participants

The Subscriber is granted a right to get familiarised with the Terms and Conditions of Q Smart-ID [9] and the Terms and Conditions of Mobile-ID [15], before agreeing to and signing it.

The Subscriber's individual notices are communicated via the Subscriber's email address or mobile phone number contained in registration form for Smart-ID Account or for Mobile-ID.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to clause 1.5.4 of this CPS.

9.12.2. Notification Mechanism and Period

Refer to clause 2.2.1 of this CPS.

9.12.3. Circumstances Under Which OID Must be Changed

Not applicable.

9.13. Dispute Resolution Provisions

Refer to clause 9.13 of SK PS [3].

The Subscriber or other party can submit their claim or complaint at the email address info@skidsolutions.eu

9.14. Governing Law

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

9.15. Compliance with Applicable Law

Refer to clause 9.15 of SK PS [3].

Additionally, SK ensures compliance with the General Data Protection Regulation [7].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

SK contractually obligates each RA to comply with this CPS and applicable industry guidelines. SK also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party prevails, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of SK. Unless specified otherwise in a contract with a party, SK does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS remains valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

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

SK may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. SK's failure to enforce a provision of this CPS does not waive SK's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by SK.

9.16.5. Force Majeure

Refer to clause 9.16.5 of SK PS [3].

9.17. Other Provisions

Not applicable.

10. References

1. SK ID Solutions AS – Certificate Policy for Qualified Smart-ID, published: https://www.skidsolutions.eu/en/repository/CP/;
2. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
3. SK ID Solutions AS Trust Services Practice Statement, published: https://www.skidsolutions.eu/en/repository/sk-ps/;
4. ETSI EN 319 411-2 V2.2.1 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;
5. ETSI EN 319 411-1 V1.2.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
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. 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;
8. Certificate and OCSP Profile for Smart-ID, published: https://www.skidsolutions.eu/en/repository/profiles/;
9. Terms and Conditions for Use of Certificates of Qualified Smart-ID, published: https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/;
10. Requirements for Identity Providers, published: https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-for-identity-providers;
11. SK ID Solutions AS - NQ SK Certification Practice Statement, published: https://www.skidsolutions.eu/en/repository/CPS/;
12. Certificate and OCSP Profile for Mobile-ID of Lithuania, published: https://www.skidsolutions.eu/en/repository/profiles/;
13. SK ID Solutions AS - Certificate Policy for Mobile-ID of Lithuania, published: https://www.skidsolutions.eu/en/repository/CP/;
14. Mobile-ID REST API: https://github.com/SK-EID/MID;
15. Terms and Conditions for Use of Certificates of Mobile-ID of Lithuania, published: https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/;
16. Requirements for Secondary Subscriber Authentication Providers, published: https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-for-SSAP/;
17. Requirements of Identity Validation for RA, published: https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-of-identity-validation-RA/;
18. Consent for Automated Biometric Identity Verification published: https://www.skidsolutions.eu/en/repository/data-protection/.