SK ID Solutions AS – SK-rQSCD Management of Remote Qualified Electronic Signature Creation Device Service Practice Statement

Name	SK-rQSCD Management of Remote Qualified Electronic Signature Creation Device Service Practice Statement
Version No	1.0
Version History	
Date and Version No	Changes
01.05.2026 1.0	• First public version.
Effective from date	01.05.2026

1. Introduction 6
1.1. Overview 6
1.2. Document Name and Identification 7
1.3. Participants in Remote Qualified Electronic Signature Creation Device Service 7
1.3.1. Server Signing Application Service Provider 7
1.3.2. Certification Authorities 7
1.3.3. Registration Authorities 7
1.3.4. Help Line 7
1.3.5. Subscribers 7
1.3.6. Relying Parties 7
1.4. Remote Qualified Electronic Signature Creation Device Service Usage 7
1.4.1. Appropriate Service Uses 7
1.4.2. Prohibited Service Uses 7
1.5. Policy Administration 8
1.5.1. Organization Administering the Document 8
1.5.2. Contact Person 8
1.5.3. Person Determining CPS Suitability for the Policy 8
1.5.4. CPS Approval Procedures 8
1.6. Definitions and Acronyms 8
1.6.1. Terminology 8
1.6.2. Acronyms 10
2. Publication and Repository Responsibilities 11
2.1. Repositories 11
2.2. Publication of Certification Information 11
2.2.1. Publication and Notification Policies 11
2.2.2. Items not Published in the Certification Practice Statement 11
2.3. Time or Frequency of Publication 11
2.4. Access Controls on Repositories 12
3. Identification and Authentication 13
3.1. Naming 13
3.2. Initial Identity Validation 13
3.2.1. Method to Prove Possession of Private Key 13
3.2.2. Authentication of Organization Identity 13
3.2.3. Authentication of Individual Identity 13
3.2.4. Non-Verified Subscriber Information 13
3.2.5. Validation of Authority 13
3.2.6. Criteria for Interoperation 13
3.3. Identification and Authentication for Private Key Control 13
3.3.1. Identification and Authentication for Routine Re-Key 13

3.3.2. Identification and Authentication for Re-Key After Key Deletion 13
3.4. Identification and Authentication for Key Deletion 13
4. Certificate Life-Cycle Operational Requirements 14
5. Facility, Management, and Operational Controls 15
5.1. Physical Controls 15
5.2. Procedural Controls 15
5.3. Personnel Controls 15
5.4. Audit Logging Procedures 15
5.5. Records Archival 15
5.5.1. Types of Records Archived 15
5.5.2. Retention Period for Archive 15
5.5.3. Protection of Archive 15
5.5.4. Archive Backup Procedures 15
5.5.5. Requirements for Time-Stamping of Records 15
5.5.6. Archive Collection System (Internal or External) 15
5.5.7. Procedures to Obtain and Verify Archive Information 15
5.6. Key Changeover 15
5.7. Compromise and Disaster Recovery 15
5.8. Termination of Service 16
5.9. Supply Chain 16
6. Technical Security Controls 17
6.1. Key Pair Generation and Installation 17
6.1.1. Key Pair Generation 17
6.1.2. Private Key Delivery to Subscriber 18
6.1.3. Public Key Delivery to Certificate Issuer 19
6.1.4. CA Public Key Delivery to Relying Parties 19
6.1.5. Signature suites 19
6.1.6. Key Sizes 19
6.1.7. Public Key Parameters Generation and Quality Checking 20
6.1.8. Key Usage Purposes (as per X.509 v3 Key Usage Field) 20
6.2. Private Key Protection and Cryptographic Module Engineering Controls 20
6.2.1. Cryptographic Module Standards and Controls 20
6.2.2. Private Key (n out of m) Multi-Person Control 20
6.2.3. Private Key Escrow 20
6.2.4. Private Key Backup 20
6.2.5. Private Key Archival 21
6.2.6. Private Key Transfer Into or From a Cryptographic Module 21
6.2.7. Private Key Storage on Cryptographic Module 21
6.2.8. Method of Activating Private Key 22
6.2.9. Method of Deactivating Private Key 23

6.2.10. Method of Destroying Private Key 23
6.2.11. Cryptographic Module Rating 24
6.3. Other Aspects of Key Pair Management 24
6.3.1. Public Key Archival 24
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 24
6.4. Activation Data 24
6.4.1. Activation Data Generation and Installation 24
6.4.2. Activation Data Protection 24
6.4.3. Other Aspects of Activation Data 24
6.5. Computer Security Controls 24
6.5.1. Specific Computer Security Technical Requirements 24
6.5.2. Computer Security Rating 24
6.6. Life Cycle Technical Controls 24
6.7. Network Security Controls 25
6.8. Time-Stamping 25
7. Certificate, CRL, and OCSP Profiles 26
8. Compliance Audit and Other Assessments 27
9. Other Business and Legal Matters 28
9.1. Fees 28
9.2. Financial Responsibility 28
9.2.1. Insurance Coverage 28
9.2.2. Other Assets 28
9.2.3. Insurance or Warranty Coverage for End-Entities 28
9.3. Confidentiality of Business Information 28
9.4. Privacy of Personal Information 28
9.5. Intellectual Property rights 28
9.6. Representations and Warranties 28
9.6.1. SSASP Representations and Warranties 28
9.6.2. CA Representations and Warranties 29
9.6.3. RA Representations and Warranties 29
9.6.4. Help Line Representations and Warranties 29
9.6.5. Subscriber Representations and Warranties 29
9.6.6. Relying Party Representations and Warranties 30
9.7. Disclaimers of Warranties 30
9.8. Limitations of Liability 30
9.9. Indemnities 30
9.10. Term and Termination 30
9.10.1. Term 30
9.10.2. Termination 30
9.10.3. Effect of Termination and Survival 30

9.11. Individual Notices and Communications with Participants 30
9.12. Amendments 30
9.12.1. Procedure for Amendment 30
9.12.2. Notification Mechanism and Period 31
9.12.3. Circumstances Under Which OID Must be Changed 31
9.13. Dispute Resolution Provisions 31
9.14. Governing Law 31
9.15. Compliance with Applicable Law 31
9.16. Miscellaneous Provisions 31
9.16.1. Entire Agreement 31
9.16.2. Assignment 31
9.16.3. Severability 31
9.16.4. Enforcement (Attorney's Fees and Waiver of Rights) 31
9.16.5. Force Majeure 31
9.17. Other Provisions 31
10. References 32

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, Time-Stamping Unit or other Trust Services;
- 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] is included where applicable.

1.1. Overview

Server Signing Application Service (SSAS) operates remote Qualified electronic Signature Creation Device (rQSCD) that is based on Threshold Signature Scheme Protocol (TSSP) following eIDAS [6] article 29a. TSSP is the protocol to be followed by Signer, who uses client-side functions with software component (TSE), which is running on the personal mobile device of the Signer, and a server-side software component, that is connected to the Hardware Security Module (HSM). Together, TSE, server-side software component, and HSM form the QSCD) [11, 13].

SSAS provides also electronic identification (eID) mean functionality, which conforms to eIDAS [6] article 8 (2) defined assurance level high. For the eID mean operations Subscriber receives another set of keys and corresponding certificate for authentication.

The private key of the key pair of the Signer is generated in shares. It is done in such a way, that multiple shares of the private key are separately generated and they are independently protected by the Signer and TSE and the server-side software and HSM (see clause 6.1.1 of this CPS). To create the digital signature of the Signer, those individual shares of the private key must be used by their respective holders to create the shares of the signature. Those shares of the signature must then be combined, and the resulting compound signature is then verifiable with the public key of the Signer [11, 13].

The Signer, who follows the client-side functions of the TSSP, can use the server-side services to enrol new key pairs, create digital signatures and to destroy the key pairs. The important distinction here is that the server-side alone doesn't create the whole digital signature on behalf of the Signer, but they both participate in the cryptographic protocol [11, 13].

This CPS covers the practices used in management of remote qualified electronic signature creation device to comply with EUSPv2: EU SSAS Policy (EUSPV2, OID 0.4.0.19431.1.1.4) following [20]. SSAS deploys QSCD that meets the requirements laid down in Annex II of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [6]. SSASP conforms to requirements identified in the certification report of the deployed remote qualified electronic signature creation device issued pursuant to Article 30 of Regulation (EU) 2024/1183 [i.11] amending Regulation (EU) No 910/2014 [6].

SSAS can be utilised by Subscribers only in combination with Qualified Trust Service Providers issuing Qualified Certificates for Electronic Signatures. It is up to authentication and signing solution provider which Certification and Registration Authorities will be integrated for provision of complete user journey to Subscribers and Relying Parties.

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

The management of remote qualified electronic signature creation device service described in this CPS has qualified trust service status in the Trusted List of Estonia.

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

- EUSPV2;
- This CPS.

1.2. Document Name and Identification

This document is called “SK ID Solutions AS – SK-rQSCD Management of Remote Qualified Electronic Signature Creation Device Service Practice Statement.”

1.3. Participants in Remote Qualified Electronic Signature Creation Device Service

1.3.1. Server Signing Application Service Provider

SK operates as a Server Signing Application Service Provider that manages Remote Qualified Electronic Signature Creation Device Service. SK as SSASP generates and manages qualified electronic signature data on behalf of signatory.

1.3.2. Certification Authorities

Certification Authority (CA) is responsible for issuing Qualified Certificates for Electronic Signatures and Authentication Certificates to Subscriber. CA receives the Subscriber’s identity information from RA and Subscriber’s public key from SSASP. CA provides certification service related to the life cycle of Certificates.

1.3.3. Registration Authorities

Registration Authorities (RA) provide Subscriber registration, identification and authentication services for Certificate Authorities and SSASP. The RA forwards registration information to the CA, so that CA can issue the Certificates for binding together the identity and public key of Subscriber. In addition, applications from Subscriber for revocation of Certificates and key deletion are accepted by RA.

1.3.4. Help Line

The Help Line acts as the representative of SSASP or RA in the field of Subscriber telephone servicing. The Help Line provides user support for solving problems related to SSAS and Certificate usage.

The Help Line accepts from Subscribers requests for revocation of Certificates and key deletion.

1.3.5. Subscribers

Subscriber is a natural person associated to the private key managed by SSASP.

1.3.6. Relying Parties

A Relying Party is a natural or legal person who relies on the SSAS provided by SSASP. RP is providing Signature Creation Application (SCA) for the Subscriber. SCA is integrated with SSAS using RP-API [19].

1.4. Remote Qualified Electronic Signature Creation Device Service Usage

rQSCD Service is provided as Subscriber key management service for generating Qualified Electronic Signatures and for electronic identification with level of assurance high.

1.4.1. Appropriate Service Uses

rQSCD Service is intended for:

- creating Qualified Electronic Signatures compliant with eIDAS [6];
- authenticating with level of assurance high compliant with eIDAS [6].

1.4.2. Prohibited Service Uses

rQSCD Service SHALL NOT be used for any of the following purposes:

- Unlawful activity (including cyber attacks and attempt to infringe the rQSCD Service);
- enabling other parties to use the Subscriber’s Private Key;
- enabling the Activation Data to be used in an automated way;

- using the Subscriber keys in a way which can bring about unwanted consequences (including signing such documents for testing purposes);
- The Subscriber authentication key SHALL NOT be used to create Qualified Electronic Signatures compliant with eIDAS [6].

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS is administered by SK.

SK ID Solutions AS

Registry code 10747013

Pärnu Ave 141, 11314 Tallinn

Tel +372 610 1880

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 ETSI TS 119 431-1 [20] 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.

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 or COO.

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.
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].

Term	Definition
Certificate	Public Key together with additional information, laid down in the Certificate Profile defined by CA, rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of SK structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.
Certificate 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.
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.
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).
Object Identifier	An identifier used to uniquely name an object (OID).
PIN code	Activation code for a Private Key.
Private Key	The key of an asymmetric 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 or authenticate Subscriber. Electronic signature creation and authentication functions have their own dedicated private keys. In the SSAS 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 an assymetric 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.
PUK code	Code for unblocking of PIN codes when they have been blocked after number of allowed consecutive incorrect entries or changing PIN/PUK codes' values.
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.
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].

Term	Definition
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications and Certificate revocation applications, check the applications and/or forward the applications to the Certificate Authority.
Relying Party	Entity that relies on the information contained within a Certificate or Certificate status information provided by SK.
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.
HSM module	The hardware security module used in the SSAS system. Common Criteria certified cryptographic device.
SSAS Account	SSAS Account binds Smart-ID App instance to a Subscriber's identity in the Smart-ID System. SSAS Account has a Qualified Electronic Signature key and an Authentication key.
SSAS Mobile Application	Android/iOS mobile application providing GUI for the Subscriber inside the Subscriber's mobile device. SSAS Mobile Application contains the software component (mobile device library), which handles the private key generation and usage.
SSAS Portal	The interaction point with the SSAS System for the Subscriber that is accessible via a web browser. The Portal provides access to SSAS Account registration and management functionality.
SSAS Server	A technical component of the SSAS System that handles back-end operations.
SSAS System	A technical and organisational environment which enables Electronic Authentication and Electronic Signatures in an electronic environment. The SSAS system provides services that allow Subscribers to authenticate themselves, to create Qualified Electronic Signatures, and to manage their keys.
Signer	In this document, the Signer is the same as the Subscriber.
Signing Key	In this document, the Signing Key is the same as the Private Key.
Subscriber	A natural person associated to the private key managed by SSASP.
Terms and Conditions	Document provided by CA that includes obligations and responsibilities of the Subscriber with respect to using private keys. The Subscriber has to be familiar with the document and accept the Terms and Conditions upon receipt of the Certificates provided by CA.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement.
CSR	Certificate Signing Request

Acronym	Definition
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, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [6]
EU	European Union
HSM	Hardware security module is a physical computing device that safeguards and manages digital encryption keys and provides crypto processing.
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [5]
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
RP	Relying Party
RP-API	Relying Party Application Programming Interface
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].

2.2. Publication of Certification Information

Refer to clause 2.2 of SK PS [3].

2.2.1. Publication and Notification Policies

This CPS is published on SK's website: https://www.skidsolutions.eu/resources/certification-practice-statement/.

This CPS and Terms and Conditions related to rQSCD Service together with the enforcement dates are published on SK's website https://www.skidsolutions.eu/resources/ no less than 30 days prior to taking effect.

Note: Terms and Conditions related to rQSCD Service are included in respective document provided by CA issuing Certificates [9].

2.2.2. Items not Published in the Certification Practice Statement

Refer to clause 9.3.1 of SK PS [3].

2.3. Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.4. Access Controls on Repositories

Refer to clause 2.4 of SK PS [3].

3. Identification and Authentication

3.1. Naming

Not applicable.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Not applicable.

3.2.2. Authentication of Organization Identity

Not applicable.

3.2.3. Authentication of Individual Identity

The Subscriber identity verification and authentication are performed by Registration Authority contracted by Certification Authority. Identity verification and authentication processes follow EN 419241-1 [23] requirements. In detail practices are defined in relevant CPS of Certification Authority and adhere to requirements of ETSI TS 119 461 [25] for extended Level of Identity Proofing (LoIP).

SSASP validates that the person identification data linked to the identity is the same as the on linked to the Subscriber of the associated Certificate of Qualified Electronic Signature.

3.2.4. Non-Verified Subscriber Information

Not applicable.

3.2.5. Validation of Authority

The Subscriber can apply for rQSCD Service only personally. RA checks whether the Subscriber has legal capacity.

If the minor applies for rQSCD Service, RA verifies the right of representation of the minor's legal representative.

3.2.6. Criteria for Interoperation

Not applicable.

3.3. Identification and Authentication for Private Key Control

SSAS requires each Subscriber to be successfully identified and authenticated before allowing any actions that can impact the sole control of any private key.

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 Key Deletion

Refer to clause 3.2 of this CPS.

3.4. Identification and Authentication for Key Deletion

Refer to relevant CPS of Certification Authority.

4. Certificate Life-Cycle Operational Requirements

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, usage and management of QSCD are kept. Audit logging function only appends information. All audit records contain following parameters:

- Date and time of event;
- Type of event;
- Identity of the entity responsible for the action;
- Success or failure of the audited event.

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 key deletion 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

Not applicable.

5.7. Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [3].

5.8. Termination of Service

Refer to clause 5.8 of SK PS [3].

5.9. Supply Chain

Refer to clause 5.9 of SK PS [3].

6. Technical Security Controls

6.1. Key Pair Generation and Installation

Subscriber's private key is generated and used within multiple components:

- in a trustworthy system, which meets the assurance requirements of assurance level EAL 4 (Evaluation Assurance Level 4) augmented by AVA_VAN.5 (Advanced methodical vulnerability analysis) and corresponds to protection profile for TSP cryptographic modules – Part 5: cryptographic module for Trust Services (EN 419221-5:2018) [21, 24];
- inside the Subscriber's mobile device using the software component (mobile device library) that is intended to be embedded inside an Android/iOS mobile application, which provides a GUI for the Subscriber. Named library meets the assurance requirements of assurance level EAL 2 (Evaluation Assurance Level 2) [22].

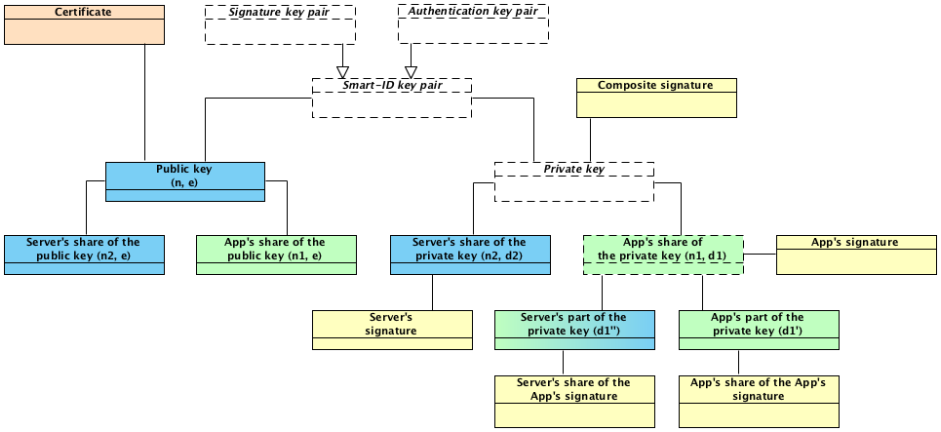
SSAS supports cryptographic algorithms, their parameters and key lengths corresponding to ETSI TS 119 312 [22]. Detailed list of supported cryptographic algorithms and key lengths are provided in clauses 6.1.5 and 6.1.6 of this CPS.

6.1.1. Key Pair Generation

SSAS Key Pair Terminology

SSAS 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 SSAS mobile application, 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 SSAS 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 SSAS 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 SSAS Mobile Application. 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 SSAS Mobile Application and stored in the SSAS Mobile Application 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 SSAS Mobile Application 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.



SSAS Key Pair Generation

Subscriber Key Pair is generated during the SSAS registration process in the SSAS Mobile Application and in the SSAS 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. SSAS Mobile Application 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. SSAS Mobile Application 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'. SSAS Mobile Application computes the 'Server's part of the private key' and transmits the 'Server's part of the private key' securely to the SSAS 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. SSAS server generates the keypair inside the SSAS 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 SSAS server from the 'App's share of the public key' and 'Server's share of the public key'. This way all the SSAS keypair components are tied together with the 'Public key'.

6.1.2. Private Key Delivery to Subscriber

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

6.1.2.1. 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.

6.1.2.2. 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 SSAS server. The transmission is handled in the following way:

1. The key-transmission-key (KTK) key pair is generated inside the SSAS 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 SSAS Mobile Application;

3. During the registration procedure, the SSAS Mobile Application and SSAS 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 SSAS 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 SSAS 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 SSAS 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 SSAS HSM module.

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

The 'Server's share of the private key' is generated inside the SSAS HSM module and is always protected by the HSM module. SSASP generates the ‘Server’s share of the private key’ in advance in batches (i.e. not linked to a Subscriber or a public key certificate).

6.1.3. Public Key Delivery to Certificate Issuer

The Subscriber's 'Public key' is computed inside the SSAS 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. Delivery of 'App's share of the public key' from SSAS Mobile Application to SSAS server

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

6.1.3.2. Delivery of 'Server's share of the public key' from SSAS HSM to SSAS server

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

6.1.4. CA Public Key Delivery to Relying Parties

Not applicable.

6.1.5. Signature suites

Supported signature algorithms:

1. RSASSA-PKCS1-v1_5;
2. RSASSA-PSS.

Supported hash functions:

1. SHA-256, SHA-384 and SHA-512;
2. SHA3-256, SHA3-384 or SHA3-512.

6.1.6. Key Sizes

Supported key sizes:

1. 'App's share of the private key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits RSA private key;
2. 'App's part of the private key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits number;

3. 'Server's part of the private key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits number;
4. 'Server's share of the private key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits RSA private key;
5. 'App's share of the public key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits RSA public key;
6. 'Server's share of the public key' is a 3071, 3072, 4095, 4096, 6143, 6144, 8191, or 8192 bits RSA public key;
7. 'Public key' is a 6142, 6143, 6144, 8190, 8191, 8192, 12286, 12287, 12288, 16382, 16383, or 16384 bits RSA public key;

6.1.7. Public Key Parameters Generation and Quality Checking

Quality of public keys is guaranteed by employing secure random number generators by the Subscriber's mobile device using the software component and trustworthy system's HSM module, and following the specified algorithms in the FIPS 186-5. 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 by CA over database of issued Certificates regularly.

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

Not applicable.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

SSAS Mobile Application cryptographic library standards

SSAS Mobile Application on the Android and iOS platforms are corresponding to EAL 2 [22].

SSAS server cryptographic library standards

The SSAS server is using SSAS HSM module for the cryptographic operations. HSM is certified to be compliant with the QSCD requirements according to eIDAS Regulation [6].

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

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 SSAS system, the presence of at least two authorized persons is required in accordance with clause 5.2.2 of SK PS [3].

6.2.3. Private Key Escrow

Refer to clause 6.2.3 of SK PS [3].

SSASP does not offer Key Escrow services to Subscribers.

6.2.4. Private Key Backup

Refer to clause 6.2.4 of SK PS [3].

In general, SSAS doesn't provide the private key backup services. SSASP makes the following exceptions to the following components of the Subscriber's private key in order to support high availability of the SSAS system,

whereas number of duplicated datasets does not exceed the minimum needed to ensure continuity of the service. All backed up components of the Subscriber's private key are securely stored while ensuring same level of confidentiality and integrity within SSAS.

6.2.4.1. 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 SSAS Mobile Application 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.

6.2.4.2. 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 SSAS database.

The SSAS database is regularly synchronised upon key generation and destruction to another data center and regularly copied to the backup storage.

6.2.4.3. 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 SSAS HSM module.

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

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

The 'Server's share of the private key' is protected by the SSAS HSM module.

The SSAS HSM module is regularly synchronised upon key generation and destruction to another data center and regularly backed up to backup storage.

6.2.5. Private Key Archival

Refer to clause 6.2.5 of SK PS [3].

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

6.2.6. Private Key Transfer Into or From a Cryptographic Module

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.

6.2.7. Private Key Storage on Cryptographic Module

SSAS access controls ensure that Subscriber does not have access to sensitive system objects and any functions which gives the user control over another's private key.

Refer to clause 6.2.7 of SK PS [3].

6.2.7.1. 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 SSAS Mobile Application 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 SSAS Mobile Application. The AES encryption algorithm is used in the CBC mode and without any padding.

6.2.7.2. 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 SSAS 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 SSAS HSM module.

6.2.7.3. 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 SSAS HSM module and protected by the HSM module.

6.2.8. Method of Activating Private Key

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.

Signature Activation Data (SAD) is a result of cryptographic operations. SAD parameters are composed by Signature Creation Application (SCA) and in the Subscriber's mobile device using the software component (library) that is intended to be embedded inside an Android/iOS mobile application and [11, 13].

SAD includes amongst others EN 419 241-1 [23] defined mandatory parameters [11, 13]:

1. A given DTBS/R (digest value that is generated from DTBS);
2. Items to identify the authenticated signer (App's part of Signature, which is created using PIN);
3. Private key unique identifier, which connects all of the assets (App's part of the private key, Server's part of the private key, Server's share of the private key) related to the private key.

SAD is used to activate private key only if Subscriber authentication (verification of App's Signature share with App's share of the public key) and additional security checks succeed. SAD verification is conducted such that activities (e.g. guessing, eavesdropping, replay or manipulation of communication) by an attacker with high attack potential is highly unlikely to subvert the authentication for signature activation [11, 13].

SAD is passed to SAM in the Signature Activation Protocol (SAP). SAP is designed such that SAD can submitted only under sole control of the Subscriber by means that are in the possession of the Subscriber [11, 13].

SAD is collected under the control of Subscriber with high level of confidence, protected by secure key storage in devices (see clause 6.1 of this CPS), and protects used secrets following EN 419 241-1 [23] requirements [11, 13].

6.2.8.1. 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 SSAS Mobile Application for each transaction. The value of PIN is never stored by the SSAS Mobile Application.

Subscriber's PIN is chosen by the Subscriber during the registration process of SSAS.

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.

6.2.8.2. 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 SSAS 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 SSAS 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 SSAS server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the SSAS Mobile Application 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 SSAS Mobile Application 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'.

6.2.8.3. 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 SSAS HSM module. To allow SSAS 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 SSAS 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 SSAS server. The access is granted only after successful validation of the possession-based authentication factor (one-time password, presented by the SSAS Mobile Application 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'.

6.2.9. Method of Deactivating Private Key

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. 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 SSAS Mobile Application memory after the operation is completed or when the SSAS server responds with 'Wrong PIN' error message.

6.2.9.2. 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 SSAS server memory after the operation is completed or when the SSAS server responds with 'Wrong PIN' error message.

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

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

6.2.10. Method of Destroying Private Key

Refer to clause 6.2.10 of SK PS [3].

Private key is automatically destroyed after the expiration of the public key certificate or if the private key is useless for the Subscriber.

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

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

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

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

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

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

6.2.11. Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS.

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 SSAS 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 CA's respective CPS.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

Refer to clause 6.4.1 of SK PS [3].

SSAS Mobile Application 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 SSAS Mobile Application nor in the SSAS System.

6.4.2. Activation Data Protection

Refer to clause 6.4.2 of SK PS [3].

The initial activation data is generated by the SSAS Mobile Application or chosen by the Subscriber.

After that, activation codes themselves are never stored in the SSAS Mobile Application nor in the SSAS System.

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

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 mobile 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 mobile device.

6.6. Life Cycle Technical Controls

Refer to clause 6.6 of SK PS [3].

Subscriber is responsible for applying reasonable protections on mobile device.

6.7. Network Security Controls

Refer to clause 6.7 of SK PS [3].

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

SSAS Mobile Application and SSAS server further use the established transmission-encryption-key (TEK) to secure the network requests and responses. SSAS Mobile Application 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 mobile device.

6.8. Time-Stamping

Refer to clause 6.8 of SK PS [3].

Not applicable to Subscribers.

7. Certificate, CRL, and OCSP Profiles

Not applicable.

8. Compliance Audit and Other Assessments

Refer to chapter 8 of SK PS [3].

9. Other Business and Legal Matters

9.1. Fees

Fee for management of rQSCD is included in the issuance fee of certificate, which is published on CA's website. Fees for other services are specified in SK's price list or in the Subscriber's or Relying Party's agreement.

Refund policy is described in 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. SSASP Representations and Warranties

Refer to clause 9.6.1 of SK PS [3].

SSASP ensures that:

- the supply of the SSAS is in accordance with the relevant legislation;
- rQSCD is recognised as QSCD;
- the SSAS Mobile Application includes the mobile device library that has been recognised as part of QSCD;
- it keeps account of the keys managed by it and of their validity;
- it provides security with its internal security procedures;
- it complies with all requirements identified in certification report of the QSCD [21, 24];
- QSCD is operated in its configuration as described in the appropriate certification guidance documents [21, 24];
- signature activation data (SAD) contains the unique identifier of the signature session which is uniquely linked to the SASS and the unique identifier of the identity verification process;
- the public key certificate is valid before using the corresponding private key;
- adequate controls are provided for countering threats of PIN guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing and masquerading attacks;
- Subscriber's keys are linked with appropriate Subscriber's public key certificate;
- private key is not used before its public key Certificate is linked by SSASP, except for signing a proof of possession in order to obtain a certificate;

- integrity of links between Subscriber's private key and public key certificate is protected;
- identity verification and authentication processes of Certification Authority follow EN 419241-1 [23] requirements.

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

9.6.2. CA Representations and Warranties

Certification Authority ensures that:

- it is qualified trust service provider that issues Qualified Certificates for electronic signatures compliant with the relevant requirements as defined in eIDAS [6];
- it issues Authentication Certificates based on the requirements of the COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 [26] and the Policy NCP+: Normalised Certificate Policy requiring a Secure Cryptographic Device.

9.6.3. RA Representations and Warranties

Registration Authority ensures that:

- it accepts Subscriber applications for generation of key generation and usage, and for Qualified Certificates of Electronic Signature;
- it verifies Subscriber's legal capacity and in case of minor right of representation of Subscriber's legal representative;
- identity verification and authentication processes follow EN 419241-1 [23] requirements, in particular adhere to requirements of ETSI TS 119 461 [25] for extended Level of Identity Proofing (LoIP).

9.6.4. Help Line Representations and Warranties

Refer to clause 9.6.2 of SK PS [3].

The Help Line ensures that:

- it accepts requests for revocation of Certificates and key deletion 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.

9.6.5. Subscriber Representations and Warranties

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 SSAS;
- in case of a change in his/her personal details, he/she notifies CA of the correct details and revokes his/her Certificates during a reasonable time;
- he/she uses the SSAS Mobile Application that is distributed by SSAS;
- he/she uses his/her respective Private Keys solely for creating Qualified Electronic Signatures or electronic identification;
- 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 has to accept the Terms and Conditions [9].

9.6.6. Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [3].

The Relying Party ensures that:

- SCA service provided to Subscribers conforms to established requirements and technical specifications of SSAS.

A Relying Party studies the risks and liabilities related to usage of SSAS. The risks and liabilities have been set out in this CPS, and in the General Terms of Subscriber Agreement [27].

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 [9].

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 CA 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 [9], 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 SSAS.

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 CA and 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. RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
2. SK ID Solutions AS Trust Services Practice Statement, published: https://www.skidsolutions.eu/resources/trust-services-practice-statement/;
3. ETSI EN 319 411-2 V2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;
4. ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
5. 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, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework;
6. 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;
7. Terms and Conditions, published: https://www.skidsolutions.eu/resources/conditions-for-use-of-certificates/;
8. Smart-ID REST API, published: https://github.com/SK-EID/smart-id-documentation/ and https://sk-eid.github.io/smart-id-documentation/rp-api/introduction.html;
9. ETSI TS 119 431-1 V1.3.1 (2024-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev;
10. eIDAS compliant QSCD certificate for Smart-ID SecureZone, published: https://www.skidsolutions.eu/wp-content/uploads/2025/03/9803UE.pdf;
11. Common Criteria Certificate and Certification Report for Smart-ID App Threshold Signature Engine, published: https://www.skidsolutions.eu/wp-content/uploads/2024/11/9266UE.pdf and https://www.skidsolutions.eu/wp-content/uploads/2024/11/9266BE.pdf;
12. EN 419241-1:2018 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements, published: https://www.cencenelec.eu/;
13. Common Criteria Certificate and Certification Report for Smart-ID SecureZone, published: https://www.tuev-nord.de/fileadmin/Content/TUEV_NORD_DE/zertifizierung/Zertifikate/en/9265UE.pdf and https://www.tuev-nord.de/fileadmin/Content/TUEV_NORD_DE/zertifizierung/Zertifikate/en/9265BE.pdf;
14. ETSI TS 119 461 V2.1.1 (2025-02) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
15. COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
16. SK ID Solutions – General Terms of Subscriber Agreement, published: https://www.skidsolutions.eu/resources/general-terms-of-subscriber-agreement/.