AS Sertifitseerimiskeskus
Trust Services Practice Statement

Version 2.0
01.07.2016

Version and Changes		
Date	**Version**	**Changes**
01.07.2016	2.0	The following amendments and additions were made: - clause 6.1.1 the key ceremony commission is appointed by CEO with internal regulation. The commission has to include the external auditor independent of SK; - clause 6.2.1 HSM is the FIPS mode activated; - clause 6.2.1 SK checks and verifies that HSM is not tampered after its receive and installation. This is documented in a HSM life-cycle protocol.
01.04.2016	1.9	Draft version of SK PS version 2.0 valid from 01.07.2016. Redesigned according to RFC 3647. Amendments regarding eIDAS Regulation compliance.
01.10.2014	1.0	First public version.

1. INTRODUCTION

AS Sertifitseerimiskeskus (hereafter 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 in the Baltic region. 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 Trust Services Practice Statement (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.

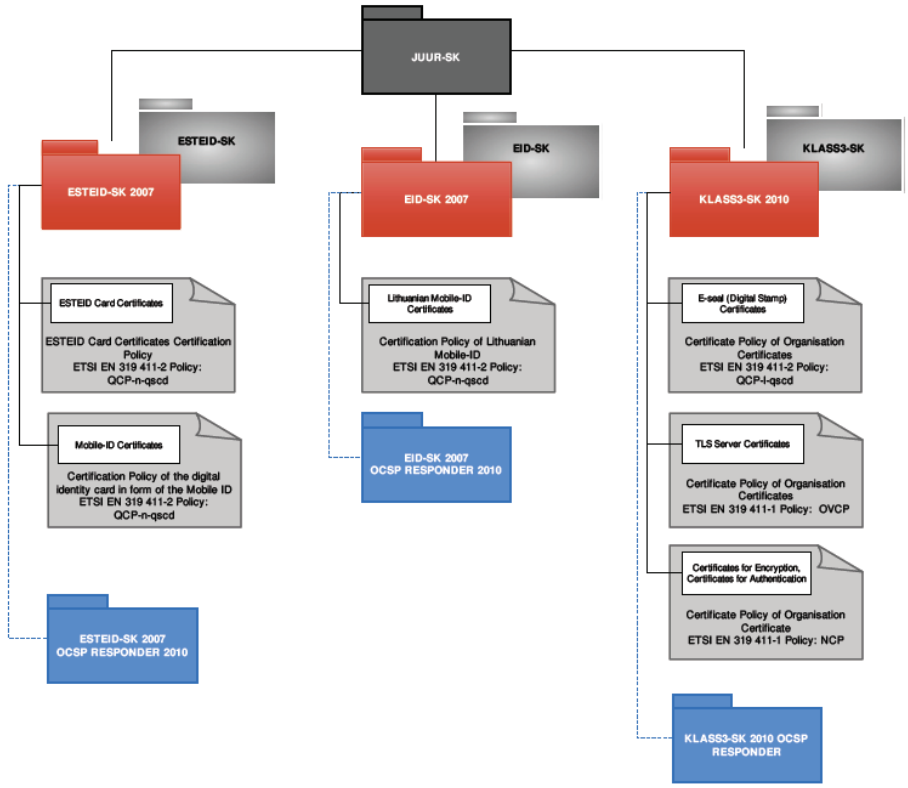
Pursuant to the IETF RFC 3647 [4] this document is divided into nine parts. To preserve the outline specified by RFC 3647 [4], section headings that do not apply have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them. Each first-level chapter includes reference to the corresponding chapter in ETSI EN 319 401 [2].

1.1 Overview

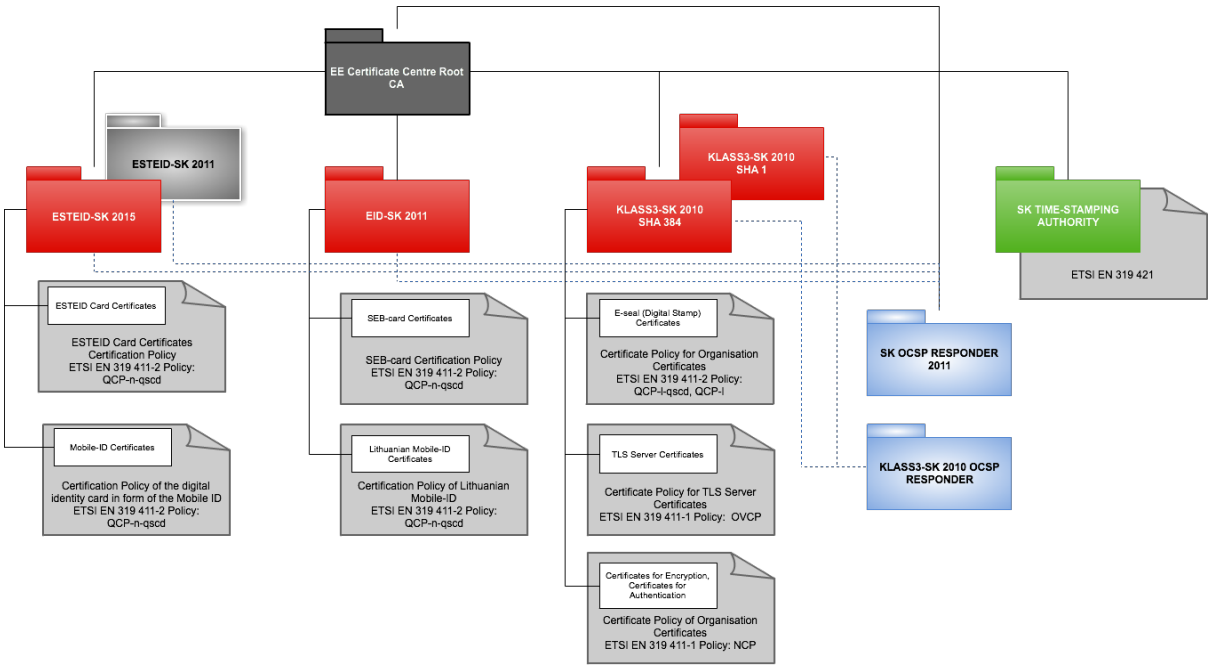
SK operates a Public Key infrastructure in order to provide Trust Services. SK is currently using two certificate chains; root certification authorities are Juur-SK and EE Certification Centre Root CA.

Their relations to Subordinate CA-s and Certification Policies are shown on the following figures:

1) Juur-SK, valid 2001-2016



2) EE Certification Centre Root CA chain, valid 2010-2030



The AS Sertifitseerimiskeskus Trust Services Practices Statement (SK PS) presents the criteria established by SK to provide electronic Trust Services, which enhance trust and confidence in electronic transactions. SK PS describes AS Sertifitseerimiskeskus (SK) practices of providing Qualified Trust Services in conformity with the eIDAS regulation [1], legal acts of Estonia, ETSI EN 319 401 General Policy Requirements for Trust Service Providers [2], and other related service-based standard requirements. Additionally SK follows CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [3].

This SK PS describes practices necessary for the achievement of the security level approved by the SK management. SK has achieved ISO/IEC 27001:2013 certification. The statement of applicability includes more detailed description of security measures.

In the event of conflict between the SK PS and the practice statements of specific services, the provisions of the practice statements of specific services shall prevail. In the event of conflict between the original document in English and the translated document in Estonian, the original document in English shall prevail.

1.2 Document Name and Identification

This document is called “AS Sertifitseerimiskeskus Trust Services Practice Statement.”

1.3 PKI Participants

1.3.1 Trust Service Provider

SK is Trust Service Provider (TSP). The roles of SK as TSP are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of SK are described in the clause 9.6.1 of this SK PS.

1.3.2 Registration Authorities

Registration Authority (RA) and its roles are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of RA are described in the clause 9.6.2 of this SK PS.

1.3.3 Subscribers

Subscriber is specified in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of Subscriber are described in the clause 9.6.3 of this SK PS.

1.3.4 Relying Parties

Relying Party is defined in the clause 1.6.1 in this SK PS.

Obligations and warranties of Relying Party are described in the clause 9.6.4 of this SK PS.

1.3.5 Other Participants

Specified in relevant service-based Policy and/or Practice Statement.

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

Specified in relevant service-based Policy and/or Practice Statement.

1.4.2 Prohibited Certificate Uses

Specified in relevant service-based Policy and/or Practice Statement.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This SK PS is administered by SK.

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu Ave 141, 11314 Tallinn
Tel +372 610 1880
Fax +372 610 1881
Email: info@sk.ee
http://www.sk.ee/en/

1.5.2 Contact Person

Quality Manager
Email: info@sk.ee

1.5.3 Person Determining SK PS Suitability for the Policy

Not applicable.

1.5.4 SK PS Approval Procedures

Amendments which do not change the meaning of the certification practice, such as corrections of misspellings, translation and updating of contact details, are documented in the versions and changes section of the present document and the fraction part of the document version number shall be enlarged.

In the case of substantial changes, the new Trust Service Practice Statement version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The amended SK PS along with the enforcement date, which cannot be earlier than 30 days after publication, is published electronically on SK's website.

SK has a right to publish before publication of SK PS the draft version of the document. The Subscriber has the chance to provide reasoned comments within 30 days of publication of draft version. The amended version of SK PS is published electronically on SK's website 30 days before its enforcement.

The SK PS is approved by the SK Chief Executive Officer and Service Managers. SK ensures that the practices are properly implemented by conducting regular internal audits and conformity assessments.

All amendments will be submitted to the Supervisory Body.

1.6 Definitions and Acronyms

1.6.1 Terminology

Certificate Revocation List	a list of invalid (revoked, suspended) certificates.
Qualified e-Signature (i.e. Qualified Electronic Signature)	means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures; Before 01.07.2016 term "digital signature" was used instead of Qualified e-Signature in Estonia and SK documents.
Directory Service	certificate publication service
eIDAS Regulation	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
e-Signature (i.e. Electronic Signature)	data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign.

Policy	a set of rules that indicates the applicability of a Trust Service Token to a particular community and/or class of application with common security requirements.
Practice Statement	a statement of the practices that a TSP employs in providing a Trust Service.
Registration Authority	entity that is responsible for identification and authentication of subjects of certificates. Additionally, an RA accepts certificate applications, checks the applications and/or forwards the applications to the CA.
Relying Party	a recipient of a Trust Service token who acts in reliance on that Trust Service Token. NOTE: Relying Parties include parties verifying a Digital Signature using a public key certificate.
Private key	the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key	the key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify digital 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.
Root CA	the top level Certification Authority whose certificate is distributed by application software suppliers and that issues subordinate SK CA certificates.
Sensitive Information	information which allows for simulation or replication of service, or also for the destruction or publication of the service private key. It also includes personal information.
SK CA	a Certification Authority of SK whose certificate is signed by the Root CA, or another subordinate CA
Subscriber	an entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
Subscriber Certificate	public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the Certification Authority, which issued it.
Supervisory Body	the authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS [1] in the territory of that member state.
Time-Stamping Unit	a set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
Trust Service	described in eIDAS [1] as an electronic service which is normally provided in return for remuneration and which consists of:

	- the creation, verification, and validation of Electronic Signatures, electronic seals or electronic time-stamps, electronically registered delivery services and certificates related to these services or - the creation, verification and validation of certificates for website authentication or - the preservation of Electronic Signatures, seals or certificates related to these services.
Trust Service Provider	an entity that provides one or more electronic Trust Services.
Trust Service Token	a physical or binary (logical) object generated or issued as a result of the use of a Trust Service (e.g. certificate).
Qualified Trust Service	means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.

1.6.2 Acronyms

CA	Certification Authority
CRL	Certificate Revocation List
DMZ	Demilitarised Zone
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Modules
RA	Registration Authority
SK	AS Sertifitseerimiskeskus
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

SK ensures that its repository is available 24 hours a day, 7 days a week with a minimum of 99,44% availability overall per year with a scheduled down-time that does not exceed 0,28% annually.

2.2 Publication of Information

SK publishes in its public information repository following information:

- Overview of its certification hierarchy (https://sk.ee/en/repository/);
- Trust Services Practices Statement (https://www.sk.ee/en/repository/sk-ps/)
- Certification Practice Statements (https://sk.ee/en/repository/CPS/);
- Time-Stamping Authority Practice Statement and Time-Stamping Principles (https://sk.ee/en/repository/tsp/);
- Audit results (https://sk.ee/en/repository/audit/);
- Conditions for insurance policy (https://sk.ee/en/repository/insurance/);
- Certification policies (https://sk.ee/en/repository/CP/);
- Certificates, including root certificates and CA certificates under which certificates for subscribers are issued (https://sk.ee/en/repository/certs/);
- Profiles (https://sk.ee/en/repository/profiles/);
- Conditions for use of certificates (https://sk.ee/en/repository/conditions-for-use-of-certificates/);
- Certificate Revocation Lists (https://sk.ee/en/repository/CRL/);
- LDAP directory (https://sk.ee/en/repository/ldap/);
- Principles of Client Data Protection (https://sk.ee/en/repository/data-protection/).

2.2.1 Publication and Notification Policies

This SK PS is published in SK's public information repository.

SK PS along with the enforcement dates is published no less than 30 days prior taking effect.

2.2.2 Items not Published in the Practice Statement

Refer to clause 9.3.1 of this SK PS.

2.3 Time or Frequency of Publication

Refer to clause 2.2.1 of SK PS.

Information on certification status is published in accordance with clauses 4.9.7 and 4.9.9 of this SK PS.

2.3.1 Directory Service

SK publishes information on certificates and their validity generally via LDAP directory service.

The purpose of LDAP directory service is to provide the Subscribers, Relying Parties and other persons access to the certificates register to make inquiries about certificates and their validity.

The directory service meets the following requirements:

- LDAP directory contains valid (i.e. not revoked and not expired) certificates;
- LDAP directory may not contain sensitive personal information in the meaning of the Personal Data Protection Act;
- LDAP directory is accessible in a public data communications network (ldap.sk.ee) 24 hours a day.

2.4 Access Controls on Repositories

Information published in SK's repository is public and not considered confidential information.

SK has implemented security measures in order to prevent unauthorized access to add, delete, or modify entries into its repository. Publishing into SK's repository is restricted to authorized employees of SK.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Specified in relevant service-based Policy and/or Practice Statement.

3.2 Initial Identity Validation

Specified in relevant service-based Policy and/or Practice Statement.

3.3 Identification and Authentication for Re-Key Requests

Specified in relevant service-based Policy and/or Practice Statement.

3.4 Identification and Authentication for Revocation Request

Specified in relevant service-based Policy and/or Practice Statement.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Specified in relevant service-based Policy and/or Practice Statement.

4.2 Certificate Application Processing

Specified in relevant service-based Policy and/or Practice Statement.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Specified in relevant service-based Policy and/or Practice Statement.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Specified in relevant service-based Policy and/or Practice Statement.

4.4 Certificate Acceptance

Specified in relevant service-based Policy and/or Practice Statement.

4.5 Key Pair and Certificate Usage

Specified in relevant service-based Policy and/or Practice Statement.

4.6 Certificate Renewal

Specified in relevant service-based Policy and/or Practice Statement.

4.7. Certificate Re-Key

Specified in relevant service-based Policy and/or Practice Statement.

4.8 Certificate Modification

Specified in relevant service-based Policy and/or Practice Statement.

4.9 Certificate Revocation and Suspension

Specified in relevant service-based Policy and/or Practice Statement.

4.10 Certificate Status Services

Specified in relevant service-based Policy and/or Practice Statement.

4.11 End of Subscription

Specified in relevant service-based Policy and/or Practice Statement.

4.12 Key Escrow and Recovery

Specified in relevant service-based Policy and/or Practice Statement.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

In the field of security management, SK guides itself by the generally recognised standards, e.g. ISO/IEC 27001 [5] , and other standards required by regulations and law.

The SK's security management policy documents include the security controls and operating procedures for the SK facilities, systems and information assets providing the services. SK carries out and revises risk assessment regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures.

The SK management establishes the security policy, which forms a basis for consistency and completeness of information security and management support.

The SK Chief Executive Officer approves policies and practices related to information security for the overall SK services. The SK management communicates information security policies and procedures to employees and relevant external parties who are impacted by it. In addition, the SK management sets out the SK approach to manage information security objectives for Trust Services, including auditable procedures for internal control.

SK has achieved ISO/IEC 27001: 2013 certification.

5.1 Physical Controls

SK is using physically separated space in rented server rooms specifically designed for data center operations. It is the responsibility of the owner of the premises to provide necessary environment for the equipment. A Service Level Agreement is arranged between SK and the owner of the premises to guarantee uninterrupted and secure operation.

5.1.1 Site Location and Construction

The SK services are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of Sensitive Information and systems whether covert or overt.

The protection provided is commensurate with the identified risks. The SK ensures that physical access to critical services is controlled and that physical risks to its assets are minimised.

5.1.2 Physical Access

The SK data centers are protected by a minimum of three tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Access to the highest tier requires the participation of two persons in Trusted Roles.

The employees of SK may gain access to the facilities concerned with Trust Services of SK only on the basis of an approved list. A log is kept for recording all entries to the data processing centre of SK.

The owner of the premises has no independent access to SK-s servers.

Any persons entering this physically secure area will not remain there without oversight by an authorised person.

5.1.3 Power and Air Conditioning

SK's secure facilities are equipped with:

- power systems to ensure continuous, uninterrupted access to electric power; and
- heating, ventilation, air conditioning systems to control the temperature and relative humidity.

5.1.4 Water Exposures

SK has taken reasonable precautions to minimise the impact of water exposure to the information systems.

5.1.5 Fire Prevention and Protection

SK has taken reasonable precautions to prevent and extinguish fires or other damaging exposure toflame or smoke. The fire prevention and protection measures of the SK have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

Portable media, appliances and software may be removed from the premises of the SK pursuant to the established procedure. Data media containing sensitive information may be stored only in a special fireproof safe designed for storing data media.

5.1.7 Waste Disposal

Media containing Sensitive Information are securely disposed of when no longer required. Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal. Any media with Sensitive Information removed from use (removable media, hard disks etc.) are sanitised when decommissioned or recycled for other use, to prevent data leaks.

5.1.8 Off-Site Backup

SK performs routine backups of critical system data, audit log data, and other Sensitive Information. The SK has dual data centres to ensure availability requirements. Databases in dual data centres are synchronised in real time. In addition, routine backups are performed. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage.

5.2 Procedural Controls

5.2.1 Trusted Roles

The employees of SK have job descriptions that specify the following Trusted Roles critical for security:

- Security Officer: he/she is responsible for the administration of and the implementation of the security practices;
- System Administrators: they are responsible for the installation, configuration and maintenance of the information system of the SK, including performing the system backup and recovery.
- System Auditor or Evaluator: he/she is responsible for periodically reviewing procedures; for that he/she has access to monitor the document archives and information system audit logs.

SK has separated System Administrators with internal regulation into two roles called A- and B-type. The assignment is made person by person with a decree of the CEO. See clause 5.2.2 for details.

SK ensures that personnel have achieved trusted status, and departmental approval is given before such personnel are:

- Issued access devices and granted access to the required facilities; or
- Issued electronic credentials to access and perform specific functions on SK or other IT systems.

Security operations are managed by SK personnel in Trusted Roles, but may actually be performed by a non-specialist, operational personnel (under supervision), as defined within the roles and responsibility documents.

The role of RA Officer is also considered security critical as he/she is responsible for identification and authentication of subjects of certificates and may be responsible for registration, certificate suspension, termination of suspension and revocation procedures.

5.2.2 Number of Persons Required per Task

The SK has established, maintains and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The following activities require a minimum of two System Administrators in Trusted Roles, specifically one in A-type and other in B-type:

- generation of certification keys;
- backup of the certification keys;
- restoration of the certification keys;
- management of HSM-s and CA core systems located in Secure Zone;
- physical visit to data centres.

5.2.3 Identification and Authentication for Each Role

All Trusted Roles are performed by persons assigned into this role by SK management and accepted by this person to fulfill this role.

The SK has implemented an access control system, which identifies authorities and registers all the SK information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use.

User accounts are locked as soon as possible when the role change dictates. Access rules are audited annually.

5.2.4 Roles Requiring Separation of Duties

The Trusted Roles of the Security Officer, System Auditor and System Administrators are completely separate and are staffed by different persons. A single person cannot be simultaneously A- and B-type of System Administrator.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The employees of the SK have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

The employment contracts signed by the employees of the SK provide for the following obligations:

- to maintain the secrecy of confidential information that has come to their knowledge in the course of their performance,
- to prevent them from holding business interests in a company, which may affect their judgment in the supply of the service and
- to ensure that they have not been punished for a wilful crime.

All personnel in Trusted Roles and RA Officers are free from any interests that may affect their impartiality regarding SK operations.

5.3.2 Background Check Procedures

For all personnel seeking to become personnel in Trusted Roles, the verification of identity is performed through the personal (physical) presence of such personnel before the personnel in Trusted Roles can perform the SK operational or security functions. Furthermore, officially recognised documents of identification e.g., ID card or passports are checked. Suitability is further confirmed through background checking procedures.

Background verification checks are carried out in accordance with relevant laws, regulations and principles of ethics. The checks are proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. These checks are conducted on all candidates for employment and on contracted partners directly performing the Trust Service providing operations with access to production data.

Backround checks about criminal record are refreshed at least every 3 years.

5.3.3 Training Requirements

The employees of SK have received adequate training and have all the necessary experience for

carrying out the duties specified in the employment contract and job description before they perform any operational or security functions.

SK ensures that all personnel performing managerial duties with respect to the operation of the SK receive comprehensive awareness training in:

- security principles and rules in SK;
- SK internal regulations and processes;
- duties they are expected to perform.

5.3.4 Retraining Frequency and Requirements

The requirements of this SK PS 5.3.3 will be kept current to accommodate changes in the SK system. Refresher training will be conducted as required, and the SK is testing security awareness of all personnel at least once a year.

5.3.5 Job Rotation Frequency and Sequence

No rotation used.

5.3.6 Sanctions for Unauthorized Actions

The SK establishes, maintains and enforces employment policies (as part of the SK Security Policy) for the discipline of personnel following unauthorised actions. Disciplinary actions include measures up to and including termination and will be commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Independent Contractor Requirements

The SK does not use independent contractors in Trusted Roles.

5.3.8 Documentation Supplied to Personnel

The SK gives its personnel (including persons in Trusted Roles and RA Officers) the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

SK ensures that all relevant information concerning the operation of the Trust Services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of Trust Service Tokens and the audit log of the Trust Service operation.

SK's information systems leave an audit log of:

- all events relating to the life cycle of keys and certificates managed by SK, including CA and TSU keys and certificates and Subscriber key pairs;
- all significant security events, including changes in the security policy settings, system start-up and shutdown, system crashes and hardware failures, changes in firewall configuration and rulebase and PKI system access attempts, the activities of system users with superuser rights;
- all events relating to the synchronisation of the clock to UTC, the detection of loss of synchronisation;
- all events related to registration including requests for certificate re-key and renewal;
- all registration information, including identity proofing:
    - type of document(s) presented by the applicant to support registration;
    - record of unique identification data, numbers, or a combination thereof of identification documents;
    - storage location of copies of applications and identification documents;
    - identity of the entity accepting the application;
    - method used to validate identification documents;
    - name of receiving TSP/submitting Registration Authority;
- all requests and reports relating to suspension and termination of suspension;
- all requests and reports relating to revocation, as well as the resulting actions.

5.4.2 Frequency of Processing Log

System administrators are responsible for regular reviewing of system logs and reporting of possible incidents.

Product managers are responsible for reviewing their applications logs from central log system and creating automated searches for product failure discovery and event correlation.

Identifying important event types and extracting fields is responsibility of system administrators, product managers and integrators according to their work task.

Business development managers are responsible for at least weekly review of reports generated by log system about their services.

5.4.3 Retention Period for Audit Log

Audit logs are retained on-site for no less than 7 years until 31.12.2015. From 01.01.2016 audit logs are retained on-site no less than 10 years.

Physical or digital archive records about certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained at least for 10 years after validity of relevant certificate.

In case of termination SK audit logs and archive records are retained and accessible until abovementioned term for retention accordance with clause 5.8 of this SK PS.

5.4.4 Protection of Audit Log

The SK uses information security solutions confirming with the standards, which ensure non-recording of private keys, activation codes, access codes (e.g. PIN) or other security critical information in the audit log.

All logs are stored locally and are sent to the central log server. The central log servers implement the logging policy – retention and archiving.

Application logs have a cryptographic protection.

Internal development process defines security requirements for logging process and logs, including protection of logs.

Non-electronic audit information is protected from unauthorised viewing, modification and destruction through organisational means.

Access to the audit log is limited on the role/privilege basis.

5.4.5 Audit Log Backup Procedures

SK performs regular backups of critical system data, audit log data, and other Sensitive Information. Audit log data backup is the part of general back-up system. SK has defined backup strategy and policies in internal regulations.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Non-electronically generated audit data is recorded by the SK persons in Trusted Roles.

5.4.7 Notification to Event-Causing Subject

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised. These assessments are based on real-time

automated logging data and are performed on a daily, monthly, and annual basis.

5.5 Records Archival

5.5.1 Types of Records Archived

Specified in relevant service-based Policy and/or Practice Statement.

5.5.2 Retention Period for Archive

The retention period for archive is described in clause 5.4.3 of this SK PS.

5.5.3 Protection of Archive

The archive is located in a separate room and is protected by access control systems.

The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period required.

5.5.4 Archive Backup Procedures

The archive is not backed up.

5.5.5 Requirements for Time-Stamping of Records

Database entries contain accurate time and date information. The time-stamps are not cryptography-based.

5.5.6 Archive Collection System (Internal or External)

The SK uses an internal archive collection system.

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

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorised personnel in Trusted Roles are allowed access to the archive.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

The integrity of the information is verified during recovery tests. The archive systems with built-in integrity controls are in use.

5.6 Key Changeover

Specified in relevant service-based Policy and/or Practice Statement.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

SK has implemented a business continuity management framework, which covers procedures of risk assessment, incident handling (includes a response to incidents and disasters), recovery and recovery exercises.

SK carries out an annual risk assessment of SK's Trust Services to prevent possible danger to the availability of SK's operations and to minimise the risk of losing control of the Trust Services. The list of situations considered as emergency situations is determined by the risk assessment. The result of the risk assessment includes the requirements for recovery plans and recovery testing scenarios. The recovery plans and testing scenarios include at least the following threats:

- for SK CA and SK TSA, the private key used for the provisioning of the service is compromised or there is a serious suspicion thereof;
- for SK TSA, the loss of synchronisation of a time-stamping service clock.

The procedures for the handling of information security incidents, emergency situations and critical vulnerabilities are documented in the SK Internal Crisis Management Regulation. The objective of that regulation is the immediate response and recovery of availability and the continuous protection of SK services.

Recovery plans are tested annually.

In the event of an emergency, SK will inform all the Subscribers and Relying Parties immediately (or at least within 24 hours of the crisis committee's decision) of the emergency situation and proposed solution through public information communication channels.

SK will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies as national CERT or Data Inspectorate, of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The event of the corruption of computer resources, software and data is handled according to the SK internal Crisis Management Regulation.

5.7.3 Entity Private Key Compromise Procedures

SK private key compromise is handled according to the SK Internal Crisis Management Regulation.

5.7.4 Business Continuity Capabilities After a Disaster

In order to ensure the business continuity capabilities after a disaster SK organises periodically crisis management trainings. The SK Internal Crisis Management Regulation defines how crisis management and communication take place in emergency situations.

There is an internal agreement about priorities for systems and services recovery after the emergency situation or/and service interruption. SK maintains necessary back-up copies and archives to able to restore data after the emergency situation. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage.

SK has dual data centres to ensure the availability of services. SK office and data centres are independent of each other. In case of the emergency in data centres guidance's, source codes and other necessary materials are available from SK Office. In case of the emergency situation in SK office services in data centres will continue to work.

5.8 CA Termination

The Trust Service is terminated:

- with a decision of the SK Board;
- with a decision of the authority exercising supervision over the supply of the service;
- with a judicial decision;
- upon the liquidation or termination of the operations of SK.

SK ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation of SK's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of Trust Service Tokens.

Before SK terminates a Trust Service the following procedures will be executed:

- SK informs the following of the termination: all Subscribers and other entities with which the SK has agreements or other forms of established relations. In addition, this information will be made available to other Relying Parties;
- SK makes the best effort for doing arrangements with other Trust Service Provider to transfer

the provision of services for its existing customers;
- SK destroys the CA and TSU private keys, including backup copies or keys withdrawn from use in such a manner that the private keys cannot be retrieved;
- SK reinitialises or destroys any hardware appliances related to this service depending on the security regulations;
- SK terminates authorisation of all subcontractors to act on behalf of SK in carrying out any functions relating to the process of issuing Trust Service Tokens for this service;
- SK maintains the documentation related to they supply of the Trust Service and information needed to verify the Trust Service Tokens if SK is not terminated according to the clause 5.4 and 5.5. In case SK will be terminated, SK hands over the aforementioned documentation related to the supply of the service and information needed to verify the Trust Service Tokens to the Supervisory Body pursuant to the established procedure.

In case of compromise the SK will additionally:
- Indicate that Trust Service Tokens and validity information issued using this CA or TSU key may no longer be valid;
- Revoke any CA and TSU certificate that has been issued for SK when SK is informed of the compromise of another CA or TSA.

In case of algorithm compromise SK will additionally:
- Schedule a revocation of any affected Trust Service Token.

The notice of termination of SK's Trust Service will be published in the public media.

SK does not assume liability for any loss or damage sustained by the user of the service as a result of such termination provided that SK has given the notice of termination through public information communication channels at least one month in advance.

SK has an arrangement with an insurer to cover the costs to fulfil these minimum requirements in case the TSP goes bankrupt, or for other reasons, is unable to cover the costs by itself.

The requirements are applicable also in case of RA termination. SK takes over the documentation and information related to the supply of the Trust Service and provides evidence of the operation for a time period defined in relevant service-based Policy and/or Practice Statement.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

SK uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms.

6.1.1 Key Pair Generation

The signing keys of the SK Trust Services are created in accordance with the internal regulations of the SK: Procedure for Creating the SK Root Key and Procedure for Creating Keys for Intermediate Certification Authorities. For the key ceremony of SK CA key pair generation for all CA's, whether root or intermediate CAs, the commission is appointed by SK Chief Executive Officer with internal regulation. The commission has to include the external auditor independent of SK. The creation of the SK's Trust Service keys is observed by a commission, which after the creation of the keys draws up an appropriate deed containing the public key of the created pair of keys and the hash thereof. The Trust Service key pair generation and the private key storage occur in the HSM, which is used for providing keys that at least meet the requirements established in the security standard FIPS PUB 140-2 Level 3. The HSM protects the key from external compromise and operates in a physically secure environment.

SK has documented procedure for conducting SK CA key pair generation for all CA's, whether root or intermediate CAs, including CAs that issue end user certificates. SK produces a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. Report is signed by the commission members, including external auditor. The procedures for key ceremony are documented in SK internal Regulation of the Key Procedures.

The Subscriber Private Key generation is specified in relevant service-based Policy and/or Practice Statement.

6.1.2 Private Key Delivery to Subscriber

Specified in relevant service-based Policy and/or Practice Statement.

6.1.3 Public Key Delivery to Certificate Issuer

Specified in relevant service-based Policy and/or Practice Statement.

6.1.4 CA Public Key Delivery to Relying Parties

All SK Trust Services public keys are distributed in the form of X.509 certificates issued by the SK CA. The primary distribution mechanism for the SK Trust Service certificates is via the SK repository at https://www.sk.ee/en/repository/. The SK takes obligation to provide the SK Trust Service certificates to Trusted List of Estonia. The SK makes every effort to include the certificates in web browsers' vendor-supplied trust stores.

6.1.5 Key Sizes

Specified in relevant service-based Policy and/or Practice Statement.

6.1.6 Public Key Parameters Generation and Quality Checking

Specified in relevant service-based Policy and/or Practice Statement.

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

Specified in relevant service-based Policy and/or Practice Statement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The HSM used by the SK is certified with FIPS 140-2, level 3 standard and is the FIPS mode activated.

SK checks and verifies that HSM is not tampered after its receive and installation. This is documented in a HSM life-cycle protocol.

Cryptographic module standards and controls for cryptographic devices which carry the Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

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

The access to the SK CA keys is divided into two parts that are secured by different persons in Trusted Roles. For activation of the signing key of the SK the presence of at least two authorized persons is required in accordance with clause 5.2.2 of this PS.

6.2.3 Private Key Escrow

The SK CA private keys are held in secure cryptographic devices certified with the FIPS 140-2 level 3 standard. The activation and use of the private key requires multi-person control as explained in clause 6.2.2 in this SK PS.

Subscriber Private Keys escrow is specified in relevant service-based Policy and/or Practice Statement.

6.2.4 Private Key Backup

To meet the availability requirements, a backup copy are made of the SK CA private keys by securely cloning them into the backup HSM. Key access is divided into two parts that are secured by different persons. A security envelope is used for storing the certification key of the SK and the opening of this envelope can be established. The certification keys of the SK can be used only when they are activated.

For activation of the certification key of the SK the presence of at least two authorised persons is required as explained in clause 6.2.2 in this SK PS.

The Subscriber's Private Keys backup is specified in relevant service-based Policy and/or Practice Statement.

6.2.5 Private Key Archival

SK will not archive the SK CA private keys after it has expired. All copies of the SK CA private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible.

The Subscriber's Private Keys archival is specified in relevant service-based Policy and/or Practice Statement.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All SK CA keys must be generated by and in the a cryptographic module. The SK generates CA key pairs in the HSM in which the keys will be used.

6.2.7 Private Key Storage on Cryptographic Module

The SK CA Private Keys held in the HSM are stored in encrypted form.

The Subscriber's Private Keys storage is specified in relevant service-based Policy and/or Practice Statement.

6.2.8 Method of Activating Private Key

The SK CA private keys are activated according to the specifications of the cryptographic module manufacturer. For activation of the certification key of the SK the presence of at least two authorised persons is required as explained in clause 6.2.2 of this SK PS.

Method of activating Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.9 Method of Deactivating Private Key

The SK CA private keys are deactivated when an attempt is made to open the security module used for storage of the keys, when the configuration is changed, the power supply is disconnected or transferred or in other events endangering the security.

Method of deactivating Subscriber Private Key is specified in relevant service-based Policy and/or Practice Statement.

6.2.10 Method of Destroying Private Key

Method of the destroying SK CA private keys and internal control mechanisms depend from the options available to specific secure cryptographic module.

6.2.11 Cryptographic Module Rating

Refer to the clause 6.2.1 of this SK PS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All certificates issued (including all expired or revoked certificates) are retained and archived as part of the SK routine backup procedures. The retention period is indefinite.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a certificate ends upon revocation. The operational period for key pairs is the same as the operational period for the certificates, except that they may continue to be used for signature verification.

In addition, the SK stops issuing new certificates at an appropriate date prior to the expiration of the CA's certificate such that no Subscriber certificate expires after the expiration of the CA certificate.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by the SK management.

For Subscriber certificates, the validity period is defined in relevant service-based Policy and/or Practice Statement.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The SK CA private key activation data generation and installation is performed according to the user manual of HSM.

The Subscriber's Private Key PINs generation and installation is specified in relevant service-based Policy and/or Practice Statement.

6.4.2 Activation Data Protection

HSM is kept in secure storage and access to it have only authorized personnel in Trusted Roles.

The Subscriber's Private Key PINs protection is specified in relevant service-based Policy and/or Practice Statement.

6.4.3 Other Aspects of Activation Data

Specified in relevant service-based Policy and/or Practice Statement.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The SK ensures that the certification system components are secure and correctly operated, with an acceptable risk of failure.

The SK certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All critical software components of the SK are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorised software.

All media containing production environment software and data, audit, archive, or backup information are stored within the SK with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media containing Sensitive Information are securely disposed of when no longer required. All removable media are used only for the intended period of the user (either by time or by number of uses).

SK has no defined capacity management process. The performance of SK services and IT systems is monitored by Business Service Managers and changes are done when necessary according to internal change management procedure.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

The SK security operations include: operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backups, network management, active monitoring of audit logs event analysis and follow-up, media handling and security, data and software exchange.

SK's personnel are authenticated before using critical applications related to the services.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

6.5.2 Computer Security Rating

SK uses standard computer systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the SK; or an analysis is carried out on behalf of the SK to ensure that security is built into the Information Technology's systems.

The software will be approved by the Security Officer and will originate from a trusted source. New versions of software are tested in a testing environment of the appropriate service and their deployment is conducted according to documented change management procedures.

6.6.2 Security Management Controls

Measures are implemented In the information system of the SK, including all workstations for guaranteeing the integrity of software and configurations, as well as for detecting fraudulent software and restricting its spread.
Only the software directly used for performing the tasks is used in the information system.

6.6.3 Life Cycle Security Controls

The SK policies and assets for information security are reviewed at planned intervals, or should significant changes occur, they are reviewed to ensure their continuing suitability, adequacy and

effectiveness.

The configurations of the SK systems are regularly checked for changes that violate the SK security policies. A review of configurations of the issuing systems, security support systems, and front-end/internal-support systems occurs at least on a weekly basis. The Security Officer approves changes that have an impact on the level of security provided.
The SK has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

The SK manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment. A responsible person has been appointed for all important information security assets. All SK policies and assets related to information security will be reviewed internally at planned intervals, or should significant changes occur, they will be reviewed to ensure their continuing suitability, adequacy and effectiveness.

6.7 Network Security Controls

The SK network is divided into zones by security requirements. Communication between the zones is restricted. Only the protocols needed for the SK services are allowed through the firewalls.

The front-end systems are in a DMZ protected by a firewall and TLS offload servers. Actual security-critical services and corresponding HSMs run in a secure zone that is separated by dedicated firewall and has no direct Internet access.

The root CA is in a high security zone and is air-gapped from all the other networks. The SK systems are configured with only these accounts, applications, services, protocols, and ports that are used in the Trust Service operations.

The SK ensures that only personnel in Trusted Roles have access to a secure zone and a high security zone.

The cabling and active equipment along with their configuration in the SK internal network are protected by physical and organisational measures.

The SK operates multiple data centres in separate sites for redundancy. Communication between sites is cryptographically secured.

All data centres are considered to be in a common internal secure network carrying the DMZ and secure zone. The transfer of Sensitive Information outside the SK internal network is encrypted.

The security of the SK internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

The SK performes a vulnerability scan once in a quarter on public and private IP addresses identified by SK.

The SK undergoes a penetration test on the certification systems annually at the set up and after the infrastructure or application upgrades or modifications determined significant by the SK.

The SK records evidence that each vulnerability scan and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8 Time-Stamping

SK is providing time-stamping service as qualifed Trust Service and is specified in AS Sertifitseerimiskeskus Time-Stamping Authority Practice Statement [6].

The SK does not use time-stamping in relation to certification service. Database entries contain accurate time and date information. The time information is not cryptographic-based. The maximum allowed time variance in all parts of the certification system is 1 second. This is guaranteed by an internal Reference Clock service, according to which the chronologies of all parts of the certification system are synchronised. The Reference Clock uses GPS (Global Positioning System) as a primary time source which determines preciseness of the time in the SK's system.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.2 CRL Profile

Specified in relevant service-based Policy and/or Practice Statement.

7.3 OCSP Profile

Specified in relevant service-based Policy and/or Practice Statement.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The conformity of information system, policies and practices, facilities, personnel, and assets of SK are assessed by an conformity assessment body pursuant to the eIDAS regulation [1], the corresponding legislation and standards or whenever a major change is made to Trust Service operations.

Twice a year SK's internal auditor carries out an internal audit.

8.2 Identity/Qualifications of Assessor

Conformity assessment body is accredited in accordance with Regulation EC no 765/2008 as competent to carry out conformity assessment of qualifed Trust Service Provider and qualified Trust Services it provides.

8.3 Assessor's Relationship to Assessed Entity

The auditor of the conformity assessment body shall be independent from the SK and the SK assessed systems.

The internal auditor shall not audit his/her own areas of responsibility.

8.4 Topics Covered by Assessment

The conformity assessment covers the conformity of information system, policies and practices, facilities, personnel, and assets with eIDAS regulation [1], respective legislation and standards. Conformity assessment body audit the parts of the SK information system used to provide Trust Services.

The areas of activity subject to internal auditing are the following:

- quality of service;
- security of service;
- security of operations and procedures;
- protection of the data of Subscribers and security policy, performance of work procedures and contractual obligations, as well as compliance with the SK PS and service-based Policies and Practice statements.

The Conformity Assessment Body and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing SK Trust Services (e.g. including RA-s).

8.5 Actions Taken as a Result of Deficiency

In the event of a result showing deficiency in the assessment, the Supervisory Body requires the SK to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body.

The SK makes efforts to stay compliant and fulfil all requirements of the deficiency on time. The SK management is responsible to implement a corrective action plan. The SK evaluates the significances of deficiencies and prioritizes appropriate actions to to be taken at least during the time limit declared by Supervisory Body or reasonable period of time.

Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

8.6 Communication of Results

Audit conclusions or certificate(s) for trust service(s), which are based on audit results of the conformity assessment conducted pursuant to the eIDAS regulation, corresponding legislation and standards, are published on SK's website https://www.sk.ee/en/repository/ .

In addition the SK submits the resulting conformity assessment report to the Supervisory Body within at period of three working days of receiving it. SK submits the audit conclusions or certificate(s) for trust service(s) to maintainers of the Browsers Root Programs in which SK is participating and other interested parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.2 Certificate Access Fees

SK's public directory service with valid and activated certificates is available via the LDAP at ldap.sk.ee.

9.1.3 Revocation or Status Information Access Fees

Specified in relevant service-based Policy and/or Practice Statement.

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy

SK handles refund requests case-by-case.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

In accordance with the relevant legislation, SK publishes the terms of the compulsory insurance policy on its website https://www.sk.ee/en/repository/insurance/.

9.2.2 Other Assets

According to relevant agreements SK may give some additional warranties.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of this SK PS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to SK because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from SK about him/herself according to legal acts.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential or intended for internal use is public information.
Information considered public in SK is listed in clause 2.2 of this SK PS.

Additionally, non-personalised statistical data about SK's services is also considered public information. SK may publish non-personalised statistical data about its services.

9.3.3 Responsibility to Protect Confidential Information

SK secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

9.4 Privacy of Personal Information

9.4.1 Personal Data Protection Principles

SK's principles of personal data protection are described in the principles of client data protection. The principles are published on SK's website https://sk.ee/en/repository/data-protection/.

By adhering to the above mentioned principles, SK guarantees compliance with the Personal Data Protection Act [7] as well as non-disclosure of confidential information and adequacy of subscriber's information storage.

9.4.2 Personal Information Processed by SK

The scope of personal information processed by SK is described in the Principles of Client Data Protection [8].

9.4.3 Responsibility to Protect Private Information

SK ensures protection of personal information by implementing security controls as described in chapter 5 of this SK PS.

9.4.4 Notice and Consent to Use Private Information

The exact terms under which the subscriber grants SK his/her notice and consent to use his/her personal information are described in the Principles of Client Data Protection [8].

9.4.5 Disclosure Pursuant to Judicial or Administrative Process

The circumstances under which SK may disclose the subscriber's personal information to third parties are described in the Principles of Client Data Protection [8].

9.4.6 Other Information Disclosure Circumstances

The circumstances under which SK may disclose the subscriber's personal information to third parties are described in the Principles of Client Data Protection [8].

9.5 Intellectual Property Rights

SK obtains intellectual property rights to this SK PS.

9.6 Representations and Warranties

9.6.1 Trust Service Provider Representations and Warranties

SK is party to the mutual agreements and obligations between the TSP, Subscribers, and Relying Parties. This SK PS and service-based Practice Statements are integral parts of these agreements.

SK shall:

- provide its services consistent with the requirements and the procedures defined in this SK PS and service-based policies and practice statements;
- comply with eIDAS regulation [1] and related legal acts defined in this SK PS and service-based policies and practice statements;
- publish its SK PS and service-based policies and practice statements and guarantee their availability in a public data communications network;
- publish and meet its claims in terms and conditions for subscribers and guarantee their availability and access in a public data communications network;
- maintain confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- keep account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- inform the Supervisory Body of any changes to a public key used for the provision Trust Services;
- without undue delay but in any event within 24 hours after having become aware of it, notify the Supervisory Body and, where applicable, other relevant bodies as national CERT or Data Inspectorate, of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein;
- where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach of security or loss of integrity without undue delay;
- preserve all the documentation, records and logs related to Trust Services according to the clauses 5.4 and 5.5;
- ensure an conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- has the financial stability and resources required to operate in conformity with this SK PS;
- publish the terms of the compulsory insurance policy and the conclusion of conformity assessment body or certificate in a public data communications network.

An employee of SK may not have been punished for an intentional crime.

9.6.2 RA Representations and Warranties

RA shall:

- provide its services consistent with the requirements and the procedures defined in the contract between SK and RA, in this SK PS and service-based Policies and Practice statements;
- provide its employees with necessary training for supply of high-quality service;
- without undue delay after having become aware of it, will notify SK of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

An employee of RA may not have been punished for an intentional crime.

9.6.3 Subscriber Representations and Warranties

The Subscriber shall:

- observe the requirements provided by SK in this SK PS and the respective service-based policies and/or practice statements;
- supply true and adequate information in the application for the services, and in the event of a change in the data submitted, he/she shall notify the correct data in accordance with the rules established in the service-based policies and practice statements;
- be aware of the fact that SK may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- be solely responsible for the maintenance of his/her private key and Trust Service Tokens. The Subscriber shall use his/her private key and Trust Service Tokens in accordance with this SK PS, service-based practice statements and service terms and conditions.

9.6.4 Relying Party Representations and Warranties

A Relying Party shall:

- study the risks and liabilities related to the acceptance of Trust Service Tokens. The risks and liabilities have been set out in this SK PS, in the appropriate service-based policies and practice statements and in the service terms and conditions.
- verify the validity of Trust Service Tokens on the basis of validation services offered by SK using
    - published information on SK's website https://www.sk.ee/en/repository/ or
    - applicable validation service or
    - appropriate cryptographic information.

9.6.5 Representations and Warranties of Other Participants

Specified in relevant service-based Policy and/or Practice Statement.

9.7 Disclaimers of Warranties

SK:

- is liable for the performance of all its obligations specified in clause 9.6.1 to the extent prescribed by the legislation of the Republic of Estonia;
- has compulsory insurance contracts, which cover all SK Trust Services to ensure compensation for damage which is caused as a result of violation of the obligations of SK.

SK is not liable for:

- the secrecy of the private keys of the Subscribers, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service Token validation checks;
- the non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the data protection supervision authority, Trusted List or any other public authority;
- non-fulfilment of the obligations arising from the SK PS if such non-fulfilment is occasioned by Force Majeure.

9.8 Limitations of Liability

The upper limit of the liability for any claim is established in the referred policy available at https://sk.ee/en/repository/insurance/.

9.9 Indemnities

Indemnities between the Subscriber and SK are regulated in service based Terms and Conditions.

9.10 Term and Termination

9.10.1 Term

Refer to clause 2.2.1 of this SK PS.

9.10.2 Termination

This SK PS and/or service-based Practice Statements remain in force until they are replaced by a new version or when they are terminated due to Trust Service or SK's termination.

Upon SK's termination, SK is obliged to ensure the protection of personal and confidential information.

9.10.3 Effect of Termination and Survival

SK communicates the conditions and effect of this SK PS's and/or service-based Practice Statements 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 public information of repository, SK archives for determined period and logs survive termination. All Subscriber agreements remain effective until the certificate is revoked or expired, even if this SK PS and/or service-based Practice Statements terminate.

Termination of this SK PS and/or service-based Practice Statements cannot be done before termination actions described in clause 5.8 of this SK PS.

9.11 Individual Notices and Communications with Participants

In general, SK's website www.sk.ee will be used to make any type of notification and communication.

Other means of individual notices and communication is specified in relevant service-based Policy and/or Practice Statement.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to clause 1.5.4 of this SK PS.

9.12.2 Notification Mechanism and Period

Refer to clause 2.2.1 of this SK PS.

9.12.3 Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

All disputes between the parties will be settled by negotiations. If the parties fail to reach and amicable agreement, the dispute will be resolved at the court of the location of SK.

The other parties will be informed of any claim or compliant not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

The Subscriber or other party can submit their claim or complaint on the following email: info@sk.ee.

9.14 Governing Law

This SK PS is governed by the jurisdictions of the European Union and the Republic of Estonia.

9.15 Compliance with Applicable Law

SK ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- 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 [1];
- Personal Data Protection Act [7];
- related European Standards:
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [2];
  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [9];
  - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [9];
- CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [3].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SK contractually obligates each RA and other participants to comply with this SK PS 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 SK PS, 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 SK PS 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 SK PS is held invalid or unenforceable by a competent court or tribunal, the remainder of the SK PS remains valid and enforceable. Each provision of this SK PS 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 (Attorneys' 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 SK PS does not waive SK's right to enforce the same provision later or right to enforce any other provision of this SK PS. To be effective, waivers must be in writing and signed by SK.

9.16.5 Force Majeure

The subject of Force Majeure and other parties are responsible for any consequences caused by circumstances beyond his reasonable control, including but without limitation to war (whether declared or not), acts of government or the European Union, export or import prohibitions, breakdown or general unavailability of transport, general shortages of energy, fire, explosions, accidents, strikes or other concerted actions of workmen, lockouts, sabotage, civil commotion and riots.

Communication and performance in the case of Force Majeure are regulated between the parties with the agreements.

Non-fulfilment of the obligations arising from the SK PS and/or relevant service-related Policies and/or Practice Statements is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this SK PS and/or relevant service-related Policies and/or Practice Statements caused by Force Majeure.

9.17 Other Provisions

Not applicable.

REFERENCES

[1] eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
[2] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[3] CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.3.pdf;
[4] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, https://www.ietf.org/rfc/rfc3647.txt;
[5] ISO/IEC 27001: 2013 Information technology - Security techniques -Information security management systems – Requirements;
[6] AS Sertifitseerimiskeskus Time-Stamping Authority Practice Statement, published: https://www.sk.ee/en/repository/tsp/;
[7] Personal Data Protection Act, RT I 06.01.2016, 10;
[8] Principles of Client Data Protection, published: https://www.sk.ee/en/repository/data-protection/;
[9] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
[10] ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.