AS Sertifitseerimiskeskus
Trust Services Practice Statement

Version 1.0
Valid from 01.10.2014

Version Information		
Date	**Version**	**Modifications**
01.10.2014	1.0	First public version

Introduction

AS Sertifitseerimiskeskus, which is a limited liability company, was founded on March 27, 2001. The company has three owners: AS Swedbank, AS SEB Pank, each owning 25 percent, and AS Eesti Telekom owning 50 percent of the shares. AS Sertifitseerimiskeskus was registered as a certification and time-stamping services provider on November 2nd, 2001. The principal activities of AS Sertifitseerimiskeskus include offering services associated with certification, time-stamping and other related Trust Services required for the implementation of Digital Signatures and stamps. These services guarantee secure and verified electronic communication with both public institutions and businesses in everyday life.

The AS Sertifitseerimiskeskus Trust Services Practice Statement (SK PS) presents the criteria established by SK to provide electronic Trust Services, which enhance trust and confidence in electronic transactions. The SK PS may be revised regularly as appropriate, in accordance with the legal acts of the Republic of Estonia, the European Union and international standards. This SK PS outlines the contents of the ETSI EN General Policy Requirements for Trust Service Providers (ETSI EN 319 401).

Contact information:

For information about SK services please contact:

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Tel +372 610 1880
Fax +372 610 1881
E-mail: info@sk.ee
Homepage: http://www.sk.ee/en/

Table of Contents

1. Scope

This AS Sertifitseerimiskeskus Trust Services Practice Statement (hereafter SK PS) describes AS Sertifitseerimiskeskus (SK) practices of providing Trust Services, including services needed for creating legally binding Digital Signatures in conformity with the Digital Signatures Act of the Republic of Estonia, the EU Directive 1999/93/EC and the ETSI EN General Policy Requirements for Trust Service Providers (ETSI EN 319 401). This SK PS is registered in the Estonian Register of Certificates (*Sertifitseerimise Register*).

This document is an overall Practice Statement for all SK Trust Services. Each service also has its own specific Policy and Practice statements.

This SK PS describes practices necessary for the achievement of the security level approved by the SK management.

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.

2. References

2.1. Normative references

[DAS] Digital Signatures Act of Estonia.

[Audit Regulation] Regulation No 68 of the Minister of Economic Affairs and Infrastructure (September 1, 2014), "Auditing procedure of the certification and time-stamping service providers' information systems".

[ISO27001] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[PDPA] Personal Data Protection Act of Estonia.

2.2. Informative references

[eIDAS] Regulation (EU) No 910/2014 of 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.

CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

CA/Browser Forum: "Network and certificate system security requirements".

Directive 1999/93/EC of the European Parliament and of the Council of 13 December, 1999 on a Community framework for electronic signatures.

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”.

ETSI EN 319 411-3: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates. Part 2: Policy requirements for certification authorities issuing public key certificates”.

ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures".

ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

ETSI TS 102 023: “Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities”.

FIPS PUB 140-2: “Security Requirements for Cryptographic Modules”.

ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management".

ISO/IEC 27005: “Information technology - Security techniques - Information security risk management”.

RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

3. Definitions, symbols and abbreviations

3.1. Definitions

Digital Signature:	a data unit, created by using a system of technical and organisational means, which is used by a signatory to indicate his or her link to a document. Detailed requirements are described in [DAS]. A Digital Signature is a form of Electronic Signature.
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.
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.
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.
Subscriber:	an entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
Trust Service:	described in [eIDAS] as an electronic service which is normally provided in return for remuneration and which consists of: (a) 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 (b) the creation, verification and validation of certificates for website authentication or (c) the preservation of Electronic Signatures, seals or certificates related to these services.
Trust Service 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.
Trust Service Practice Statement:	a statement of the practices that a TSP employs in providing a Trust Service.
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).

3.2. Abbreviations

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

4. General concepts

4.1. Trust Service Provider

SK is a Trust Service Provider that provides electronic services, which enhance trust and confidence in electronic transactions. SK maintains the overall responsibility for meeting the requirements defined in the present document and the liability for the issuing of Trust Service Tokens to the public as required in regulations and legal acts.

4.2. Trust Service Policy and Practice Statement

In general, the purpose of the Trust Service Policy, which may be referenced by a policy identifier in a token, states "what is to be adhered to", while the Trust Service Practice Statement states "how it is adhered to", i.e. the processes it will use in providing services. The relationship between the Trust Service Policy and the Trust Service Practice Statement is similar in nature to the relationship of other business policies, which state the requirements of the business, while the operational units define the practices, procedures and implementation of these policies.

Policies for the Trust Services offered by SK can be defined either by SK or by external sources.

The SK PS establishes the general rules concerning the operations of the SK Trust Services. Additional Practice Statements and other documents define how SK meets the requirements identified for each Trust Service. All Practice Statements may be downloaded at the SK repository https://www.sk.ee/en/repository/.

5. Obligations and Liability

5.1. TSP Obligations

5.1.1. General

SK provides its services consistent with the requirements and the procedures defined in this SK PS and service-based policies and practice statements.

SK ensures that all requirements on the SK PS are implemented and applicable to the service practice statements.

SK complies with [DAS] and related legal acts defined in this SK PS and service-based policies and practice statements.

5.1.2. TSP Obligations towards Subscribers

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:

- 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;
- inform the authorised processor of the Estonian Register of Certificates of any changes to a public key used for the provision of certification services or time-stamping services;

- preserve all the documentation related to Trust Services until the termination of its activity;
- ensure an annual audit of the information system and present the auditor's report to the authorised employee of the registry to ensure continual registration at the Estonian Register of Certificates;
- publish the terms of the compulsory insurance policy in a public data communications network.

5.2. Subscriber Obligations

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.

5.3. Relying Party Obligations

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.

5.4. Information for Relying Parties

5.4.1. SK Liability

SK:

- is liable for the performance of all its obligations specified in clause 5.1 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 Register of Certificates, the data protection supervision authority or any other public authority;
- non-fulfilment of the obligations arising from the SK PS if such non-fulfilment is occasioned by Force Majeure.

5.4.2. Dispute Resolution Procedure

All disputes between the parties will be settled by negotiation. If the parties fail to reach an 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 complaint not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

5.4.3. Publication of Information

All the SK documents directly related to the provisioning of Trust Services are available in the public data network at https://www.sk.ee/en/repository/. At least the following materials are made available in the repository:

- Trust Services Practice Statement;
- service-based policies and/or practice statements;
- terms and conditions of services;
- disclosure statement of services;
- terms and conditions of the compulsory insurance policy;
- revocation lists;
- public keys and relevant service certificates of SK;
- external audit conclusions.

Valid root certificates and the archive of root certificates of SK are published at https://www.sk.ee/en/repository/certs/.

Principles of personal data protection of services are published at https://www.sk.ee/en/.

SK guarantees the integrity and availability of the above-mentioned information 24 hours a day and 7 days a week.

Access to the above-mentioned information in the public data communications network is free of charge and unrestricted. In the event of other manners of publication, SK may fix a fee in a pricelist and/or require the existence of a service contract.

5.4.4. Compliance Audit

The information system, policies and practices, facilities, personnel, and assets of SK are audited in compliance with Estonian law and the Internal Audit Statute according to the following guidelines:

- the information system, policies and practices, facilities, personnel, and assets of SK are audited by an external auditor pursuant to the [DAS] and the corresponding legislation once a year or whenever a major change is made to Trust Service operations;
- External Auditors audit the parts of the SK information system used to provide Trust Services.

All exceptions are mentioned in detailed policies and practice statements.

The external auditor must have a certificate of a Certified Information Systems Auditor (CISA) issued by the ISACA, and it must be valid during the auditing period.

Audit conclusions, which are based on audit results of the external audits conducted pursuant to the [DAS] and [Audit Regulation], are published on SK's website https://www.sk.ee/en/repository/ .

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

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

a) quality of service;

b) security of service;

c) security of operations and procedures;

d) 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 External Auditor 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.

5.4.5. Confidentiality Provisions

5.4.5.1. 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.

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.

5.4.5.2. Public Information

Access to public information is ensured in accordance with clause 5.4.3. Additionally, SK may publish non-personalised statistical data about its services.

6. TSP Practices

6.1. Trust Services Practice Statement Administration

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 and external audits. The Quality Manager is responsible for the review and maintenance of the SK PS.

Amendments which do not change the meaning of the Trust Service practice, such as corrections of misspellings, translation and updating of contact details, shall be 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 event of substantial changes, the new Trust Service Practice Statement version shall be clearly distinguishable from the previous ones. The new version shall bear a serial number enlarged by one. The amended SK PS along with the enforcement date, which cannot be earlier than 30 days after publication, will be published electronically on SK's website.

All amendments will be submitted to the Register of Certificates.

6.2. TSP Dissemination of Terms and Conditions

Terms and conditions for each service are publicly available at https://www.sk.ee/en/ Conditions define the Trust Service Policy and/or the Practice Statement being applied; the expected life-time of the Trust Service Token and any other limitations on the use of the service; the subscriber's obligations as described in clause 5.2; information on how to verify the Trust Service Token and any possible limitations on the validity period; the period of time during which the TSP event logs are retained; limitations of liability as defined in clause 5.4.1; the applicable legal system as defined in clause 6.4.10 procedures for complaints and dispute settlement as defined in clause 5.4.2 conformity assessment scheme and SK contact information.

6.3. Key Management Life Cycle

SK uses cryptographic keys for its Trust Services and follows industries best practices for key lifecycle management.

6.3.1. TSP Key Generation

The signing keys of the SK Trust Services are created in accordance with the internal regulations of SK: Procedure for Creating SK Root Key and Procedure for Creating Keys for Intermediate Certification Authorities. The creation of 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 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.

6.3.2. TSP Key Storage, Backup, Recovery and Destruction

To meet the availability requirements, a backup copy is made of SK's signing keys. Key access is divided into two parts secured by different persons. Key cloning procedures (including key backup and key restore) require two persons using dual control. These persons must be in Trusted Roles. A security envelope is used for storing the access codes or access tokens to the keys of the SK Trust Services, and the opening of this envelope is detected.

The signing keys of the SK Trust Services can be used only when they are activated.

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

SK takes measures to permanently disable access to the private keys of Trust Services after their expiry or revocation so that further use or derivation thereof is impossible.

6.3.3. TSP Public Key Distribution

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/.

SK takes obligation to provide the SK Trust Service certificates to Trusted List of Estonian Register of Certificates.

SK makes its best effort to include the certificates in web browsers' vendor-supplied trust stores.

6.3.4. Life Cycle Management of Cryptographic Devices Used to Sign TSP Token

Cryptographic devices are purchased only from trusted providers. A device operator checks the integrity of the device prior to its implementation. Only persons in Trusted Roles operate cryptographic devices used for providing Trust Services.

The decommissioned cryptographic devices containing the SK Trust Services private keys or key backups are stored in a controlled area until their critical components are physically destroyed.

6.4. TSP Management and Operation

6.4.1. Security Management

In the field of security management, SK guides itself by the generally recognised standards, e.g. [ISO 27001], [ISO 27002] 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.

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. 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 configurations of SK's systems are regularly checked for changes that violate SK's security policies.

SK has procedures for ensuring that security patches are applied to Trust Service systems within a reasonable time after they become available, but not later than six months following the security patch's availability. The reasons for not applying any security patches will be documented.

6.4.2. Asset Classification and Management

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.

6.4.3. Personnel Security

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.

The employment contracts signed by the employees of 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.

SK establishes, maintains and enforces employment policies (as part of 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.

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

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

The roles of the Security Officer, System Auditor and System Administrators are completely separate and are staffed by different persons.

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 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.

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.

6.4.4. Physical and Environmental Security

SK uses trustworthy systems and products, which are protected against modification and ensure the technical and cryptographic security of the process supported by them.

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.

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

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.

Any persons entering this physically secure area will not remain for any significant period without oversight by an authorised person.

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 temperature and relative humidity.

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

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

Portable media, appliances and software may be taken away from the premises of SK pursuant to the established procedure. Media containing Sensitive Information may be stored only in a special safe designed for media storage.

6.4.5. Operations Management

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

The SK Trust Services system components are managed in accordance with change management procedures. These procedures include system testing in an isolated test environment and the approval of the Security Officer. The approval is documented for further reference.

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

All media containing production environment software and data, audit, archive, or backup information are stored within 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).

Capacity demands are monitored and projections for future capacity requirements are made to ensure that adequate processing power and storage are available.

Incident response and vulnerability management procedures are documented in an internal document.

SK has established a procedure for the regular analysis of the audit logs and the detection of possible attacks. Personnel in Trusted Roles review audit logs and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with. They also involve a brief inspection of all log entries with a more thorough investigation of any alerts or irregularities in the logs. Actions taken following these reviews are documented.

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

SK performs routine backups of critical system data, audit log data, and other Sensitive Information. SK has dual data centres to ensure availability requirements. 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.

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

All security operations are separated from other operations.

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

6.4.6. System Access Management

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

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

The network is separated into multiple security zones, as described in clause 6.4.12

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

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 SK's internal network is encrypted.

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.

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.

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

6.4.7. Trustworthy Systems Deployment and Maintenance

In the information system of SK, including all workstations, measures are implemented 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.

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.

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

6.4.8. Business Continuity Management and Incident Handling

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 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.

6.4.9. Trust Service 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 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 hands over the documentation related to the supply of the service and information needed to verify the Trust Service Tokens to the Estonian Register of Certificates pursuant to the established procedure.
- SK destroys the private keys related to the service, 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.

The notice of termination of SK's 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.

6.4.10. Compliance with Legal Requirements

SK ensures compliance with legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, the requirements of [PDPA], [DAS] and [eIDAS].

SK's principles of personal data protection have been stipulated in the document titled Personal Data Protection Principles by ensuring the personal data protection principles, confidentiality of non-public information, adequacy of client information storage as well as compliance with the [PDPA].

The information contributed by users to SK is completely protected from disclosure unless SK has their consent or there is a court order or other legal requirement.

6.4.11. Recording of Information Concerning Operation of the Service

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 trail of the Trust Service operation.

SK's information systems leave an audit trail of:

- all the life cycle stages and use of the certification keys of SK;
- all the life cycle stages of other signing keys and their certificates of SK;
- all life cycle stages of the client's keys;
- all security events, such as user authorisations or failed attempts of authorisation;
- the activities of system users with special rights;
- all events relating to the synchronisation of the clock to UTC;
- all events relating to the detection of loss of synchronisation;
- all significant environmental events.

All audit log entries include the following elements:

- date and time of entry;
- type of entry;
- result of the operation: success or failure;
- host name;
- identity (user name) of the entity making the journal entry.

The audit trail is protected with a mechanism that protects the log files from unauthorised viewing, modification, deletion, or other tampering; furthermore, only additions are allowed to the log file. Entries in the audit log are time-stamped.

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

A full backup of the audit log is performed weekly. The backup is stored on an external medium.

Audit logs are retained for no less than seven years.

Archive records that are required for proving the validity of Digital Signatures will be kept for an indefinite period without any loss of data. Such records include issued time-stamps.

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.

The archive is backed up in different physical locations. Thus, in the event of loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time. Only authorised personnel in Trusted Roles are allowed access to the archive. The integrity of the information is verified when it is restored.

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.

6.4.12. General Protection for the Network and Supporting Systems

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 in 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 another firewall and has no direct Internet access.

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.

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

6.5. Organisational Practices

Integral to its organisational practices SK:

- ensures that its organisation is reliable;
- ensures that policies and procedures under which SK operates are non-discriminatory;
- makes its services accessible to all applicants whose activities fall within its declared field of operation and who agree to abide by their obligations as specified in terms and conditions of services;
- has adequate arrangements to cover liabilities arising from its operations and/or activities;
- has the financial stability and resources required to operate in conformity with Trust Services requirements;
- has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of services or any other related matters;
- has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements;
- implements internal regulations and procedures, which support the security requirements of this SK PS.