AS Sertifitseerimiskeskus
Time-Stamping Authority Practice Statement

Version 1.2
Valid from 04.01.2016

Version Information		
Date	**Version**	**Modifications**
03.12.2015	1.2	p. 7.3.1. Removed support for SHA1 and SHA224 hash algorithms in time-stamp requests.
01.11.2015	1.1	Additions and amendments: - p. 5.2. Object-identifier (OID) has been changed. The OID was incorrect as it contained an extra zero. - p. 7.1.2. Disclosure Statement is provided as a part of Terms and Conditions.
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.

SK information system, security measures, organisation, processes and procedures developed to satisfy the requirements of the law and relevant international standards are documented in SK Trust Services Practice Statement (SK PS).

This SK Time-Stamping Authority Practice Statement (SK TSA PS) states only additional, time-stamping specific practices. In particular, the facility, management and operational controls such that Subscriber and Relaying Parties may evaluate their confidence in the operation of the time-stamping services.

SK time-stamping service conforms to ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities Time-Stamp protocol RFC 3161 and complies with the Digital Signatures Act of Estonia, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 and 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 .SK time-stamps may be applied to any application requiring proof that datum existed before particular time.

This SK TSA PS outlines the contents of the [ETSI 102023].

Table of Contents

1. Scope

The SK Time-Stamping Authority (SK TSA) uses the public key infrastructure and trusted time sources to provide reliable, standards-based time-stamps. This document states time-stamping specific practices of SK. In particular, the facility, management and operational controls such that Subscriber and Relaying Parties may evaluate their confidence in the operation of SK time-stamping services. This document should be read in conjunction with the SK Trust Services Practice Statement (SK PS), which describes overall SK trust services practices.

This SK TSA PS has been registered in the Estonian Register of Certificates (*Sertifitseerimise register*).

In the case of conflict between SK TSA PS and SK PS the provisions of SK TSA PS shall prevail. In case of conflict between the English original document and the Estonian translation, the English original shall prevail.

2. References

2.1. Normative references

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

[DAS] Digital Signatures Act of Estonia.

[ETSI 102023] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[PDPA] Personal Data Protection Act of Estonia.

[RFC 3161] RFC 3161: "Internet X.509 Public Key Infrastructure Time-stamp Protocol".

[SK PS] AS Sertifitseerimiskeskus Trust Services Practice Statement.

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.

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

Draft EN 319 421 V1.0.0 (2015-06): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services".

ITU-R Recommendation TF.460-6 (02/02): "Standard-frequency and time-signal emissions".

RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

3. Definitions, symbols and abbreviations

3.1. Definitions

Coordinated Universal Time (UTC)	the time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/02)
Network Time Protocol (NTP)	Protocol to synchronize system clocks among a set of distributed time servers and clients as defined in RFC 5905
Relying Party	the recipient of a Time-Stamp Token who relies on that Time-Stamp Token
Subscriber	the entity which requires the services provided by a TSA and has entered into the AS Sertifitseerimiskeskus Subscriber agreement
Time-Stamping Policy	a named set of rules that indicates the applicability of a Time-Stamp Token to a particular community and/or class of application with common security requirements applicable; the Time-Stamping Policy is defined in [ETSI 102023]
Time-Stamp Token (TST)	the data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Time-Stamping Authority (TSA)	the authority which issues Time-Stamp Tokens
Time-Stamping Unit (TSU)	a set of hardware and software which is managed as a unit and has a single Time-Stamp Token signing key active at a time (cluster of server nodes and hardware security modules (HSM) using common signing key)
TSA Disclosure Statement	a set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and Relying Parties, for example to meet regulatory requirements
TSA Practice Statement	statement of the practices that a TSA employs in issuing Time-Stamp Tokens
TSA System	a composition of information technology products and components organized to support the provision of time-stamping

3.2. Abbreviations

CA	Certification Authority
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
HSM	Hardware Security Modules

NTP	Network Time Protocol
SK	AS Sertifitseerimiskeskus
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement
SK TSA PS	AS Sertifitseerimiskeskus Time-Stamping Authority Practice Statement
TSA	Time-Stamping Authority
TST	Time-Stamp Token
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4. General concepts

4.1. General Policy Requirements Concepts

The concepts described in section 4 of SK PS apply.

4.2. Time-Stamping Services

SK takes overall responsibility for the provision of the time-stamping services, which include the following components:

- time-stamping provision - the service component that generates TSTs.
- time-stamping management - the service component that monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified in overall SK PS and in this SK TSA PS.

SK TSA adheres to the standards and regulations in section 2 of this document to keep trustworthiness of the time-stamping services for Subscribers and Relying Parties.

4.3. Time-Stamping Services Participants

4.3.1. Time-Stamping Authority

SK TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue TSTs. SK TSA has overall responsibility for the provision of the time-stamping services identified in section 5.2 SK TSA may operate several identifiable TSUs. SK has responsibility for the operation TSU that creates and signs on behalf of the TSA. SK TSA is identified in the digital certificates used in the TST.

Contact information:

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/

4.3.2. TSA Subscriber

The Subscribers are entities that hold a Subscriber agreement with SK time-stamping service. Subscriber may be an organisation comprising several end-users or an individual end-user. Organisations that are Subscribers, are responsible for the correct fulfilment of the obligations from its end-users and therefore are expected to suitably inform its end-users about the correct use of time-stamps and the conditions of the SK PS and SK TSA PS.

4.3.3. TSA Relying Party

A Relying Party is an individual or entity that acts in reliance of a TST generated under [ETSI 102023] policy by SK TSA. A Relying Party may, or may not also be a Subscriber.

4.4. Time-Stamping Policy and TSA Practice Statement

SK TSA Time-Stamping Policy is based on the Time-Stamping Policy specified in [ETSI 102023] and is applied to TSAs issuing TSTs.

This SK TSA Practice Statement is a form of SK Trust Services Practice Statement (SK PS) as specified in [ETSI 102023] applicable to SK TSA issuing TSTs.

5. Time-Stamping Policies

5.1. Overview

SK TSA issues the TSTs in accordance with [ETSI 102023] baseline Time-Stamping Policy.
The TSTs are issued with an accuracy of 1 second of UTC or better.

5.2. Identification

The object-identifier (OID) of the baseline Time-Stamping Policy is 0.4.0.2023.1.1:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-
policy(2023) policy-identifiers(1) baseline-ts-policy (1)
```

Note: The OID 0.4.0.02023.1.1 in [ETSI 102023] was incorrect as it contained an extra zero.

This OID is referenced in every TST issued by SK TSA.

6. Obligations and Liability

6.1. TSA Obligations

6.1.1. General

The general obligations specified in section 5.1.1 of SK PS apply.

6.1.2. TSA Obligations towards Subscribers

SK TSA obligations towards Subscribers specified in section 5.1.2 of SK PS apply.

6.2. TSA Subscriber Obligations

The general obligations specified in section 5.2 of SK PS apply.

Subscribers and Relying Parties must use secure cryptographic functions for time-stamping requests.

Subscriber obligations are also defined in the Subscriber agreement.

6.3. TSA Relying Party Obligations

The general obligations specified in section 5.3 of SK PS apply.

Relying Parties verify that TST has been correctly signed with the key corresponding to TSU certificate and that the private key used to sign the TST has not been compromised until the time of verification and take measures in order to ensure the validity of the TSTs beyond the life-time of the SK TSA certificates.

Validity information has to be verified according to section 7.3.1in this SK TSA PS.

6.4. Liability

The liability provisions in section 5.4.1 of SK PS apply.

The liability of the SK to the Subscribers is stipulated in the Subscriber agreements to be signed with the Subscribers.

The liability of the SK to Relying Parties interested in the preservation of the proof value of the validity confirmations is regulated herein.

SK is not liable for the mistakes in the verification of the validity of time stamps or for the wrong conclusions conditioned by omissions or for the consequences of such wrong conclusions.

SK shall assume no liability for the loss of the proof value of validity confirmation due to Force Majeure.

7. TSA practices

7.1. Practice and Disclosure Statements

SK TSA implements all practices described in section 7.

The provision of a TST in response to a request is at the discretion of SK TSA depending on the Subscriber agreement.

7.1.1. TSA Practice Statement

The requirements identified in section 6.1 of SK PS apply.

7.1.2. TSA Disclosure Statement

TSA Disclosure Statement is provided as a part of Terms and Conditions, which are available at https://www.sk.ee/en/repository/ .

7.2. Key Management Life Cycle

7.2.1. TSU key generation

The practices of key generation is described in section 6.3.1 of SK PS apply.

Personnel restrictions are described in section 6.4.3 of SK PS.

SK TSU is using RSA key pair with 2048 bit modulus. This key pair is used only for signing TSTs.

7.2.2. TSU Private Key Protection

The practices of TSU key storage, backup and recovery described in section 6.3.2 of SK PS apply

TSU private key will be backed up and securely stored for the unlikely event of key loss due to unexpected power interruption or hardware failure. Key backup will occur as part of key generation ceremony. Backed up private key remains secret and their integrity and authenticity is retained.

7.2.3. TSU Public Key Certificate

TSU public keys are made available to Relying Parties in a public key certificate.

The certificate for TSU public key is issued by SK root CA and is distributed in X.509 form on SK public web site https://www.sk.ee/en/repository/ and in the Estonian Trusted List (TL) http://sr.riik.ee/en/. Validity information is available in periodically updated CRLs.

Only one certificate is issued to any specific TSU key. TSU certificates are not renewed.

7.2.4. TSU Key Rekeying

TSU keys will have the expected lifetime of 5 years. A certificate is issued for the whole expected lifetime. TSU key lifetime is limited by SK root CA certificate validity. With new root CA certificate, a new TSU key will be generated.

7.2.5. End of TSU Key Life Cycle

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

7.2.6. Life Cycle Management of Cryptographic Module Used to Sign TSTs

The practices of HSM life cycle management are described in section 6.3.4 of SK PS apply.

7.3. Time-Stamping

7.3.1. Time-Stamp Token

SK TSA offers time-stamping services using RFC 3161 Time Stamp Protocol over HTTP transport. Service URL is specified in Subscriber agreements. Each TST contains Time-Stamping Policy identifier, unique serial number and TSU certificate containing SK TSA identification information.

SK TSU accepts SHA256, SHA384, SHA512 hash algorithms in time-stamp requests and uses SHA-512 cryptographic hash function in TST signatures.

SK TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

SK TSA logs all issued TSTs. TSTs will be logged for indefinite period. SK can prove the existence of particular TST on the request of Relying Party. SK might ask the Relying Party to cover the costs of such service.

7.3.2. Clock Synchronisation with UTC

SK TSA ensures that its clock is synchronised with UTC within the declared accuracy of 1 second using the NTP.

SK TSA monitors its clock synchronisation and ensures that, if the time that would be indicated in a TST drifts or jumps out of synchronisation with UTC, this will be detected. In the case of a TST drift or jump out of synchronisation with UTC, SK TSA stops issuing time-stamps until the issue is corrected. Information about loss of clock synchronisation will be made available in public media.

Both local and remote NTP servers with GPS time sources are used for NTP reference. Monitoring of clock synchronisation is done by comparing the time sources.

7.3.3. Dissemination of Terms and Conditions

The general obligations specified in section 6.2 of SK PS apply.

7.4. TSA Management and Operation

SK TSA has implemented the security regulations. Validation of the compliance with these regulations is performed during the annual independent security audit as described in section 5.4.4 of SK PS.

The SK TSA's security regulations contain sensitive security information and are only available upon special agreement with SK. An overview of the regulations content is described below.

7.4.1. Security Management

The practices identified in section 6.4.1 of SK PS apply.

7.4.2. Asset Classification and Management

The practices identified in section 6.4.2 of SK PS apply.

7.4.3. Personnel Security

The practices identified in section 6.4.3 of SK PS apply.

In addition, SK has employed a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

7.4.4. Physical and Environmental Security

The practices identified in section 6.4.4 of SK PS apply.

In addition, the access to TSA HSM's is allowed only for persons in the corresponding Trusted Roles.

7.4.5. Operations Management

The practices identified in section 6.4.5 of SK PS apply.

7.4.6. System Access Management

The practices identified in section 6.4.6 of SK PS apply.

7.4.7. Trustworthy Systems Deployment and Maintenance

The practices identified in section 6.4.7 of SK PS apply.

7.4.8. Business Continuity Management and Incident Handling

The practices identified in section 6.4.8 of SK PS apply.
Backups of the database of all issued TSTs by SK TSA are kept in off-site storage.

7.4.8.1. Entity Private Key Compromise Procedures

If TSU private key is compromised or suspected to be compromised, SK will inform Subscribers and Relying Parties and will stop using the compromised key. SK TSA will revoke the TSU certificate. The following actions will be carried out in accordance with the crisis commitee[1]s decision and recovery plan.

7.4.8.2. Loss of Clock Synchronisation

In case of loss of clock synchronisation, SK TSA suspends its operations to prevent further damage. Recovery plan is activated to restore the synchronisation and service.

7.4.9. SK TSA Termination

In case of SK TSA termination SK follows the procedures described in section 6.4.3 of SK PS.

Additionally SK takes steps to have the TSU certificates revoked.

7.4.10. Compliance with Legal Requirements

The practices identified in section 6.4.10 of SK PS apply.

7.4.11. Recording of information Concerning the Operation of Time-Stamping Service

The practices identified in section 6.4.11 of SK PS apply.

7.4.12. General Protection for the Network and Supporting Systems

The practices identified in section 6.4.12 of SK PS apply.

TSU systems are configured with only these accounts, applications, services, protocols, and ports that are necessary in SK TSA's operations.

7.5. Organisational Practices

The practices identified in section 6.5 of SK PS apply.

SK organisational structure, policies, procedures and controls apply to SK TSA. SK TSA organisational procedures comply with the standards and regulations referred in section 2.1 of this SK TSA PS.