AS Sertifitseerimiskeskus
Time-Stamping Authority Practice Statement

Version 1.3
Valid from 01.07.2016

Version Information		
Date	**Version**	**Modifications**
01.06.2016	1.3	Document is restructured according to ETSI EN 319 421 and AS Sertifitseerimiskeskus Trust Service Practice Statement.
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

Table of Contents

1. Introduction

AS Sertifitseerimiskeskus (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.

The SK Time-Stamping Authority (SK TSA) uses the public key infrastructure and trusted time sources to provide reliable, standards-based qualified time-stamps. SK time-stamps may be applied to any application requiring proof that datum existed before particular time.

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.

SK time-stamping service conforms to [eIDAS regulation], legal acts of Estonia and ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and other related standards.

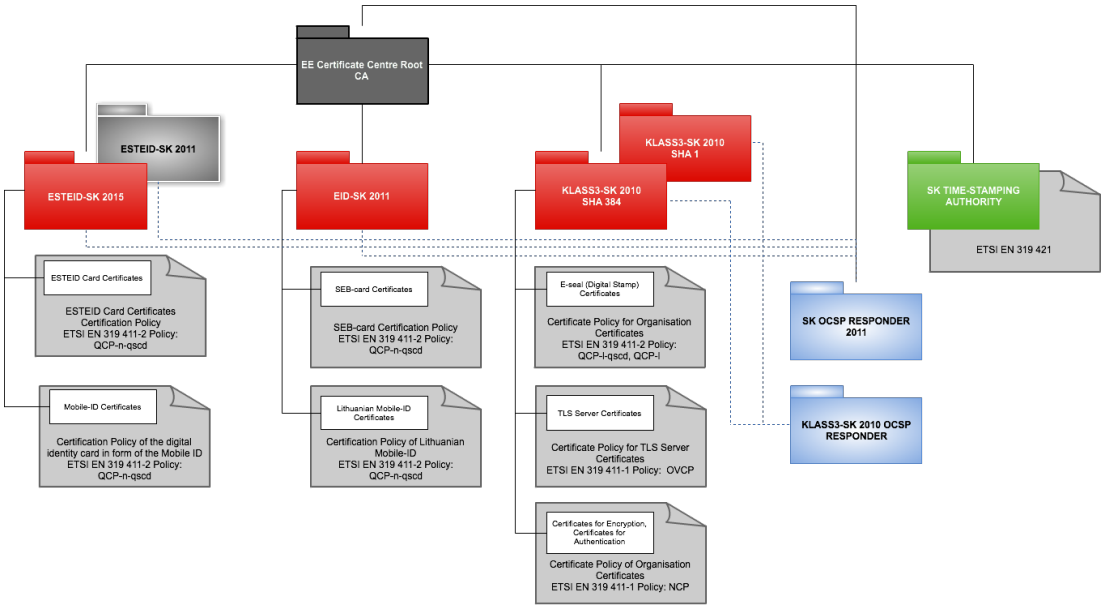
1.1. Overview

SK issues Time-Stamping Tokens in accordance with ETSI EN 319 421 best practice for time-stamping policy.

EE Certification Centre Root CA has certified SK Time-Stamping Authority.

The Root CA certificates and other certificates necessary for PKI operation are available from SK's homepage at http://www.sk.ee/en/repository/certs.

The relations between EE Certification Centre Root CA, subordinate CA-s and the CP-s are shown on the following figures:



The time-stamping service described in this SK TSA PS has qualified status in the Trusted List of Estonia, https://sr.riik.ee/en/tsl/estonia.html.

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

[eIDAS regulation] 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.

[ETSI EN 319 421] ETSI EN 319 421 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

[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

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
Root CA	the top level certification authority whose certificate is distributed by application software suppliers and that issues subordinate SK CA and TSU certificates.
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 SK TSA PS references SK PS for common practices to all SK trust services.

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 TSU certificate used to sign TST:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            24:af:ec:eb:12:68:d0:02:54:17:f7:86:ed:6f:01:59
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification Centre Root
CA/emailAddress=pki@sk.ee
        Validity
```

```
            Not Before: Sep 16 08:40:38 2014 GMT
            Not After : Sep 16 08:40:38 2019 GMT
        Subject: C=EE, O=AS Sertifitseerimiskeskus, OU=TSA, CN=SK TIMESTAMPING
AUTHORITY
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:93:da:fd:d4:0a:7a:64:8a:08:d4:b0:94:c5:29:
                    f5:82:90:63:ac:d0:39:fb:3d:be:05:27:6f:34:d1:
                    1c:24:41:45:db:1a:6d:96:24:9f:14:c8:e0:3a:90:
                    e7:e2:4f:ab:0f:0c:4e:40:ef:6f:a9:df:0d:91:9d:
                    d7:9b:78:a1:8e:2d:1d:75:e8:09:f4:6b:6c:c8:c9:
                    f7:e0:d5:f8:ce:db:77:eb:eb:04:8f:2f:8b:b0:c1:
                    08:ce:7d:fd:50:23:c4:10:2e:67:d3:fb:4e:c8:3c:
                    a3:c0:6b:56:aa:81:f5:cd:1e:ce:54:82:b4:58:3c:
                    5f:4c:76:11:3d:d9:06:d6:78:f5:40:11:87:f5:cf:
                    d3:b2:3b:79:19:3f:0e:d4:8b:61:ab:b1:24:33:f3:
                    5d:51:19:99:22:42:23:26:dc:96:8c:7d:de:ef:05:
                    e7:fa:3c:1b:24:9b:0f:91:98:32:17:df:38:98:17:
                    9a:e9:7f:57:3e:de:47:47:79:4b:10:8c:bc:92:11:
                    ac:fe:d6:7e:22:58:69:48:cb:62:a2:f6:c2:31:50:
                    7b:f9:d4:96:d7:06:0a:7d:8a:b6:a1:82:c8:7e:ef:
                    97:e5:f3:79:f7:9a:e9:78:dc:f1:e6:d3:81:a9:f6:
                    14:9d:14:1f:49:87:bf:df:25:58:00:ca:b9:32:36:
                    7d:77
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
            X509v3 Extended Key Usage: critical
                Time Stamping
            X509v3 Subject Key Identifier:
                B1:B0:BD:F7:E6:A0:69:16:6C:20:E5:51:FB:5C:F4:30:62:73:57:27
            X509v3 Authority Key Identifier:
                keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99

            X509v3 CRL Distribution Points:
                URI:http://www.sk.ee/repository/crls/eeccrca.crl

    Signature Algorithm: sha256WithRSAEncryption
        a8:a5:c5:3d:df:6c:15:3c:3e:9e:79:df:ac:0c:18:6d:e3:3b:
        7e:90:c3:cf:15:7b:f5:a4:85:f4:46:06:e2:cd:a2:af:1d:65:
        38:a0:7a:51:1f:cc:dc:82:8f:e0:a6:8b:51:2e:52:e1:65:b1:
        ed:bb:de:29:2c:53:7a:7a:7a:62:c8:73:70:7a:f9:26:53:2b:
        eb:05:6c:a5:38:d4:75:62:1c:1b:e1:d2:d2:f2:90:46:18:54:
        7a:79:17:61:1b:3a:0a:01:41:78:07:87:48:a1:73:a3:e2:9d:
        ba:ab:5c:98:50:b1:79:66:46:47:c6:14:05:36:2e:6e:c5:a9:
        3d:b6:00:85:94:6b:73:5e:e9:a3:2f:98:c1:9a:d5:9e:0d:31:
        84:e1:84:9a:df:8a:73:0d:78:f3:f1:50:23:3c:9f:6c:56:e3:
        a6:2b:61:34:83:25:b1:51:32:d7:17:d6:1e:be:b5:b3:44:bc:
        d5:16:ac:3e:a9:ec:01:57:62:38:a1:ff:fa:9a:26:4e:39:3d:
        b0:94:0f:e6:78:be:f3:af:78:67:7e:8e:ca:48:94:26:30:d5:
        23:67:a9:61:e9:10:48:56:f6:08:d2:df:80:fd:fa:53:2a:26:
        5f:be:2c:ff:5e:7d:9e:e0:f0:ba:8b:9e:f0:98:7e:44:80:e3:
        9a:bf:45:0a
```

Contact information:

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Estonia
Tel +372 610 1880 (Mon-Fri 9.00-18.00 East European Time)
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 EN 319 421] 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 EN 319 421] 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 EN 319 421] applicable to SK TSA issuing TSTs.

5. Time-Stamping Policies

5.1. General

SK TSA issues the TSTs in accordance with [ETSI EN 319 421] 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)
```

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

6. Policies and practices

6.1. Risk assessment

Refer to clause 5.7.1 of SK PS.

6.2. Trust Service Practice Statement

Refer to 1.5.4, 2.2 and 5.8 of SK PS.

6.3. Terms and conditions

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

6.4. Information security policy

Refer to section 5 of SK PS.

6.5. TSA Obligations

SK TSA obligations towards Subscribers and Relying Parties specified in section 9.6.1 of SK PS apply.

6.6. TSA Subscriber Obligations

The general obligations specified in section 9.6.3 of SK PS apply.

Subscriber is obligated to verify the signature of TSTs and ensure that the private key used to sign the TST has not been revoked.

Subscriber is obligated to use secure cryptographic functions for time-stamping requests.

Subscriber is obligated to inform its end-users (e.g. Relying Parties) about correct use of time-stamps and the conditions of the SK PS and SK TSA PS.

Subscriber obligations are also defined in the Subscriber agreement.

6.7. TSA Relying Party Obligations

The general obligations specified in section 9.6.4 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 7.7.1 in this SK TSA PS.

6.8. Liability

The liability provisions in section 9.7, 9.8 and 9.9 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 management and operation

7.1. Introduction

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.

7.2. Internal Organisation

The practices identified in section 9 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.

7.3. Personnel Security

The practices identified in section 5.2 and 5.3 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. Asset Management

The practices identified in section 5, 6.5 and 6.6.3 of SK PS apply.

7.5. Access Control

The practices identified in section 6.5 and 6.7 of SK PS apply.

7.6. Cryptographic Controls

7.6.1. TSU key generation

The practices of key generation described in section 6.1 and 6.2 of SK PS apply.

Personnel restrictions are described in section 5.2 and 5.3 of SK PS.

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

All cryptographic modules are associated with the same public key certificate.

7.6.2. TSU Private Key Protection

The practices of TSU key protection, storage, backup and recovery described in section 6.2 and 6.3 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.

7.6.3. 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) https://sr.riik.ee/en/tsl/estonia.html. Validity information is available in periodically updated CRLs or OCSP service references located in the certificate.

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

SK TSU does not issue any TST before public key certificate is loaded into the TSU.

7.6.4. 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.

7.6.5. Life cycle management of signing cryptographic hardware

The practices of HSM life cycle management are described in section 6.2 of SK PS apply.

7.6.6. 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.

7.7. Time-Stamping

7.7.1. Time-Stamp Issuance

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.

SK TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2. 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.

Leap seconds are not considered and TSTs are issued as usual.

7.8. Physical and Environmental Security

The practices identified in section 5.1 and 6.7 of SK PS apply.

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

7.9. Operation Security

The practices identified in section 6.5, 6.6 and 6.7 of SK PS apply.

7.10. Network Security

The practices identified in section 6.7 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.

7.11. Incident Management

The practices identified in section 5.7.1 of SK PS apply.

7.12. Collection of evidence

The practices identified in section 5.4.1 of SK PS apply.

7.13. Business Continuity Management

The practices identified in section 5.7 of SK PS apply.

Backups of the database of all issued TSTs by SK TSA are kept in off-site storage.

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 commitee¹s decision and recovery plan.

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.

7.14. TSA termination and termination plans

In case of SK TSA termination SK follows the procedures described in section 5.8 of SK PS.

Additionally, SK takes steps to have the TSU certificates revoked.

7.15. Compliance

SK TSA has implemented the security regulations. Validation of the compliance with these regulations is performed during the annual independent conformity assessment as described in section 8 of SK PS.

The SK TSA's security regulations contain sensitive security information and are only available upon special agreement with SK.