# AS Sertifitseerimiskeskus
# Terms and Conditions for Use of Time- Stamping Service

Valid from 01.07.2016

## 1. Definitions and acronyms

| | |
|---|---|
| CA | Certificate Authority |
| Coordinated Universal Time (UTC) | The time scale based on the second as defined in ITU-R Recommendation TF.460-6 (02/02) |
| 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 |
| 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 |
| GPS | Global positioning system |
| Network Time Protocol (NTP) | Protocol to synchronize system clocks among a set of distributed time servers and clients as defined in RFC 5905 |
| Qualified Trust Service | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body. |
| 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 Time-Stamp Authority and has entered into the AS Sertifitseerimiskeskus Subscriber agreement |
| SK | AS Sertifitseerimiskeskus, Time-Stamp Authority which issues Time-Stamp Tokens |
| Subscriber Agreement | Agreement between SK and Subscriber for use of time-stamping service provided by SK |
| SK PS | AS Sertifitseerimiskeskus Trust Services Practice Statement |
| SK TSA PS | AS Sertifitseerimiskeskus Time-Stamping Authority Practice Statement |
| Terms and Conditions | Present document, that describes the rights, obligations and responsibilities for the Subscriber and Relying Party while using and/or relying on the time-stamping service |
| Time-Stamp Authority (TSA) | The authority which issues Time-Stamp Token |
| 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 |
| 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 |
| Trust Service | Described in eIDAS regulation as an electronic service which is normally provided in return for remuneration and which consists of:<br>- 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<br>- the creation, verification and validation of certificates for website authentication or<br>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 |

# 2. General terms

2.1. 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.

2.2. Present Terms and Conditions describe main policies and practices followed by TSA and provided in SK TSA PS (e.g. Disclosure Statement).

2.3. Present Terms and Conditions provide the conditions of use of time-stamping service and are binding for the Subscriber, while using time-stamping service and for the Relying Party, while relying on issued time-stamps.

2.4. Subscriber and SK conclude Subscriber Agreement, which includes present Terms and Conditions and where all specific service conditions are detailed. In the case of conflict between Subscriber Agreement and Terms and Conditions, the provision of Subscriber Agreement shall prevail.

2.5. SK has the right to amend Terms and Conditions at any time should SK have a justified need for such amendments. The amended Terms and Conditions along with the enforcement date, is published 30 days before enforcement electronically on the website of SK at https://www.sk.ee/en/repository/tsa.

# 3. Time-stamp types and usage

3.1. SK TSU issues qualified electronic time-stamps as per eIDAS regulation, SK TSU do not issue non-qualified electronic time-stamps.

3.2. SK issues the TSTs in accordance with ETSI EN 319421 best practice for time-stamping policy. The object-identifier (OID) of 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).

3.3. SK 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.

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

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

3.6. The lifetime of TST is indefinite.

3.7. SK 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.

# 4. Reliance limits

4.1. SK TSA ensures that its clock is synchronised with UTC within the declared accuracy of 1 second using the NTP.
4.2. 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.
4.3. 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.
4.4. Logs all issued TSTs are retained for indefinite time. Audit logs for other events are retained for no less than 10 years.

# 5. Obligations of Subscribers

5.1. Subscriber is obligated to use time-stamping service in compliance with the Terms and Conditions and applicable agreements set out in art 8.
5.2. Subscriber is obligated to verify the signature of TSTs and ensure that the private key used to sign the TST has not been revoked.
5.3. Subscriber is obligated to use secure cryptographic functions for time-stamping requests.
5.4. 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.

# 6. Obligations of Relying Party and TSU public key certificate status checking

6.1. Relying Party is obligated to study the risks and liabilities related to the acceptance of TSTs. The risks and liabilities have been set out in SK PS, SK TSA PS and present Terms and Conditions.
6.2. Relying Party is obligated to check the validity of the TSU public key certificate status by CRL or OCSP service references located in the certificate.
6.3. TSU public keys are made available to Relying Parties in a public key certificate.
6.4. Relying Party is obligated to verify the signature of TSTs and ensure that the private key used to sign the TST has not been compromised until the time of verification by CRL or OCSP service references located in the certificate. Relying Party is obligated to take measures in order to ensure the validity of the TSTs beyond the life-time of the SK TSA certificates.

# 7. Limited warranty and disclaimer

7.1. SK is liable for the performance of all its obligations specified in SK PS and TSA PS to the extent prescribed by the legislation of the Republic of Estonia and European Union;
7.2. SK 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.
7.3. SK informs all Subscribers before SK terminates service of time-stamping and maintains the documentation related to the terminated services and information needed according process set out in SK TSA PS and SK PS.
7.4. SK is not liable for:
7.4.1. 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.

7.4.2. 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;

7.4.3. non-fulfilment if such non-fulfilment is occasioned by Force Majeure.

# 8. Applicable agreements and practice statements

8.1. Relevant agreements, policies and practice statements related to present Terms and Conditions are:

8.1.1. AS Sertifitseerimiskeskus Time-Stamping Authority Practice Statement (SK TSA PS), published: https://sk.ee/en/repository/sk-ps/;

8.1.2. AS Sertifitseerimiskeskus Trust Services Practice Statement (SK PS), published: https://sk.ee/en/repository/tsa/;

8.1.3. Subscriber Agreement, published: https://sk.ee/en/repository/tsa/;

8.1.4. Principles of Client Data Protection https://sk.ee/en/repository/data-protection/.

# 9. Privacy policy and confidentiality

9.1. SK follows Principles of Client Data Protection in the SK repository https://sk.ee/en/repository/data-protection/ when handling personal information, and logging information.

9.2. 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 time-stamping service) is confidential. Subscriber has a right to get information from SK about him/herself according to legal acts.

9.3. 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.

9.4. 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.

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

# 10. Refund policy

10.1. SK handles refund requests case-by-case.

# 11. Applicable law, complaints and dispute resolution

11.1. The time-stamping service is governed by the jurisdictions of Estonia and European Union as the location where SK is registered as a CA.

11.2. 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.

11.3. 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.

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

11.5. All dispute requests should be directed to Contact info given in these Terms and Conditions.

# 12. TSA and repository licenses, trust marks, and audit

12.1. Time-stamping service has qualified status in the Estonian Trusted List https://sr.riik.ee/en/tsl/estonia.html. Prerequisite requirement of this registration is compliance with applicable regulations and standards.

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

12.3. Audit conclusions, 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://sk.ee/en/repository/certs/

# 13. Contact information

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt. 141, 11314 Tallinn
Estonia
Phone: +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