guardtime

JULY 2023

GUARDTIME KSI SERVICE DISCLOSURE STATEMENT

ID: GT/KSI/TSA/DS

Version: 2.6

Effective from: 23 March 2022

Next review: July 2024

Classification: Public

Review and maintenance: Product Owner

Approved by: Management Team

Contents

1. Purpose

A. This document is the GuardTime OÜ ("Guardtime") Time-Stamping Authority (TSA) Disclosure Statement as per [ETSI-401] and Guardtime Timestamping Policy.

B. The purpose of this document is to provide information about the policies and practices of the TSA that require particular emphasis or disclosure to Subscribers and Relying Parties. This document does not replace or substitute other definitive Guardtime agreements, policy and practice documents which are available at https://guardtime.com/library/tsp.

C. This document is not intended to provide comprehensive technical details and specifications of KSI technology. This information is available in the KSI Developer Guide and other documentation that is made available to Subscribers.

D. This document is not intended to create contractual relationships between Guardtime and any other person. All applicants who agree to abide by the obligations described in the Applicable Agreements section of this document are eligible to sign a Service Subscription Agreement for the provision of the service.

E. The Service Subscription Agreement signed by the applicant includes a restatement of the points of the Applicable Agreements section, adding to it the Subscriber's specific details, such as the desired service level of the KSI Services. The Service Subscription Agreement prevails in case of a conflict with another agreement.

F. Guardtime has the right to amend this document at any time when justified and appropriate. New versions of this document are published at https://guardtime.com/library/tsp no later than 30 days before their enforcement.

2. References

Reference	Document
[eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
[ETSI-401]	ETSI EN 319 401 V2.3.1 (2021-05). Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI-421]	ETSI EN 319 421 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
Guardtime Timestamping Policy	OID: 1.3.6.1.4.1.27868.2.3.2 First Published 2019-11

3. Definitions

A. For definitions and abbreviations turn to KSI Definitions and Abbreviations (GT/KSI/DEF).

4. Contact Information

A. The time-stamping service is operated by a private limited company Guardtime OÜ registered in Estonia. The contact information for the time-stamping service is as follows:

A. H. Tammsaare tee 60
11316 Tallinn
Estonia

E-mail: info@guardtime.com
Website: https://guardtime.com
Phone: +372 6555097

Technical support: support@guardtime.com

5. Time-Stamp Type and Usage

B. Time-stamps may be applied to any application requiring proof that a datum existed before a given time.

C. Guardtime delivers the time-stamping service in accordance with [eIDAS]. The time-stamping policy applied is Guardtime Timestamping Policy 3, version 2. The object-identifier (OID) of the policy is: iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) Guardtime OÜ (27868) policies (2) time-stamping policy (3) version (2).

D. Universally supported time-stamp request hash functions include SHA-256, SHA-384 and SHA-512. Supported hash functions may be marked as depreciated or not trusted at the end of their life-cycle, possibly requiring software updates in order to maintain access to KSI Services.

E. A KSI time-stamp consists of an Aggregation Hash-Chain (AHC), a Calendar Hash-Chain (CHC) and an optional Calendar Authentication Record (CAR) that cryptographically links the request input hash to a root of trust.

F. The CHC is extracted from the perpetual and global Calendar Blockchain (hash-tree) where the root hash of the Global Aggregation Tree is added every second. The shape of the CHC encodes the time attribute of time-stamp.

G. Right after the creation of a time-stamp, the CAR contains a cryptographic signature. Once the next Publication is issued, the time-stamp can be *extended*: the CHC is extended to the last Publication, and CAR is replaced with one containing a Publication Code and Publication References.

H. It is recommended to extend time-stamps before archiving and prefer extended time-stamps for verification.

I. Guardtime's KSI time-stamping service is backed and secured by one unique instance of the Calendar Blockchain. Therefore, exactly one Timestamping Policy is used.

6. Verification of Time-stamps

A. The verification of a time-stamp establishes the integrity of the time-stamped data and returns the time of time-stamping and optionally additional meta-data, preserved at the moment of time-stamping. The validation of time-stamped data and additional meta-data, as presented at the time of time-stamping, is optional and may be covered by additional agreements.

B. KSI time-stamp components are verified as follows:

   a. The hash of the time-stamped data is verified using the AHC.

   b. The AHC is verified either using the CHC or an authentic copy of the KSI Calendar Blockchain.

   c. The CHC is verified using either the CAR or an authentic Publication Code.

   d. The CAR is verified using an authentic Publications File.

C. Verification may include a time-stamp extending step, where extended time-stamp is not persisted after the verification. This assumes on-line access to a (not necessarily trusted) Extender service.

D. KSI time-stamp verification algorithm is parameterized using a Verification Policy, which is chosen based on concrete circumstances like risk profile, network connectivity, available root of trust, and the age of verified time-stamps. A list of predefined Verification Policies is provided in Table 1.

Table 1: Verification Policies

Verification Policy	**Trust Anchor**	**Availability**	**Networking Needed**
Calendar Based	Authentic Calendar Blockchain (trusted Extender service)	In a few seconds	Yes
Key Based	Authentic Publications File	Immediately, but for limited time[1]; If not extended[2]	No
Publications File Based	Authentic Publications File	If Publication exists[3]	If not extended
User Publication Based	Authentic Publication Code	If Publication exists	If not extended
General (default)	Authentic Publications File	Immediately	*Yes* if not extended and Publication exists, with fallback to *No*

E. The General Verification Policy (see Fig. 1):

a. Extends the time-stamp if not extended and possible by time-stamp age, relative to the latest publication in Publications File.

b. Performs Key Based Verification using signature in CAR if time-stamp is still not extended.

c. Performs Publications File Based (using a Publication Code from the file) Verification if extended.

[1] It is recommended to not use this policy after "Publication Exists"; there may be a longer grace period when this policy still works, as long as its cryptographic strength is definitive.
[2] If the KSI time-stamp being verified is not extended, see Clause G.
[3] If at least one Publication Code has been generated after issuing the time-stamp.

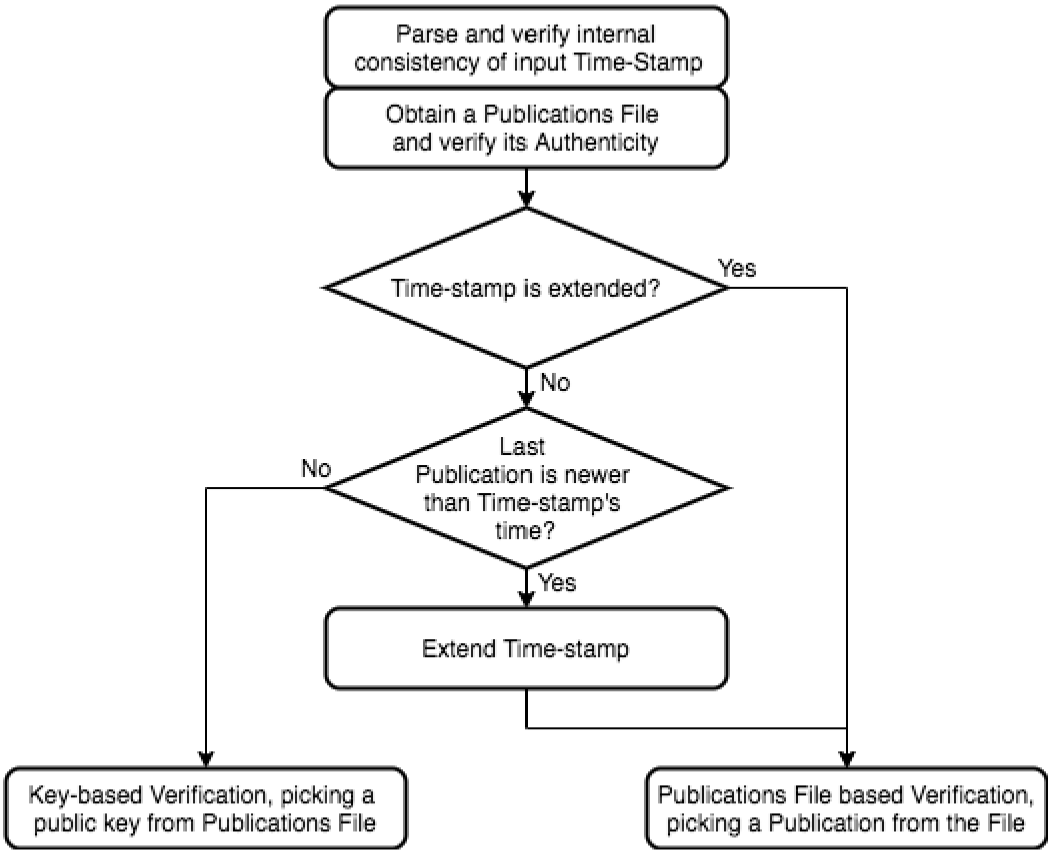
Parse and verify internal consistency of input Time-Stamp
Obtain a Publications File and verify its Authenticity
Time-stamp is extended?
Yes
No
Last Publication is newer than Time-stamp's time?
No
Yes
Extend Time-stamp
Key-based Verification, picking a public key from Publications File
Publications File based Verification, picking a Publication from the File

Figure 1: Flow-chart of the General Verification Policy

F. KSI time-stamp verification algorithm relies on an authentic Trust Anchor. Authentication of Trust Anchors is a critical step and must be performed either algorithmically based on appropriate roots of trust, or manually with due care. Possible Trust Anchors are listed in Table 1.

G. Publications File is authenticated using a trusted CA Root Certificate, applying a set of pre-configured restrictions: URL for downloading the file and the content of validated fields and extensions of Publications File Signing Certificate (together referred as Appropriate Restrictions, see Clause K and [GT/KSI/ToS] for exact values). The CA Root Certificate may be one of the certificates in provided Trust-store (by user or by underlying platform).

H. The time-stamp is valid and its issuance conforms to requirements for Qualified Time-stamps, as defined in the eIDAS regulation, if:

   a. Publications File is authenticated according to Clause G,

   b. Certificate for signing the Publications File is Qualified Certificate for Electronic Seals provided by an eIDAS qualified trust service provider, this implies presence in the EU Trustlist,

   c. Either General (default) or Publications File Based verification policy is chosen and executed successfully.

I. If the formal guarantees of Qualified Timestamp status are important for a customer's use-case, then all requirements in Clause H must be satisfied.

J. Guardtime provides and maintains the source code for the verification of time-stamps which is available at https://github.com/guardtime in various programming languages under non-restrictive license.

K. Guardtime distributes a Publications File at https://verify.guardtime.com/ksi-publications.bin

L. Guardtime replicates and provides access to the Calendar Blockchain through the Extender service, a component of KSI Gateway. New blocks are distributed in near real-time.

M. Guardtime will notify all Subscribers at least 2 months prior to the termination of KSI time-stamping service. The Subscribers will receive explicit instructions on the actions required to make sure that all time-stamps issued before termination can be verified at any point of time in the future.

7. Time-Stamp Lifetime and Reliability Factors

A. The lifetime of KSI Time-stamps is not limited.

B. The accuracy of the time in KSI Time-stamps with respect to UTC is ±1 second.

C. Extended KSI Time-stamps rely on the hash functions used in the hash-chains and the integrity of the publication (e.g., newspaper). The integrity of Publications is guaranteed by an authentic Publications File.

The publications are published periodically in a newspaper. Due to large circulation, distribution and archiving by independent parties the Publication serves as a strong long-term trust anchor.

D. Extended KSI time-stamps are not vulnerable to collisions potentially found in the hash function in the future, and to the leakage of any cryptographic keys.

E. Publications are issued on a monthly basis.

F. KSI Time-stamping infrastructure is redundant in order to provide high availability. Availability guarantee is provided in the KSI Service Subscription Agreement.

G. Guardtime monitors the cryptographic strength of the algorithms used and takes necessary actions in the time-stamping service infrastructure as well as in the verification tools as appropriate.

H. Guardtime retains the audit log concerning the operation of the time-stamping service for a period of 10 years, in order to provide supportive evidence if necessary.

8. Overview of Conditions of Use

A. For conditions of use of the time-stamping service refer to the KSI Terms of Service (GT/KSI/ToS), unless otherwise stated in the KSI Service Subscription Agreement.

9. Applicable Agreements

ID	**Name**
GT/PP	Guardtime Privacy Policy
GT/KSI/DEF	Guardtime KSI Definitions and Abbreviations
GT/KSI/ToS	Guardtime KSI Terms of Service
GT/KSI/TSA/PS	Guardtime KSI Practice Statement

GT/KSI/TSA/DS	Guardtime KSI Disclosure Statement (this document)
GT/KSI/EULA	Guardtime KSI Software End-User License Agreement

10. Limited Warranty and Limitation of Liability

A. Guardtime undertakes the operation of KSI Services in accordance with the Applicable Agreements and Estonian legislation.

B. For applicable warranties and limitation of liability refer to the KSI Terms of Service (GT/KSI/ToS), unless otherwise stated in the KSI Service Subscription Agreement.

C. Guardtime has a compulsory insurance contract, which covers KSI Services to ensure compensation for damage, which is caused as a result of violation of the obligations of Guardtime.

11. Privacy Policy

A. For privacy policy, refer to the Guardtime Privacy Policy (GT/KSI/PP) document.

12. Refund Policy

A. Refund requests for service fees will be handled on a case-by-case basis and in accordance with the KSI Service Subscription Agreement in effect.

13. Applicable Law, Complaints and Dispute Resolution

A. KSI Services is governed by the laws and regulations of Estonia. For applicable law, dispute resolution and complaint submission refer to the KSI Terms of Service (GT/KSI/ToS), unless otherwise stated in the KSI Service Subscription Agreement.

14. TSA and Repository Licenses, Trust Marks and Audit

A. Compliance with the requirements for IT systems and organization is checked according to Guardtime information security policy and the compliance management procedure.

B. External audits are carried out in accordance with regulatory requirements set out by Estonian law and [eIDAS], by auditors of an independent company holding valid certificates.

C. The conformity assessment for qualified electronic time-stamps according to Estonian law and [eIDAS] is conducted by an accredited conformity assessment body.

D. Audit reports and certificates are published at https://guardtime.com/library/tsp.

Appendix A: Document Versioning and Review History

Date (MM.YYYY)	Version	Author	Changes
09.2018	1.0	Guardtime	Creation of the document.
12.2018	2.0	Guardtime	Major refactoring and amendments for [eIDAS] compliance and auditing purposes.
01.2019	2.1	Technical Writer	Updated style formats to be consistent with other Guardtime documents.
05.2019	2.2	Product Owner	Changed approver from CEO to Management Team.
11.2019	2.3	Product Owner	Reference change from ETSI-421 to Guardtime Timestamping Policy. Updates to section 14
01.2020	2.4	Product Owner	Company legal form change (Guardtime AS -> Guardtime OÜ)
09.2020	2.5	Product Owner	Clarifications on qualified timestamp verification method & authenticity verification of the Publications File.
08.2021	2.6	KSI Auditor	Detailed description of verification process in order to expose the significance of choosing a Trust Anchor and a Verification Policy. Update of ETSI 401 reference to latest version 2.3.1.
07.2023	2.6	Product Owner	Annual review, no changes.