guardtime

Guardtime

KSI Service Disclosure Statement

ID: GT/KSI/TSA/DS

Version: 2.5

Effective from: 18 December 2020

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 online end-user 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 V2.2.1 (2018-04). 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: 1.3.6.1.4.1.27868.2.3.1 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

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

B. Guardtime aims to deliver the time-stamping service in accordance with [eIDAS]. The time-stamping policy applied is Guardtime Timestamping Policy 3, version 1. 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 (1).

C. Acceptable time-stamp request hash functions include SHA-256, SHA-384 and SHA-512.

D. The time-stamp consists of an Aggregation Hash-Chain (AHC) and Calendar Hash-Chain (CHC) that cryptographically link the request input hash to a widely-witnessed publication in electronic or physical media.

E. 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 CHC shape provides the time attribute of the time-stamp token.

F. The Guardtime Aggregation Network and Calendar Blockchain, where the AHC and CHC are extracted from, currently use the SHA-256 hash function.

G. Right after the creation of the time-stamp token, the CHC is authenticated by means of an RSA signature or a copy of the Calendar Blockchain. Once the next Publication is issued, the CHC in the time-stamp token can be extended to the Publication or any following Publication. During the time-stamp extension, the signature created by the RSA private key is replaced by the CHC that cryptographically links the time-stamp to the Publication.

H. Guardtime's time-stamping service is backed and secured by one unique

instance of the Calendar Blockchain. Therefore exactly one Timestamping Policy is used, by which only Qualified Timestamps are issued.

I. This document describes multiple ways for establishing the authenticity of Calendar Blockchain and subsequently of all timestamps. Only publication-based verification, with Publications File as the trust anchor, is accredited as the verification method of Qualified Timestamps under EIDAS regulation. Thus, if the formal guarantees of Qualified Timestamp status are important for a customer´s use-case, an appropriate verification policy must be configured.

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 the Apache License.

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

   a. convenient, machine-readable access to all issued widely-witnessed Publications;

   b. obtaining public keys for the short-term RSA-based authentication of CHC.

L. Guardtime will notify all Subscribers at least 2 months before terminating the KSI Services. The Subscribers will receive explicit instructions on the actions required to make sure that all time-stamp tokens issued before termination can be verified at any point of time in the future.

6. Time-Stamp Lifetime and Reliability Factors

A. The lifetime of time-stamps is not limited. Verification of the timestamps assumes availability of an authentic Publications File.

B. Guardtime assures time within ±1 second of a trusted UTC time source.

C. The time-stamp tokens in which the CHC has been extended to a Publication only 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 strong trust anchor..

D. The time-stamp tokens in which the CHC has not yet been extended to a Publication rely on RSA or the integrity of a copy of the Calendar Blockchain.

E. The time-stamp tokens issued and extended to a Publication are not vulnerable to collisions potentially found in the hash function in the future.

F. Publications are issued on a monthly basis.

G. The updates to the Calendar Blockchain are distributed to Subscribers in near real-time.

H. Time-stamping infrastructure is redundant in order to provide high-availability.

I. Guardtime monitors the collision and 2nd preimage resistance of the hash functions used and takes necessary actions in the time-stamping service infrastructure as well as in the verification tools as appropriate.

J. The Core Nodes' public keys in the Publications File are available for 5 years; however, this is not guaranteed as they should be used for only short-term verification of the new time-stamp tokens.

K. 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.

7. 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.

8. 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

9. 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.

10. Privacy Policy

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

11. 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 made with a particular Subscriber.

12. 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.

13. 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, based on the requirements in [ETSI-401] and the Guardtime Timestamping Policy. The assessment consists of, firstly, a review of the documentation followed by an on-site inspection to check the implementation.

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

14. Requirements Related to TSU Public Key Certificate Status Checking

A. This section and its title relate to the Guardtime Timestamping Policy document, which is based on [ETSI-421]. The standard assumes a time-stamping implementation where a TSU directly signs the time-stamp token with a certificate issued to the TSU by a CA that operates under ETSI EN 319 411-1 [i.10]. The [eiDAS] regulation does not restrict the methods for the verification of qualified electronic time-stamps in order to allow the new technologies like KSI to be developed. The following points clarify briefly how KSI technology compares to the implementation foreseen by ETSI regarding terminology and requirements.

B. KSI uses only cryptographic hash functions and widely-witnessed publications in electronic and physical media (for example, newspapers) as trust anchors for verifying time-stamp tokens and proving that a datum existed at a given time.

C. The Core Nodes operated by Guardtime for the KSI service are similar to the TSUs foreseen by [ETSI-421], as they are also synchronized to UTC using accurate and reliable time sources. However, due to a different approach, these capabilities are exploited in a different way:

    a. A number of Core Nodes operate as a cluster (collectively called Core) with a consensus protocol in order to provide high availability and reliability.

    b. The primary purpose of the Core is to accurately maintain the Calendar

Blockchain - add a unique hash to it exactly every second and distribute the Calendar Blockchain downstream.

c. The Publications File is signed using a Qualified Certificate for Electronic Seals provided by an eIDAS accredited trust service provider, to the e-mail publications@guardtime.com.

d. The Publications File signing certificate is listed as the digital identity of the KSI timestamping service in the EU List of eIDAS Trusted Lists: https://webgate.ec.europa.eu/tl-browser/#/tl/EE/1

D. Automated authenticity verification of Publications File is based on a public truststore provided by the underlying platform.

E. The CRL and OCSP responder pointers in the Publications File signing certificate are used to check the revocation status of the certificate, according to industry-standard procedures.

Appendix A: Document Versioning

A.1. Version 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.