guardtime

# Guardtime

# KSI Service Disclosure Statement

ID: GT/KSI/TSA/DS

Version: 2.1

Effective from: 01 April 2019

Classification: Public

Review and maintenance: Product Owner

Approved by: CEO

# Contents

# 1. Purpose

A. This document is the GuardTime AS (“Guardtime”) Time-Stamping Authority (TSA) Disclosure Statement as per [ETSI-401] and [ETSI-421].

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 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 their obligations arising from the Applicable Agreements (as defined in section Applicable Agreements), are eligible for signing a Service Subscription Agreement for the provision of the service.

E. The Service Subscription Agreement signed with the applicant includes the statements of Applicable Agreements and adds all 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 |

# 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 public limited company Guardtime registered in Estonia. The contact information for the time-stamping service is as follows:

   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 the Best practices Time-Stamp Policy defined by [ETSI-421]. The object-identifier (OID) of the policy is: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1).

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

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

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

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

I. 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 PKI-based authentication of CHC.

J. The electronic Publications File is not meant for long-term verification.

K. 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 the time-stamp is indefinite.

B. Guardtime assures time with ±1 second of a trusted UTC time source. If a trusted UTC time source cannot be acquired or if the time in the time-stamp would differ more than 200ms from UTC, the time-stamp will not be issued.

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 publications are published periodically in a newspaper. Due to large circulation, distribution and archiving by independent parties the Publication cannot be forged.

D. The time-stamp tokens in which the CHC has not yet been extended to a Publication rely on PKI or the integrity of the 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 source code 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 turn to 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 to operate the KSI Services in accordance with Applicable Agreements and Estonian legislation.

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

C. Guardtime has 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, turn to Guardtime Privacy Policy (GT/KSI/PP).

# 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 with the particular Subscriber.

# 12. Applicable Law, Complaints and Dispute Resolution

A. The KSI Services is governed by the laws and regulations of Estonia. For applicable law, dispute resolution and complaint submission turn to 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 compliance management procedure.

B. External audits are carried out according to regulatory requirements set out by Estonian law and [eIDAS] by auditors of an independent company who holds valid certificates.

C. The conformity assessment for qualified electronic time-stamp according to Estonian law and [eIDAS] is conducted by an accredited conformity assessment body based on the requirements in the [ETSI-401] and [ETSI-421]. A review on the documentation is performed first, followed by an on-site inspection to check the implementation.

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

# 14. TSU Public Key Certificate Status Checking

A. This section and its title is suggested by [ETSI-421] standard which assumes

a time-stamping implementation where a TSU directly signs the time-stamp token with a certificate issued to this 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 (newspapers) as trust anchors for verifying the time-stamp tokens and proving that a datum existed at a time. This provides stronger proof and makes the verification independent of any parties or any secrets (private keys).

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 and have private keys for creating digital signatures securely. 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 hash to it at exactly every second and distribute the Calendar Blockchain downstream.

    c. The private key of the Core Node is used to create an RSA signature on the Calendar Hash-Chain in the time-stamp which is only used for short-term authentication of the calendar-hash chain (in the process of extending the time-stamp, this RSA signature is replaced with a full Calendar Hash-Chain and the time-stamp can be then verified using the Publication Code as trust anchor instead).

D. The corresponding public keys of the Core Nodes are made available for the verification of the aforementioned RSA signature as part of the Publications File. The Publications File is signed using a certificate issued by publicly trusted CA to the e-mail publications@guardtime.com.

E. The CRL and OCSP data included in the certificate of Publications File are

used to check that the certificate has not been revoked according to standard PKI procedure.

F. Due to the design explained above how Core and Core Nodes work and that there is one single Core, it is impossible for the Core (or the KSI Services) to issue qualified and non-qualified time-stamps in the same time.

# 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. |