guardtime

Guardtime

KSI Service Practice Statement

ID: GT/KSI/TSA/PS

Version: 3.1

Effective from: 01 April 2019

Classification: Public

Review and maintenance: Product Owner

Approved by: CEO

Contents

1. Purpose and General Terms

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

B. The purpose of this document is to provide the Subscribers and Relying Parties with the practices that Guardtime employs in providing the KSI Services. 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. A number of practices listed in this document describe or stem from Guardtime overall security policy. The intention is to recap these practices in a suitable form in order to establish trust with Subscribers and Relying Parties.

D. This document does not reiterate the statements that are available to Subscribers and Relying Parties in the KSI Service Disclosure Statement (GT/KSI/TSA/DS) unless further details are necessary to provide. In particular, please see GT/KSI/TSA/DS for the following topics:

    a. The time-stamping policy supported and the related details.

    b. The complaints and dispute resolution provisions.

E. This document is not intended to create contractual relationships between Guardtime and any other person.

2. References

2.1. Normative 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

2.2. Informative References

ID	Document
GT/KSI/DEF	KSI Definitions and Abbreviations

3. Policy and Practices Governance

A. Guardtime information security policy is established and maintained as part of its ISO/IEC 27000 based information security management system.

B. Guardtime management is committed to the information security via CEO who approves the overall information security policy as well as the trust service provider policies and practices.

C. The policies and practices are reviewed at least once a year, the role

responsible for maintenance is indicated on the cover page of the document.

D. Editorial changes (such as fixing spelling mistakes or formatting) need only to be accepted by the role responsible for maintenance and do not require official approval.

E. Policy and practice documents that are for internal use, are published on Guardtime intranet and communicated to all relevant employees. The impact of the changes defines the length of the period between publishing and effective date of the changes and if additional training is required to cope with the changes.

F. Trust service provider policy and practice documents that are public, are published on https://guardtime.com/library/tsp at least 30 days before their enforcement, unless changes are editorial. Subscribers are notified via email in case explicit actions are required on their side.

4. Compliance with Regulations

A. Guardtime's KSI Services and issued time-stamp tokens are in accordance with the requirements for qualified electronic time-stamps service as defined by [eIDAS] regulation and Estonian Electronic Identification and Trust Services for Electronic Transactions Act.

B. Personal data is acquired and processed according to the Guardtime Privacy Policy (GT/PP), GDPR regulation and national data protection laws.

C. Guardtime provides the KSI Services in a non-discriminatory manner to all potential Subscribers and Relying Parties with legal capacity. Support to disabled people is provided on a best effort basis to help them accessing the service.

D. Guardtime's KSI Services organization and information systems are in accordance with the standards [ETSI-401] and [ETSI-421].

5. Obligations of External Organizations Used

A. In delivering the KSI Services, Guardtime is outsourcing the following functions:

   a. Physical server rooms for the accomodation of Core Nodes together with reactive technical support service;

   b. Cloud services for the Aggregator and Extender servers and distribution of Publications File;

   c. Periodicals for printing and distributing the Publication Code;

   d. Electronic media for sharing the Publication Code;

   e. Internet access.

B. Guardtime retains the overall responsibility for operating the KSI Services and has written agreements with the service providers to ensure the desired level of service.

6. Provisions for the Termination of the Service

A. The decision to terminate the KSI Services is made by the board of Guardtime.

B. All Subscribers whose Service Subscription Agreement with Guardtime is in force or was in force not earlier than 1 year before the planned termination date, will be informed by email at least 2 months before the termination date.

C. The respective Estonian supervisory body will be notified at least 2 months before the termination date.

D. All other Relying Parties will be informed via public announcement on Guardtime Twitter (https://twitter.com/guardtime) account at least 2 months

before the termination date.

E. Guardtime will try to minimize the impact of the termination and enable the Subscribers and Relying Parties to verify of time-stamp tokens issued before the termination via the following means:

   a. At least one Publication is issued after the termination date.

   b. The certificate used to authenticate the Publications File will remain valid for at least 1 month after the termination date.

   c. The Extender Network will continue to distribute the calendar hash-tree until the last publication has been issued.

   d. The Subscribers can continue to run the Extender service on their KSI Gateways for at least 6 months after the date of last Publication in order to extend any time-stamp tokens.

   e. The source code of the SDKs and other tools used for verification will remain available at Guardtime Github account (https://github.com/GuardTime) for at least 1 month after the termination date.

   f. The end user documentation will remain available online for at least 1 month after the termination date.

   g. Detailed instructions will be provided regarding the actions that are required by the Subscribers and Relying Parties on their side with the notification.

F. The certificates will be revoked and private keys will be destroyed for security purposes at once when they're not used or needed anymore. Hardware security modules will be re-initialized according to the manufacturer's instructions. Other private keys or mediums used for key component storage will be destroyed physically in a manner which makes them unrecoverable.

7. Key Management Practices

7.1. Private Key Management

A. All private keys are generated and stored in FIPS 140-2 level 3 certified hardware security modules.

B. The hardware security modules are checked for tampering and malfunctioning before installation and during operations on a regular basis.

C. Private keys generated in a certain hardware security module are only used by and in this module. Private key backup and export functions are disabled.

D. The Core Nodes as well as the Publications File signing server can only have one private key and certificate active at any time.

E. Private key and certificate usage and lifetime restrictions are enforced. Expired private keys and certificates are not used, they are replaced timely and removed after key rollover procedure.

F. The lifetime of a private key associated with a public key certificate is chosen according to the validity period of the certificate. The private key must not expire later than the certificate.

G. The key pair and the certificate containing the public key for the Core Node are always created together as a whole. Never a new certificate is created for an existing key.

H. Key generation is performed in physically secured environment by 2 individuals in Trusted Roles. An audit trail in form of a signed statement is created.

I. Industry standard (NIST approved) algorithms and key parameters with conservative security reserve are used. Current recommendations:

   a. SHA-2 with 256-bit output for hashing.

   b. RSA with 2048-bit modulus for asymmetric cryptography.

c. AES with 128-bit key for symmetric cryptography.

J. Private key activation parameters like user PINs, passphrases do not hinder the availability – there should be possibility to reset user PINs/passphrases.

K. Private keys are revoked in case of:

a. disclosure or suspected disclosure;

b. loss of integrity of host system in the same security domain.

L. Before decommissioning the security module, all private keys and certificates in it are erased in a manner which makes them unrecoverable.

7.2. Public Key and Publication Code Distribution

A. The Core Node public keys as well as electronic copies of Publication Codes are distributed to Relying Parties with guaranteed integrity and authenticity enforced with clear public key certification path ending with pre-distributed public keys on Relying Party side, and appropriate key usage restrictions.

B. The validity period of the public key certificate is chosen according to the algorithms and parameters of the corresponding private key.

C. The Publication Code is published in newspapers according to a strict internal procedure, in particular:

a. At least 2 independent periodicals are used for publishing.

b. Before publishing the Publication Code is verified using two independent sources.

c. The print files are checked for correctness of the Publication Code, date, QR code and visual aspects before sending to printing.

d. A copy of the newspaper is obtained after publishing and checked for correctness. In case of any inconsistencies between Publication Code and newspaper, electronic publication is not published and the publishing process is re-started with earliest possible publishing datum.

8. Business Continuity Practices

A. Preventive measures are built into the service architecture and exploited in practice to minimize the likelihood or reduce the impact of a disaster, in particular:

   a. Core Nodes are redundant and independent.

   b. The Aggregation Network consists of clusters of redundant members.

   c. The Subscribers are distributed over the clusters of the Aggregation Network.

B. The cryptographic strength of the used and permitted hash functions is monitored in order to proactively upgrade the service infrastructure to a stronger function before the actual collisions are found and deprecate the function in the client-side libraries.

C. A yearly risk assessment is performed to update the list of threats and review the procedures for responding to the incidents and recovering the service in the business continuity plan.

D. Responding to the emergency (as defined by the business continuity plan) situations and recovering the service correspondingly is rehearsed on a regular basis. The emergency situations are:

   a. time-stamp tokens which do not conform to the specification are issued (or were issued in the past), however, the verification of such time-stamp tokens is successful (for instance time is not accurate);

   b. the service is down for majority of the Subscribers or time-stamp tokens which do not verify successfully are issued (e.g. a broken hash-chain);

   c. a critical system component has been compromised, even in case there is no impact on the overall availability and integrity of the service (e.g. compromise of private key in one of the Core Nodes).

E. Compromised or malfunctioning components of the system which can lead to issuing compromised, inaccurate or invalid time-stamp tokens are not used,

even in case it makes the entire service unavailable.

F. If the private key used for short-term authentication of the time-stamp token is compromised:

   a. The usage of the private key is halted and the corresponding public key is removed from the Publications File immediately.

   b. The compromised part of the system is reset (new key is generated) and activated once the root cause of the incident has been found and eliminated.

G. If a incorrect Publication is issued in physical media, the correction will be published as soon as possible.

H. In case the incident threatens the integrity of the time-stamp tokens or their verification, the following parties are informed within 24 hours clearly indicating the severity and scope of the incident:

   a. Supervisory Body (Information System Authority, ria@ria.ee) via email;

   b. Competent Information Security Authority (Information System Authority, ria@ria.ee) via email;

   c. Subscribers via email;

   d. Relying Parties through mass media or via email.

I. The Subscribers and Relying Parties are provided with instructions regarding the actions to be taken on their side in order to mitigate or recover from the incident.

J. A report is filed with the police regarding the incident when appropriate.

9. Audit Logging Practices

A. The audit log denotes all events that are recorded for the purpose of business continuity and providing evidence in legal proceedings, disregarding the form of collection (automated vs manual) and data format (syslog file vs text document).

B. Audit log data that is not generated by a software process, is captured and archived by the personnel in Trusted Roles.

C. All automatically recorded events contain the time of event which is obtained using a clock synchronized to UTC at least once a day.

D. The following type of events are recorded:

    a. Visits to the zone where critical system components are hosted and addition or removal of hardware and media used there.

    b. Private key generation and any following events related to its lifecycle (such as revocation or expiration).

    c. Publication Code publishing in newspapers and updates to the electronic Publications File.

    d. Core Node clock synchronization related events and alarms.

    e. Security related events from critical system components such as attempts to access systems and data, changes to configuration, exceptions and alarms at application, operating system and network level.

E. Private keys, shared keys and passwords are not captured in the records of audit log or any other type of log.

F. The audit log records are retained in archive for 10 years.

G. By default the audit log records are classified as strictly confidential and are available only to personnel in Trusted Roles. Exposing audit log records to other persons as evidence must be approved by the Security Officer.

H. The confidentiality and integrity of audit log is protected with procedural measures, e.g. by limiting access to the operating system, file-system or equivalent using role-based access control.

I. All logs produced automatically by an application or an operating system are sent to the central log server for archival.

J. Backups are created of archived audit log records on a regular basis.

K. The following event types are captured but are not considered as part of the

audit log as they have lower security requirements:

a. Technical parameters (e.g. IP-address) received from Subscribers and provided to the Subscribers (e.g. configuration file) for the provision of the service.

b. Results of vulnerability scans and penetration tests performed.

10. Access Control Practices

A. The system components used for providing the KSI Services are dedicated and separated from other systems (e.g. dedicated facility, physical server or VM). Access to the critical service components (e.g. Core, Publications File signing server) is separated from non-critical components.

B. Access to the system, both physical access and remote login, is granted only to personnel who is responsible for its operation, administration or auditing. Access to critical system components is limited to personnel in Trusted Roles.

C. Remote management and monitoring system access to all service components is secured with the following means:

a. Management and monitoring connections are encrypted and authenticated.

b. Management and monitoring connections are only allowed from whitelisted IP addresses and to relevant services that are necessary for management tasks.

D. Individual user accounts are assigned to each person with permissions limited to the operations and information required for the role and tasks of the person.

E. User accounts are removed or permissions are updated immediately after the changes to the person role or termination.

F. All user accounts are recorded and reviewed on a yearly basis to ensure that correct permissions are assigned and inactive accounts are removed.

G. Remote or local logins to the system are captured in system event log.

11. Physical and Environmental Practices

11.1. Critical Components

A. The Core Nodes and other critical system components are placed in dedicated and locked server cabinets which are co-located in secure facilities designed for data centre operation.

B. Authorized persons list for each co-location facility is updated immediately after the changes to the person role or termination.

C. SLA's are signed with the co-location service providers to ensure that the necessary physical and environmental measures are in place for the operation security, in particular:

   a. identification, authorization and logging of all visitors before allowing access to the facility;

   b. prevention and detection of any unauthorized physical access to the facility;

   c. redundant power systems for continuous power supply;

   d. redundant cooling systems for temperature and humidity control;

   e. fire and flooding early detection and mitigation systems.

D. When visiting co-location facilities:

   a. Visits to the facilities are captured in audit log.

   b. Server cabinet doors are locked and key or access card is securely stored at the security desk of the co-location facility.

   c. Addition or removal of any type of equipment must be authorized in advance by personnel in Trusted Roles and captured in audit log.

   d. Equipment must not contain storage media prior to its disposal or

reuse. Media containing sensitive information is physically destroyed or information is erased using means which make it unrecoverable.

E. The co-location facility technicians can assist with physical installation or removal of equipment or connecting cables. For each such case an explicit request must be sent by a person in Trusted Role providing the necessary instructions. The co-location facility technical support reports before beginning and after finishing the task.

11.2. Non-Critical Components

A. Non-critical components like Aggregation and Extender Network clusters and Publications File distribution are hosted using:

   a. dedicated and protected server rooms at Guardtime's facilities;

   b. cloud services (virtual private servers, content delivery network).

12. Network Practices

A. Dedicated environments are used for production, test and development in terms of network or other resources.

B. Only ports, protocols, accounts and services mandatory for providing the service are enabled.

C. System components with the same criticality are grouped into their dedicated network zone where necessary security controls are applied to all systems according to the risk assessment.

D. The Core Nodes are maintained in a high security zone which is accessible to only personnel in Trusted Roles.

E. Dedicated machines and network is used for the administration and monitoring of the service and the corresponding machines.

F. Communication between network zones is restricted to the minimum necessary for providing the service.

G. Network connections from service components to critical service

components are only allowed from whitelisted IP addresses and only to services that are necessary for operation.

H. Network connections from Subscribers and Relying Parties to service components are only allowed to access relevant services that are necessary for operation.

I. Network traffic from or to system components is authenticated. Additionally, encryption is applied when sensitive information is exchanged.

J. Core Node internet service connections are provided by multiple independent service providers with signed SLA's.

K. A quarterly vulnerability scan is performed on the private and public IP addresses of the system components by a qualified independent person not responsible for implementing the network security. Evidence of the scanning and the results is recorded in audit log.

L. Penetration tests are performed on the system and its components by an independent qualified party in case significant changes are made to the system.

M. The network firewall rules are reviewed on a quarterly basis.

13. Software Development Practices

A. A specification is formed before the implementation of any system component in order to be able to assess its own security and impact on the entire service.

B. The specifications are reviewed by security engineer, software architect, software tester, system administrator and other experts as necessary to identify the potential risks regarding security and other aspects such as backward-compatibility, performance and interoperability.

C. Backward-compatibility is ensured by versioning of the protocols and data formats and supporting the historic versions until all Subscribers and Relying Parties have had the chance to migrate to the latest version.

D. Third-party libraries are carefully selected and assessed, open source

components are preferred.

E. All source code is version controlled and follows Git workflow with different branches for latest release, latest development and individual features. Source code is always reviewed by at least one other developer.

F. Source code is covered with unit tests. In addition to manual testing, automated integration test sets are developed proportionally to the criticality of the component.

G. Releases are controlled and tracked according to a strict checklist for each role involved. Released packages are maintained in software repositories and digitally signed if feasible.

H. The users are provided with release notes or change log to communicate the changes that were made compared to the previous release.

14. Human Resources Practices

A. The following means are used to ensure that the candidate has the necessary expertise, reliability, experience and qualifications for their job before signing the employment contract: resume screening, phone screening, interview (1 on 1 or group interviews), assignment, additional competency or knowledge tests.

B. Background checks are performed on all candidates proportionally to the risks and responsibility irrespectively of the type of contract (e.g. employment, contractor, outsourcing) and following the applicable laws and regulations. Criminal convictions are checked periodically for personnel engaged in the provision of the service.

C. The identity of the employees is verified by means of their physical presence and valid legal document such as ID-card or passport.

D. Majority of the personnel has indefinite employment contract with Guardtime.

E. All employees are obligated to avoid conflicts of interest by their employment contract.

F. Conflicting duties and responsibilities are segregated.

G. The functions that are crucial for the security of the service are performed by the following Trusted Roles:

   a. KSI Security Officer - implementation of security practices, coordination of responding to emergencies.

   b. KSI Core Administrator - installation and configuration of the KSI Core system software and hardware, backup and restore activities.

   c. KSI Operator - generation and rollover of keys and other similar operations.

   d. KSI Auditor - assessing and witnessing the performance of past or on-going activities with respect to the target procedures and regulations.

H. The personnel in the Trusted Roles is provided with a job description that details the functions and responsibility of the Trusted Role before appointing the concerned person to the role.

I. The CEO appoints personnel to the KSI Security Officer trusted role. The KSI Security Officer appoints the person to the Trusted Role, requesting the person for an express written consent.

J. The person is allowed to perform the functions of the Trusted Role and get access to the related resources only after the KSI Security Officer has confirmed that all necessary checks have been successfully completed and he has received consent from the person.

K. A yearly training calendar is established for security awareness and expertise that concerns all employees and is tailored according to their function, e.g. security awareness training for all new employees, secure coding for software developers, hands-on hacking for system operators and administrators, log forensics.

L. Sanctions for violating the procedures and policies are foreseen by the employment contract and the Penal Code proportional to the severity and frequency of the violations, including termination.

15. Asset Management Practices

A. Inventory of all assets involved in providing the KSI Services is maintained, including information assets.

B. Information assets are classified and handled according to the Guardtime Information Classification and Handling Policy (GT/IS/ICHP).

16. System Operations Practices

A. Products from well-known suppliers which are protected against modifications and ensure the technical security and reliability of the processes supported by them are deployed.

B. Security patches to the products deployed are regularly reviewed and applied as appropriate.

C. Change control is used for KSI software releases and configuration files. Documentation of changes is part of the change control.

D. Integrity of systems and information used for the service is protected against viruses, malicious and unauthorized software by use of antivirus and malware protection software, signature verification of software packages obtained from trusted sources.

E. Only Trusted Roles have access to media used for critical system components. Regular backups of the data on this media are made to two separate protected locations.

F. Media containing service data is securely disposed of when no longer required, additionally no media is returned to the manufacturer for warranty replacement.

G. Capacity is monitored and resource demands projected by two monitoring systems.

H. Monitoring systems are configured to monitor and alert on critical events, including starting and stopping of system logging applications and system

resource exhaustion.

I. Monitoring and logging systems are configured to synchronize time with UTC using NTP servers.

J. Monitoring systems detect deviations from normal activities (a potential breach) and raise alarms accordingly.

K. All system logs are both stored in system locally and sent over network to central log servers.

17. Incident Management Practices

A. All incidents are reported and registered as soon as discovered. The resolution of the incidents is tracked and documented.

B. Subscribers and other external parties can submit potential incidents to technical support via support@guardtime.com.

C. Incidents are classified according to their character (e.g. denial of service attack or a key compromise) and impact (some users or entire service):

   a. Emergencies, as defined in section 8 and Business Continuity Plan (GT/KSI/BCP)

   b. Other deviations from nominal service - there is no loss of integrity or accuracy of the issued time-stamp tokens and/or service unavailability only concerns some users.

D. Emergencies are handled according to the protocol in GT/KSI/BCP, other incidents are assigned for resolving to the appropriate role or team.

E. Incidents are periodically reviewed in order to reduce similar incidents in the future and/or better respond to incidents.

Appendix A: Document Versioning

A.1. Version History

Date (MM.YYYY)	Version	Author	Changes
04.2008	1.0	Guardtime	Creation of the document
09.2018	2.0	Guardtime	Adaptation of the document to eIDAS
12.2018	3.0	Product Owner	Renamed to practice statement and major refactoring according to [ETSI-421] requirements.
01.2019	3.1	Technical Writer	Format change to be consistent with other GT documents.