GuardTime AS Timestamping Service Policy

Version 1: March 1, 2008

Effective since March 31, 2008

1. Introduction

GuardTime AS ("GuardTime") provides a timestamping service that complies with the Digital Signature Act and ensures the long-term preservation of the probative value of the timestamps.

In accordance with the Digital Signature Act the current document describes the timestamping service provided by GuardTime and presents its Timestamping Policy.

1.1. Terms and abbreviations

Newspaper means a widely distributed daily newspaper where the control publication verifying the timestamps is published periodically.

Timestamp is a data unit (token), which is created using a system of technical and organisational means, which certifies the existence of a document at a given time. See Digital Signature Act.

Extending a timestamp means a verification procedure where the verification info linked to the control publication is included in the timestamp token.

Public Key is a data token, which is used for the digital signature verification.

Control Publication means a data unit that includes a publishing date and hash of all timestamp requests received during the preceding service-provisioning period.

OID means a unique Object IDentifier. It is used to refer to the Timestamping Policy document.

Private Key is a data token, which creates the digital signature.

Hash means a cryptographic abbreviation of a data unit. See ISO/IEC 10118.

1.2. References

1.2.1. **Digital Signature Act** (RT I 2000, 26, 150; 2000, 92, 597; 2001, 56, 338; 2002, 53, 336; 2002, 61, 375; 2003, 88, 591; 2003, 88, 594; 2007, 12 66; 2007, 24, 127), https://www.riigiteataja.ee/ert/act.jsp?id=12825174 (14.03.2008)

1.2.2. Procedure for Information Systems Audit of Service Providers (RTL, 16.10.2000, 108, 1655), https://www.riigiteataja.ee/ert/act.jsp?id=83481 (01.01.2008)

1.2.3. ISO/IEC 10118: „Information technology - Security techniques - Hash-functions".

1.2.4. ISO/IEC 13335-1: „Information technology - Security techniques - Management of information and communications technology security": „Part 1: Concepts and models for information and communications technology security management".

2. Timestamping Service Provider

The timestamping service provider is GuardTime AS. GuardTime was founded in 2006 by two information security experts Märt Saarepera and Ahto Buldas. GuardTime's mission is to develop technologies that ensure the integrity of digitally archived documents.

In case of any timestamping related questions and for more information please refer to the following address (electronic channels are recommended):

GuardTime AS
Registration code: 11313216
Address: Tammsaare tee 60, 11316 Tallinn, Eesti

Phone: +372 655 5097
E-mail: info@guardtime.com
Web: www.guardtime.com

Any changes in the contact information will be announced on GuardTime's website.

All public documents related to GuardTime's timestamping service, and technical parameters needed for using the service and tools for verifying the timestamp tokens, are published on GuardTime's website.

3. Tools and devices for providing the timestamping service

The devices used to provide the timestamping service include timestamping servers, hardware security modules and hardware clock modules. Provided software is custom-made.

Distributed servers are hosted by several trustworthy service providers.

4. Timestamping and verifying

To get a timestamp, the client sends a timestamp request to the timestamping service and receives a timestamp token in return. The timestamp is issued according to the issuing procedure (p.5).

To extend the timestamp, the client or an interested third party presents an unextended timestamp to the timestamping service and receives an extended timestamp token in return. Extending is only possible after a control publication covering the timestamp has been published.

Timestamp verification is carried out without accessing the timestamping service. To verify a timestamp the relying party needs a fresh and authentic control publication.

5. Timestamp issuing procedure

Timestamps issued by GuardTime are signed with private keys that meet the following requirements:

- Key usage has enforced restrictions.
- Key has a limited validity period.
- The public key that corresponds to the key is delivered to the State Certification Registry.
- The list of valid signing keys is published within the electronic control publication.
- Key is created in a FIPS 140-2 level 3 certified hardware security module. The key is not exportable.
- Key management is carried out according to a written key management policy.

During the timestamp extension the signature created by the private key is replaced by a cryptographic code that links the timestamp to the control publication.

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

To make the automatic verification of timestamps easier, GuardTime also issues an electronic control publication with the same content as the paper-based publication. The electronic control publication is not

meant for long term archiving. GuardTime is not liable for damages caused by using and trusting incorrect electronic control publications.

6. Maintaining records of issued timestamps

The mechanism for maintaining records of issued timestamps ensures validation of the integrity and the issuer of the timestamp.

Record keeping is based on the immutable link between the timestamp and the control publication. The link can be validated with a control publication, timestamp token and in the case of an unextended timestamp also with the GuardTime database.

7. Publishing information about issued timestamps

GuardTime's timestamping service publishes the following information about the issued timestamps:

- Control publication in newspapers;
- Control publication published electronically;
- Information about how to convert unextended timestamps into extended timestamps using the extending service;
- Tools and technical description for verifying timestamps.

The information above is sufficient for verifying the timestamps effectively and securely and for ensuring their long-term probative value.

8. Timestamping service provider's responsibilities and obligations

GuardTime's responsibility to its clients is set out in the commercial service agreement. GuardTime's responsibility for parties relying on the probative value of the timestamps is set out in this document.

GuardTime ensures the publishing of the control publications and the availability of the timestamp extending service for third parties free of charge until the service is discontinued. The probative value of the extended timestamps is completely independent of GuardTime. Technical details of the availability of the extending service are published on GuardTime's website.

GuardTime checks the correctness of the control publication published in newspapers and publishes a notification in case of any errors.

GuardTime is not responsible for ensuring the probative value of the unextended timestamps after discontinuing the service or changing the private key for providing the service. GuardTime is also not responsible for archiving the issued timestamps.

GuardTime is not responsible for third party mistakes made during checking the validity of the timestamps, nor incorrect decisions and the consequences due to omission, nor the loss of probative value of the timestamps due to Force Majeure.

GuardTime issues timestamps for the State Certification Registry database according to the registry's queries.

9. Discontinuing the timestamping service

In the event of discontinuing the service, GuardTime shall announce the decision immediately to an authorized or chief employee of the State Certification Registry. The service will be discontinued according to the requirements of the Digital Signature Act p.5. After discontinuing the service the timestamps and documentation archive will be delivered to the State Certification Registry.

All private keys previously used will be destroyed. 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.

The procedure for ending contractual relationships is regulated in the associated service contracts. The clients and an authorized employee of the State Certification Registry will be informed at least two months in advance about termination of the service and possibilities of using the previously issued timestamps.

10. Contingency plans

Contingency is defined as a situation where an unauthorized party could impersonate GuardTime or the GuardTime service. As all timestamping procedures are carried out electronically, the timestamps are issued according to Article 5 and a records management system described in chapter 6, Therefore, a contingency situation could happen only as described below.

10.1 GuardTime has lost control of a private key used for issuing the timestamps

The contingency plan is as follows:

1. Leaked key or suspected leaked key is identified and the moment of the leak is specified as precisely as possible, as is the information about the affected timestamps.
2. Usage of the leaked key is halted; the compromised part of the system is isolated.
3. Key reference is removed from the electronic control publications.
4. Information about the compromise and its impact are communicated to relevant parties through mass media.
5. Information about the security breach is sent to all contractual clients' contact persons.
6. A GuardTime manager calls in a special board that identifies the causes of the security breach and its extent.
7. The cause of the security breach is eliminated.
8. The part of the system affected by the security breach is reinitialized, new keys are generated and databases are recovered from the archive.
9. Public keys corresponding to the new keys are registered with the State Certification Registry

Timestamps that were issued using the compromised key after the moment of the leak must be extended in order to regain their probative value.

10.2 A forged control publication is published in the newspapers

Contingency plan is as follows:

1. Correction will be published as soon as possible.
2. Information about the breach is sent to all contractual clients' contact persons.
3. Extending of the affected timestamps will be facilitated only after confirmation of publishing an authentic control publication; extending is arranged so that verification of the affected timestamps is possible only using an authentic control publication.
4. An incident report is filed with the Police.

11. Compliance with the service provider regulations

GuardTime's timestamping service and issued timestamp tokens are in accordance with the Digital Signature Act Articles 23 and 24 related to requirements for timestamps and the timestamping service.

GuardTime's timestamping service organization and information systems are in accordance with the Digital Signature Act Articles 25 and 26 as well as the timestamping service provider requirements in the "Procedure for Information Systems Audit of Service Providers" act.

The timestamping service runs in GuardTime's organizational and technological environment around a security policy that has been developed according to the standard ISO/IEC 13335 part 1.

The timestamp request includes the hash of the data to be timestamped. Due to the one-wayness property of the hash functions the confidentiality of the timestamped data is guaranteed.

The time value is provided with one-second precision. Any chance of backdating or forward-dating of issued timestamps is excluded because the time value in the issued timestamp token is defined by the service and the party requesting the timestamp cannot influence this value.

In case of a loss of system or data integrity, the issuing of timestamps will be halted. The issuing of timestamps will also be halted if the hardware clock module defining the time added into the timestamps differs from UTC by more than 200 milliseconds.

GuardTime only extends the timestamps exclusively issued by itself, thereby eliminating the chance of positively validating any counterfeit timestamps.

12. Audit

GuardTime's compliance with the requirements for information technology systems and organization is checked by carrying out regular internal and external audits. An internal audit is carried out at least once a year, and external audits are carried out according to regulatory requirements. The results of the external audit are published by the State Certification Registry and on GuardTime's website.

An external audit is carried out by an independent auditor that holds a valid Certified Information Systems Auditor (CISA) certificate issued by the international Information Systems Audit and Control Association.

13. Timestamping Policy management

Changes in the Timestamping Policy are documented, and a new version is marked with a version number and a unique OID in the version management section of this document.

The modified Timestamping Policy is published electronically on GuardTime's website with the effective date. The document must be published at least 30 days prior to its effective date.

GuardTime co-ordinates changes in the Timestamping Policy with the State Certification Registry.