guardtime

Guardtime

Timestamping Service Policy

Version: 2.0

Date: September 18, 2018

Approved: CEO

Review and Maintenance: CEO

1. Introduction

1.1. Guardtime AS ("Guardtime") provides a timestamping service that ensures the long-term preservation of the probative value of the timestamps.

1.2. The current document describes the timestamping service provided by Guardtime and presents its Timestamping Policy.

1.3. Terms and abbreviations

1.3.1. Timestamp is a data unit (token) created using a system of technical and organisational means to bind other data to a particular time establishing evidence that the latter data existed at that time.

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

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

1.3.4. Private key is a data token used to create digital signatures.

1.3.5. Public key is a data token used to verify digital signature.

1.3.6. Hash is a cryptographic abbreviation of a data unit.

2. Timestamping Service Provider

2.1. The timestamping service provider is Guardtime AS.

2.2. 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: A.H. Tammsaare tee 60, 11316 Tallinn, Estonia
Phone: +372 655 5097
E-mail: info@guardtime.com
Web: www.guardtime.com

2.3. Any changes in the contact information will be announced on Guardtime's website https://guardtime.com.

2.4. All public documents related to Guardtime's timestamping service are published on Guardtime's website.

3. Tools and Devices for Providing the Timestamping service

3.1. The devices used to provide the timestamping service include timestamping servers, hardware security modules and hardware clock modules. The software used to provide the service is custom-made.
3.2. Distributed servers are hosted by several trustworthy service providers.

4. Timestamping and Verifying

4.1. 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 timestamp issuing procedure.
4.2. To extend a timestamp, the client presents an unextended timestamp to the timestamping service. Extending is only possible after a control publication covering the timestamp has been published.
4.3. Timestamp verification is carried out without accessing the timestamping service. To verify a timestamp the relying party needs a fresh and authentic control publication.
4.4. Timestamps can be verified at Guardtime website: https://guardtime.com/verify

5. Timestamp Issuing Procedure

5.1. Timestamps issued by Guardtime are signed with private keys that meet the following requirements:
  5.1.1. Key usage has enforced restrictions.
  5.1.2. Key has a limited validity period.
  5.1.3. The list of valid signing keys is published within the electronic control publication.
  5.1.4. Key is created in a FIPS 140-2 level 3 certified hardware security module and is not exportable.
  5.1.5. Key management is carried out according to the Guardtime KSI Service Key Management Policy.
5.2. During the timestamp extension the signature created by the private key is replaced by a cryptographic code that links the timestamp to a control publication.

5.3. The control publications are published periodically in a newspaper. Due to large circulation, distribution and archiving by independent parties the control publication published in the newspaper cannot be forged.
5.4. 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

6.1. The mechanism for maintaining records of issued timestamps ensures validation of the integrity and the issuer of the timestamp.
6.2. 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's database.

7. Publishing Information about Issued Timestamps

7.1. Guardtime's timestamping service publishes the following information about the issued timestamps:
7.1.1. Control publication in newspapers, and Control publication published electronically.

8. Timestamping service provider's responsibilities and obligations

8.1. Guardtime's responsibility to its clients is set out in the commercial service level agreement. Guardtime's responsibility for parties relying on the probative value of the timestamps is set out in this document.
8.2. Guardtime ensures the publishing of the control publications and making them available for third parties free of charge until the service is discontinued.
8.3. Guardtime checks the correctness of the control publication published in newspapers and publishes a notification in case of any errors.
8.4. 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.

8.5. 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.

9. Discontinuing the Timestamping Service

9.1. In the event of discontinuing the service, Guardtime shall announce the decision immediately to all it's customers and the Conformity Assessment Body.

9.2. 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.

9.3. The procedure for ending contractual relationships is regulated in the associated commercial service level agreements. The customers and the Conformity Assessment Body 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

10.1. 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 the articles "Timestamp Issuing Procedure" and "Maintaining Records of Issued Timestamps". Therefore, a contingency situation could happen only as described below.

10.2. In situation where Guardtime has lost control of a private key used for issuing the timestamps:

10.2.1. 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.

10.2.2. Usage of the leaked key is halted; the compromised part of the system is isolated.

10.2.3. Key reference is removed from the electronic control publications.
10.2.4. Information about the compromise and its impact are communicated to relevant parties through mass media.
10.2.5. Information about the security breach is sent to all contractual clients' contact persons.
10.2.6. A Guardtime manager calls in a meeting that identifies the causes of the security breach and its extent.
10.2.7. The cause of the security breach is eliminated.
10.2.8. The part of the system affected by the security breach is reinitialized, new keys are generated and databases are recovered from the archive.
10.2.9. Timestamps that were issued using the compromised key after the moment of the leak must be extended in order to regain their probative value.

10.3. In situation where a forged control publication is published in the newspapers:

10.3.1. Correction will be published as soon as possible.
10.3.2. Information about the breach is sent to all contractual clients' contact persons.
10.3.3. 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.
10.3.4. An incident report is filed with the Police.

11. Compliance with the Service Provider Regulations

11.1. Guardtime's timestamping service and issued timestamp tokens are in accordance with the related to requirements for timestamps and the timestamping service.
11.2. Guardtime's timestamping service organization and information systems are in accordance to the standard ETSI EN 319 401.
11.3. The timestamping service runs in Guardtime's organizational and technological environment around a security policy that has been developed according to the standard ETSI EN 319 421.

11.4. 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.

11.5. 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.

11.6. 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 time added into the timestamps differs from UTC by more than 200 milliseconds.

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

12. Audit

12.1. Guardtime's compliance with the requirements for information technology systems and organization is checked according to Policy and compliance management procedure. External audits are carried out according to regulatory requirements.

12.2. An external audit is carried out by auditors of an independent company who hold valid certificates.

13. Timestamping Policy Management

13.1. Changes in the timestamping policy are documented, and a new version is marked with a version number in the version management section of this document.

13.2. 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.

14. Document Versioning

14.1. Version history

Date	Version	Author	Changes
04.2008	1.0	Guardtime	Creation of the document
09.2018	2.0	Guardtime	Adaptation of the document to eIDAS