guardtime

Guardtime

Timestamping Policy

ID: GT/KSI/TSA/GTSP3

Version: 1.0

OID: 1.3.6.1.4.1.27868.2.3.1

Effective from: 18 November 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 Policy

B. The object-identifier (OID) of the policy is 1.3.6.1.4.1.27868.2.3.1.

C. The purpose of this document is to define policy and security requirements for operating KSI Timestamping service.

D. This document does not reiterate the statements that are available in the KSI Service Disclosure Statement (GT/KSI/TSA/DS) and KSI Practice Statement (GT/KSI/TSA/PS).

E. 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

2.1. Normative References

Reference	Document
[eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
[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. Timestamping Policy

3.1 Adoption of ETSI-421

Guardtime is operating KSI Timestamping service by applying best operational and security practices to fulfill eIDAS requirements. ETSI-421 is adopted to the extent possible - only requirements which can not be fulfilled or are not applicable due to the different nature of KSI technology are excluded from Guardtime Timestamping Policy.

The requirements are adopted and in some cases interpreted in the context of KSI. A number of requirements of ETSI-421 are built around what is called a Time-Stamping Unit (TSU). In the context of KSI, a comparable component exists called Core Node. The main objectives of Core nodes in KSI Service are defined in KSI Service Disclosure statement. TSU requirements are adopted to Core Nodes to the extent possible.

3.2 Exclusions to ETSI-421

The following requirements of ETSI-421 are not part of Guardtime Timestamping Policy:

Section ”5.2 Identification”

The following requirement is excluded:
a) BTSP: a best practices policy for time-stamp.
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy(1)
By including this object identifier in a time-stamp, the TSA claims conformance to the identified time-stamp policy.

Reason: KSI timestamp format does not include policy identifier field. Applied policy is defined in Guardtime public web page.

Section ”7.6.4 TSU public key certificate”

The following requirement is excluded:
c) The TSU shall not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.

Reason: KSI Service does not use PKI to directly sign time-stamps.

Section “7.7.1 Time-stamp issuance”

The following requirements are excluded:

Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

Reason: KSI Service has different trust anchors and the timestamps have different format.

d) The time-stamp shall be signed using a key generated exclusively for this purpose.

Reason: KSI Service does not use PKI to directly sign time-stamps.

Section 7.14 TSA termination and termination plans

The following requirement is excluded:

a) When the TSA terminates its services, the TSA shall revoke the TSU's certificates.

Reason: KSI Service does not use PKI to directly sign time-stamps.

Appendix D: Document versioning

D.1. Version History

Date (MM.YYYY)	Version	Author	Changes
11.2019	1.0	Product Owner	New policy creation, based on ETSI-421