guardtime

JULY 2023

GUARDTIME
TIME-STAMPING POLICY

ID: GT/KSI/TSA/GTSP3
Version: 2.0
OID: 1.3.6.1.4.1.27868.2.3.2
Effective from: 23 March 2022
Next review: July 2024
Classification: Public
Review and maintenance: Product Owner
Approved by: CEO

Contents

1. Purpose and General Terms

A. This document is the GuardTime OÜ (“Guardtime”) Time-Stamping Policy.

B. The object-identifier (OID) of the policy is 1.3.6.1.4.1.27868.2.3.2.

C. The purpose of this document is to define the policy and security requirements for operating the KSI Time-stamping 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. Time-Stamping Policy

3.1. Adoption of ETSI-421

KSI is a hybrid technology, whose operations are not based on a single cryptographic key directly signing customer requests.

The system is designed to comply with eIDAS Article 42: Requirements for qualified electronic time stamps. In order to demonstrate this, the closest existing standard specifying exact policy and security requirements, ETSI EN 319 421 (referred as [ETSI-421]), is used. [ETSI-421] is created assuming a very specific, but different technology platform. Therefore, we show below which requirements are satisfied directly, and for the remaining requirements we show that the goals of these requirements are achieved by an alternative approach, offering at least an equal level of security and assurance.

The equivalent level of security is guaranteed by multiple layers: 1) data model, based on authenticated data structures and blockchains, 2) distributed computing infrastructure, 3) operational and administrative procedures. The risks are addressed at the lowest possible level, while making sure that higher levels cover all remaining issues.

3.2. Definition of Time Stamping Unit

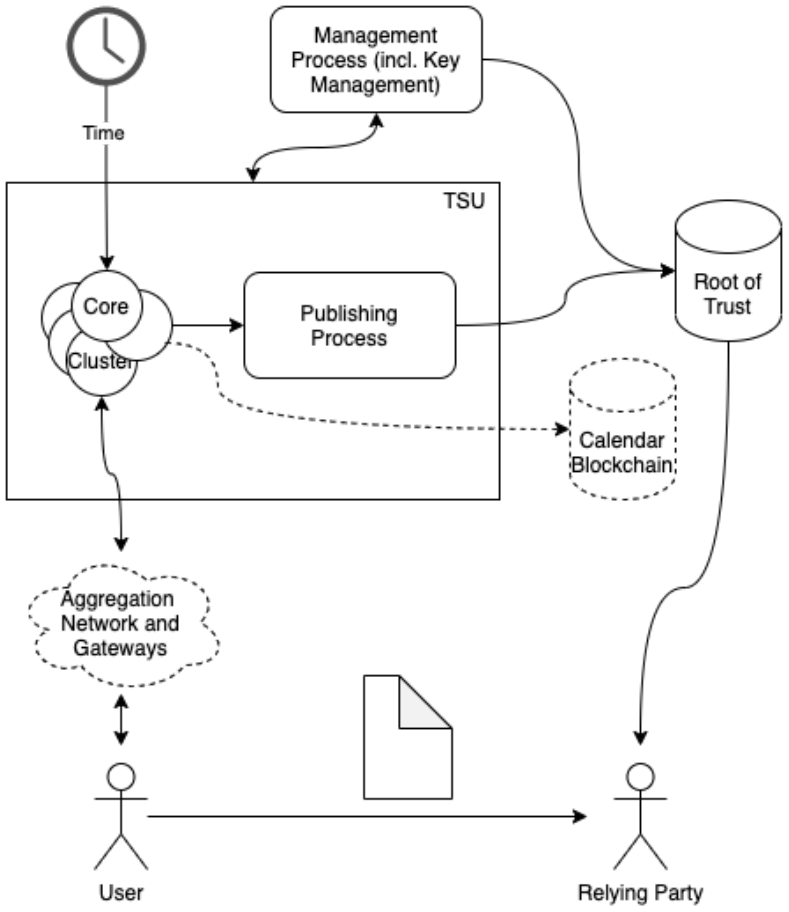

Figure 1: KSI TSU *(illustrative)*

A core concept in [ETSI-421] is Time Stamping Unit (TSU), defined as a "set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time". We look at this TSU definition as a black box and identify its interfaces with the outside world:

- Customer-facing Service Interface: time-stamping requests are accepted and time-stamps returned.
- Key Management Interface for performing administrative procedures, firstly caused by specifics of secret keys: key management as an administrative measure enforcing key lifecycle practices, mitigating risks related to the tendency of secrets to leak; and secondly caused by the

need to handle the root of trust.

- Time-source connections.

The corresponding function in KSI is the Core Cluster with the Publishing Process[1], as illustrated in Fig. 1.

We exclude all Gateways and the Aggregator and Extender network, because when ignoring scalability and separation aspects, a customer can equivalently send its time-stamping request to the Core cluster and obtain a valid response. These components are considered as external front-end for the TSU.

KSI Core Cluster is a distributed system which is deployed across multiple datacenters. One single site in isolation cannot serve customer requests. In order to create time-stamps, it is necessary to establish consensus between Core Nodes. Therefore, the Core Cluster must be treated as a whole.

For procedure-level compatibility with the Key Management Interface above, we include the Publishing Process into TSU definition. Publications File Signing Key and Certificate look and feel like [ETSI-421]'s "time-stamp signing key". We note that the significance and risk profiles of these keys are not directly comparable. Publications File Signing Key is used once per month; time-stamp verification uses fresh signatures, and there are fall-back procedures for verification without Publications File (not subject to TSA Accreditation, it is a "next level safety net").

KSI TSU has one additional interface with the outside world: it produces the Calendar Blockchain, a cryptographically secured and widely distributed output-only data stream. In the context of this Policy and TSA accreditation, this interface is an internal function of the TSU. There are no other public interfaces.

KSI TSU employs hash functions and asymmetric cryptography internally. Related keys are not part of a public PKI. Signatures created by these keys are used in the short term for establishing chain-of-trust, while the next Publication Code is not yet available. External parties do not have interfaces to access these keys. Nevertheless, these keys are managed according to [ETSI-421] chapter 7.6, excluding clause 7.6.4.

[1] Please refer to GT/KSI/DEF for definitions.

3.3. Applicability to Verification Process

The data structures involved are more complicated than ones assumed by [ETSI-421] and specified in [RFC 3161]. Accordingly, the verification procedure performed by Relying Parties when validating KSI time-stamps is more elaborate. Relying Party may choose from a range of Verification Policies to customize the process, based on concrete circumstances, for example: risk profile, network connectivity, available root of trust, and the age of time-stamp.

TSA Accreditation applies only to specifically listed Verification Policies if an appropriately authenticated trust anchor is used. The Default Verification Policy, recommended for general use and chosen by default, is one of the Accredited Policies[2].

3.4. Conformance to ETSI-421

The following requirements of [ETSI-421] are adapted to the Guardtime Time-Stamping Policy:

Section ”5.2 Identification”

The following requirement is implemented non-explicitly:

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 time-stamping service is not differentiated using multiple time-stamping policies, therefore meta-data does not include the policy identifier field. Applied policy is defined uniquely in Guardtime public web page.

[2] Verification Policies and additional requirements are elaborated in KSI Service Disclosure Statement [GT/KSI/TSA/DS].

Section ”7.7.1 Time-stamp issuance”

The following requirements are not directly applicable:

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

Reason: KSI time-stamps do not have [RFC3161] format, thus can not be based on a profile of it.

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

Reason: KSI Service does not use public-key cryptography to directly sign time-stamps.

Equivalent Control: According to internal policy, “strict key usage restrictions must be applied”. This is a more general rule, applying to all involved keys.

e) The time-stamp generation system shall reject any attempt to issue time-stamps when the end of the validity of the TSU private key has been reached.

Reason: Time-stamps are not signed directly.

Equivalent Control: It is not possible to sign a Publications File with expired key, and TSU internal keys are not used when expired. TSU as a whole continues to operate due to redundancy.

Section ”7.14 TSA termination and termination plans”

The following requirement is re-interpreted:

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. Not revoking Publications File Signing Certificate supports relying parties by allowing them to verify time-stamps after termination of the service. This does not incur the risk

of unauthorized issuance of time-stamps. Private keys are destroyed when TSA terminates its services ([GT/KSI/TSA/PS], Provisions for the Termination of the Service).

Equivalent Control: KSI Time-stamping service is designed specifically for a very long validity period of generated time-stamps. The security of time-stamps extends far beyond the life-time of involved keys and certificates. Destruction of private key material and shutting down the Core Cluster makes issuance of new time-stamps impossible, which satisfies the meaning of this clause.

Section ”8.2 TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014”

Clarification: Guardtime uses only one TSU and all issued time-stamps are qualified time-stamps, if validated appropriately (see [GT/KSI/TSA/DS], section 6, clause H). Guardtime does not exclude other validation methods which may be chosen at the discretion of the relying party. Due to the expected long lifetime of KSI time-stamps, such flexibility and diversification mitigates some cryptography-related risks.

Appendix A: Document Versioning and Review History

Date (MM.YYYY)	Version	Author	Changes
11.2019	1.0	Product Owner	New policy creation, based on ETSI-421
04.2020	1.1	Product Owner	Company legal form change (Guardtime AS -> Guardtime OÜ)
08.2021	2.0	KSI Operator	Explicit definition of TSU and elaborated relationship with eIDAS and [ETSI-421].
07.2023	2.0	Product Owner	Annual review, no changes.