guardtime

JANUARY 2021

Guardtime

KSI Definitions and Abbreviations

ID: GT/KSI/DEF
Version: 1.1
Effective from: 18 February 2021
Next review: January 2022
Classification: Public
Review and maintenance: Technical Writer
Approved by: Product Owner

Contents

1. Purpose

A. The abbreviations and definitions listed in the current document are to be used in various policies, procedure descriptions, agreements, and other similar documents related to KSI.

B. If abbreviations and/or definitions given here are used in some document, this KSI Definitions and Abbreviations document must be listed as Informative Reference and added to the documents set provided to the interested party.

2. Abbreviations

Abbreviation	Meaning
AHC	Aggregation Hash-Chain
CA	Certificate Authority
CHC	Calendar Hash-Chain
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
TSA	Time-Stamping Authority
TST	Time-Stamp

TSU	Time-Stamping Unit

3. Definitions

Term	Definition
Aggregation Hash-Chain	A hash chain where the input hash is the hash of the user data and the output hash is the root of the Global Aggregation Tree.
Aggregation Network	A tiered network of hierarchically connected Aggregators that perform Aggregation in order to build the Global Aggregation Tree from the input hashes of the signed documents.
Aggregator	A KSI service (server) whose function is to aggregate hashes received from its lower-level Aggregators or user applications into a hash-tree and send the root hash to its upper-level Aggregator.
Calendar Blockchain	A hash tree where each leaf corresponds to one second since 1970-01-01 00:00:00 UTC till present moment and the value of each leaf is the root hash of the Global Aggregation Tree. Data is never removed, only appended to Calendar Blockchain, one hash value per second.
Calendar Hash-Chain	A hash chain where the input hash is the root hash of the Global Aggregation Tree that corresponds to a specific second and the output hash is a root hash of the Calendar Blockchain.
Core (Cluster)	A cluster of servers (Core Nodes) whose role is to reliably maintain the Calendar Blockchain.
Extender	A KSI service (server) whose function is to distribute the Calendar Blockchain received from Core or upper-level Extenders to lower-level Extenders. The Extender in KSI Gateway provides the service for user applications to extend KSI Signatures.
Extender Network	A tiered network of hierarchically connected Extenders that distribute Calendar Blockchain from Core to users' KSI Gateways.
Global	A hash tree that is formed globally once every second from all user

Aggregation Tree	hashes requests and whose root hash is registered in the Calendar Blockchain.
Guardtime Software	Software programs and components (whether in source or object code form), including without limitation any associated or embedded documentation or printed materials, provided or made available by Guardtime.
Hardware Security Module	A physical device that safeguards private keys. Hardware Security Module stores private keys of Core Node and Secure Signature Creation Device (SSCD) certificates. Hardware Security Module is either: 1) cryptographic module certified and operated at least at FIPS 140-2 level 3; or 2) device certified at least at CC EAL 4+ level to conform to PP-SSCD-KG protection profile [EN-14169-2].
Intellectual Property Rights	Any patent rights, copyright, trade secret rights, trademark rights (including rights in trade names, trade dress, service marks, URLs or other source of business identifiers), rights in industrial property and industrial designs, moral rights and all other intellectual property or proprietary rights arising under the laws of any jurisdiction worldwide, including all rights or causes of action for infringement or misappropriation of any of the foregoing, and all rights in any registrations, applications, renewals, extensions, continuations, continuations-in-part, divisions or reissues for any of the foregoing.
KSI Gateway	A server running KSI Aggregator and Extender where the user applications connect to for consumption of KSI Services .
KSI Services	Online services designed by Guardtime; made available by Guardtime, its partners or Guardtime Affiliates; intended for issuing, extending and electronically verifying KSI Signatures for the purpose of proof of data integrity and time or other applications utilising said KSI Signatures.
KSI Signature	A cryptographic digital proof issued by KSI Services that contains everything needed to prove data integrity and time of signing using a widely witnessed trust anchor.
KSI Time-Stamp	A KSI Signature that serves as a qualified electronic time stamp in the context of the eIDAS regulation, respective ETSI standards and Guardtime Timestamping Policy.

Publication	Publishing of the root hash value and corresponding time of the Calendar Blockchain in a widely-witnessed way such as printing in newspapers and publishing on electronic media in order to make backdating or denying impossible.
Publication String (Code)	The Publication String (sometimes also called Publication Code) is a textual representation of the publication data (Calendar Blockchain root hash value and metainfo).
Publications File	A file containing all the Publications. It also contains PKI public keys needed for short-term key-based verification.
Relying Party	Legal or natural person who relies on the verification of KSI Signatures.
Subscriber	Legal or natural person who has KSI Service Subscription Agreement with Guardtime for the provision of KSI Services.
Trusted Role	A role that is engaged in administering or operating the Core Cluster or performs other activities which are in the same class of security.
Update	New version of the KSI Service or Software that is released for the purpose of bug fixes, enhancements or other modifications.

Appendix A: Document Versioning and Review History

Date (MM.YYYY)	Version	Author	Changes
01.2019	1.0	Technical Writer	First draft.
02.2019	1.0	Product Owner	Enhancements during refactoring the documentation set.
11.2019	1.0	Product Owner	Updated KSI Timestamp definition (added reference to KSI Timestamping policy)
01.2021	1.1	Technical Writer	Added HSM abbreviation and Hardware Security Module definition. Added next review date on the title page and removed Appendix A.2 “Review Control” table.