guardtime

MAY 2022

GUARDTIME KSI DEFINITIONS AND ABBREVIATIONS

ID: GT/KSI/DEF
Version: 1.3
Effective from: 4 July 2022
Next review: May 2023
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
CAR	Calendar Authentication Record
CHC	Calendar Hash-Chain
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module. See exact definition for the KSI context in *Definitions* table below.
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device or Qualified Seal Creation Device, see exact definition for the KSI context in *Definitions* table below.
TSA	Time-Stamping Authority
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. Part of KSI Time-stamp.
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 Authentication Record	A Record with data which authenticates the root of CHC. A digital signature if time-stamp is not extended; a Publication Code and a list of publication references if time-stamp is extended. Part of KSI Time-stamp.
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. Part of KSI Time-stamp.
Core (Cluster)	A cluster of servers (Core Nodes) whose role is to collectively reach agreement on the root of AHC for every round, synchronized to UTC; produce, retain and distribute new blocks for the Calendar Blockchain.
Extender	A KSI service (server) whose function is to distribute the Calendar Blockchain received from Core Nodes 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 Aggregation Tree	A hash tree that is formed globally once every second from all user 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 (HSM)	A physical device that safeguards private keys. An HSM must have at least one of the following certifications: • FIPS 140-2, Level 3 (or higher); • ISO/IEC 19790, Level 3 (or higher); • EAL4 (or higher) of the CWA 14169 or EN 14169 Protection Profile under the Common Criteria (ISO/IEC 15408) framework.
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 utilizing 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 and validated identity of responsible end-entity.
KSI Time-stamp	A cryptographic digital proof issued by KSI Services that contains everything needed to prove data integrity and time of time-stamping. KSI Time-stamp is valid and issued by a Qualified Time-stamping Service Provider, as defined by the eIDAS regulation, when verified in accordance with the rules specified in [GT/KSI/TSA/DS].

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 Code	The Publication Code is a textual representation of the publication data (a time, Calendar Blockchain root hash value at this time, and a checksum). A Publication Code authenticates the entire history of Calendar Blockchain, and all KSI Time-stamps issued before the Publication Code.
Publications File	A file containing all the Publications and a list of Publication References for each. It also contains a whitelist of keys for validating CAR in non-extended time-stamps. Publication file is sealed with a qualified seal certificate.
Publishing Process	A periodic process for generating Publication Codes and updating the Publications File; and publishing them in Widely Witnessed Media (newspapers, social media) and electronically.
Qualified Seal Creation Device (QSCD)	A physical device classified as QSealCD by either: • Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014; • Information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014; colloquially referred to as the EU SSCD List, compiled at: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD
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	KSI Auditor & 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.
04.2021	1.2	KSI Auditor	Added QSCD abbreviation and Qualified Seal Creation Device definition. Specified Hardware Security Module definition.
05.2022	1.3	KSI Auditor	Added Calendar Authentication Record abbreviation and definition. More detailed explanation of Core (Cluster), KSI Signature, KSI Time-stamp, Publication Code and Publications file. Addition of Publication Process definition.