Keyless Signature Infrastructure® (KSI™) Technology

An Introduction to KSI Blockchain Technology and Its Benefits

Executive Summary

The use of blockchain technology to provide digital integrity has exploded in financial applications. Widely proliferated blockchain technology consumes significant storage, communications bandwidth and time for each transaction, whereas Guardtime-Federal, LLC provides Keyless Signature Infrastructure (KSI) that is a blockchain designed for security, scalability and speed. Through the properties of verifiable authenticity, identity of the client, and non-global positioning system-based non-spoofable time; KSI provides provenance, integrity and identity associated with digital assets. This implementation consumes far less storage and bandwidth than widely proliferated blockchain technology and can provide the above defined attributes for thousands of files a second scalable to billions. KSI cryptographically links data assets with immutable properties provided by the KSI infrastructure, and implemented in a KSI signature. KSI promises this additional integrity and authenticity in newly created or already existing data whether on the network, in embedded systems or traversing the cloud. Customers who implement KSI can prove their current and future information systems are in a truthful state and meet business and mission needs with increased security. KSI was designed with considerations for security, scalability, and speed to meet the requirements for a host of complex applications.

By integrating KSI into healthcare systems, irrespective of where a digital asset is transmitted or stored, every component, configuration, and digital health record/entry generated by humans or machines can be verified independently in real-time, independent of trusted administrators. KSI provides a truth-based system wherein the need for trust can be completely eliminated.

Guardtime Federal, LLC is a small technology company that makes KSI available to the US Federal ecosystem. With KSI, digital assets and their provenance can be authenticated in real-time, anywhere in the world, independent of the service provider. KSI signatures are portable, literally become part of the digital asset, and are used to provide proof of time, identity and authenticity. Verification of digital signature at a future time provides evidence of its integrity.

Introduction

This paper is divided into three sections. First, the paper will provide a basic description of KSI technology. This description will include an explanation of the logical and mathematical processes as well and the security infrastructure necessary to offer the capability in a fashion that assures integrity of the process. Second, the paper will provide a discussion of how this implementation differs from other blockchain approaches. Finally, the last section will propose examples of how KSI may be useful for healthcare and healthcare-related research. This section will address how KSI can be used to assure integrity of patient records, compliance of personally identifiable information protection standards, provide tamper resistance of telehealth care information, impart authenticity verification into clinical trials reliability, and in healthcare fraud detection and prevention.

Keyless Signature Infrastructure® (KSI™) Technology

Keyless Signature Infrastructure (KSI) technology was initially developed in 2007 with the goal to impart a tag on any digital file that would forever be effective in determining its authenticity. Exploiting a mathematically derived artifact of a file called a hash along with the hashes of other files created in the same time increment, and combining them in a mathematically known manner called a hash tree or a Merkle Tree accomplish this. This process cryptographically links all the artifacts of the files created or modified in that time increment and creates a top root hash that can be used in a proof that shows the contribution of every file. Once this top root hash is determined, it is then combined with the top root hashes from previous time increments in a hash calendar. Combination of all the artifacts for a particular instant in time can be summarized on a publication code. The steps taken in the mathematical sequence of combining the hashes is well-defined and repeatable. The process and path used to move from initial hash to the publication code is defined in a unique digital KSI signature (approximately 2 kilobytes). In this implementation the artifacts from the files in the current time increment are cryptographically linked to all the artifacts of files brought into these processes since it was initiated and a summary is provided in the publication code. This is one instantiation of what has been called a blockchain.

To verify the authenticity of any digital file, one must have the file under test. With the hash of the file under test and the signature attributed to the original file, verification is accomplished by using the hash of the file under test as the starting hash and processing it through the Merkle Tree with the data from the original signature and comparing the result to the publication code. There is no mystery to the approach, no puzzles to be discovered, the process follows the published KSI process (the Merkle Tree) using the KSI signature and comparing the result to a published result. If the process generates the same publication code, it is identical to the original file. If it does not, then it is a forgery or an altered version.

The top root hashes of every time increment are stored in the KSI infrastructure such that it is always available for verifying signatures. This storage scales at approximately 2 gigabytes per year, scaling with time, not with number of items signed or processed.

Note that a hash is a one-way function such that a file can be hashed but there is no mathematical process that allows one to re-create the file from a hash. Once the initial file is hashed, all other processes have no insight into the content of the original file and the file content is not widely distributed. Only the hashed artifacts of the file are widely distributed. This enables anyone to verify the contribution of a hash at a point in time without having to be exposed to the potentially sensitive data in the original file (e.g., personal medical data).

The information derived from a KSI signature means the asset's chain-of-custody information (pedigree), creation time, and authenticity information remains undisputable and is subsequently verified as truth without trusting or solely relying upon an administrator or a shared secret (such as a key or Public Key Infrastructure (PKI) credential). Instead, KSI uses a 'proof-based' method to accomplish authentication and our signature is portable across any computing platform. KSI signatures are based on mathematical proofs and keyless cryptographic functions approved by the European Union (EU) and National Institute of Standards (NIST).

KSI addresses the need to prove data integrity and detect changes in data authenticity at rest and in motion. It is a blockchain technology, which provides massive scale data authentication without reliance on centralized trust authorities.

KSI forms a unique calendar hash chain (CHC) that is a distributed database across the infrastructure. Records can only be added to the database, never removed, with each new record cryptographically linked to all previous records in time. New records can only be added based on synchronous agreement or 'distributed consensus' of the parties maintaining the database. Since records are cryptographically linked, it is impossible for one party to manipulate previous records without breaking the overall consistency of the database.

1. Blockchain Meets Security

KSI is designed to provide secure, scalable, digital, signature-based authentication for electronic data, machines and personal information. Unlike traditional approaches that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of the history of cryptologically linked root hashes (the blockchain).

The KSI blockchain overcomes two of the major weaknesses of traditional blockchains, speed and storage capacity, making it usable at industrial scale. One of the most significant challenges with traditional blockchain approaches is scalability; typically they grow linearly with the number of transactions. In contrast the KSI blockchain scales temporally; it grows linearly with time and independent from the number of transactions. The second significant challenge is time to record an individual transaction. Some refer to this as settlement time for a large number of nodes to witness a transaction often taking many minutes to complete a transaction. In contrast KSI has a straightforward mathematical process that provides signatures on the order of one second, that is once a second generating signature for thousands of client requests.

The KSI approach to implementing digital integrity is to provide a secure infrastructure consisting of cores, aggregators, and gateways to create keyless signatures. This infrastructure runs on our Black Lantern Security Appliances that is an integrated hardware and software platform purposely built to mitigate both remote and physical attacks against your infrastructure and applications. It is intended to be installed within the customer perimeter providing KSI service access at the client level. The security appliance comes with a built-in KSI gateway, which allows for secure implementation of KSI-based data assurance and cybersecurity solutions with built-in active anti-tamper measures. Black Lantern uses the National Information Assurance Product (NIAP) certified Green Hills Integrity Real-Time Operating System. When combined with advanced Application Specific Integrated Circuits (ASICs) with inherent tamper protection features and escalating reaction monitors, it provides significant protection against a variety of attack vectors.

2. The KSI Infrastructure

The KSI infrastructure consists of a distributed network of Black Lantern Security Appliances configured as cores, aggregators, and gateways. The first layer of aggregation servers are the gateways which are responsible for collecting and processing requests from clients and then sending the aggregate request to the upstream server. The gateway is the customer facing component of the infrastructure and delivers KSI services to the clients.

The network aggregates the hash values and distributes the signatures. Each aggregation server processes requests from the servers below it, adds them to a hash tree and sends the local root hash to the next higher-level server. The hierarchy of aggregation servers creates the global hash tree for each round. The verification network (a part of the aggregation network) provides widely witnessed access to the state of the calendar and the history of root hashes used in the verification solutions.

The core cluster operates a distributed state machine which sits at the top of the aggregation network and manages the calendar. It calculates the top root hash at one-second intervals (a round) and votes upon (through distributed consensus) and promotes the top root hash to the CHC. The core is responsible for agreeing upon the top root hash for each aggregation period, which it then stores in the calendar database, and returns the result to the aggregation network. The regularly spaced rounds used in the aggregation and core processes produce an accurate measure of time, which is embedded into the KSI signature.

3. The Value of KSI

Digital data signed by a KSI signature is cryptographically linked to the data. Digital data of any format, protocol, or size can be signed. The data's signature is preserved in the calendar blockchain, which provides longevity and becomes an irrefutable record available to the public for verification. KSI signatures provide proof of signing time, proof of signing entity, and data integrity. The signature of the data will now be available in perpetuity, unlike a PKI-based digital signature. If a private PKI key or certificate is compromised, the PKI digital signature must now be revoked. A KSI signature cannot be revoked and does not need to be. KSI can be used in conjunction with PKI as desired to protect the longevity of PKI certificates. KSI in intended to protect integrity of an asset while PKI is intended to protect its confidentiality. These are different attributes. In the specific example of medical records, loss of confidentiality may results in embarrassment while the loss of integrity may result in the loss of life from the administration of healthcare based on incorrect information. Both have their purpose.

A signing participant uses the Software Development Kit (SDK) on a client machine and submits a signing request to the gateway. This process is transparent to the participant. The hash of the data requested to be signed is forwarded up the stack to the aggregator and core and creates evidence the signature participates in the blockchain. The signature is returned to the client for storage or forwarding of the signature to another participant. A participant is now able to independently verify the KSI signature using the verification infrastructure in the KSI stack. Since the KSI signature is part of the CHC, it can be validated at any time in the future through the KSI extension services.

KSI Compared to other Blockchain Approaches

KSI offers the opportunity to enhance mission assurance in a variety of domains that have been classically described as a three-legged stool of availability, confidentiality and integrity; few have stressed integrity. While most have used encryption and confidentiality to assume integrity, KSI and other users of blockchains, such as Bitcoin, rely on a different mechanism.

Bitcoin blockchain users rely on distributed consensus; a transaction is only complete once a sufficient number of participants (miners) have entered the transaction into a public ledger of transactions (block-chain). Once complete anyone, anywhere can verify the integrity of a

transaction without reliance on a centralized authority. It is (most likely) provably secure based on two assumptions, the security of hash functions and the availability of the widely distributed ledger. Bitcoin pushes the contents of a transaction into the ledger to document a transaction. This is necessary as participants need to see the full transaction in order to ensure the transaction is valid, i.e., the ownership is correct and to prevent "double spending." The downside of this is the transaction contents must necessarily be made public which dramatically increases the size of the ledger, i.e., the ledger size scales linearly with the number of transactions. A second downside is the mining process in which participants must solve a mathematical puzzle known as "proof of work" which can take many minutes to solve.

KSI was patented two years before Bitcoin came on the scene. KSI is focused more on integrity of processes, supply chains and the authenticity of digital data. KSI does not expose client data to a large number of entities, client data never leaves client possession. A KSI client submits a unique artifact of their data, a hash (SHA 256 or SHA 3 currently supported), through a Merkle Tree that passes the identity of the requester from known credentialed permissions, and from the path through the infrastructure (known location and path identity), to the ledger once per second to integrate the unique artifact, time (via a hash calendar) and identity creating a 2-3Kbyte signature cryptographically linking the underlying data. At any future time, the original data and associated signature can verify that the data was part of the published calendar and therefore it existed in the original form at that time identified in the signature. These signatures can be processed at a rate of billions per second, sufficient to cover all the data generated in the world within one second.

With the above information, one can easily compare Bitcoin and KSI. Both processes rely on some form of widely witnessing without reliance on a centralized authority. Bitcoin exposes transaction content to the world whereas KSI protects client data, only exposing an irreversible hash value to anyone wishing to inspect it or validate authenticity. Bitcoin requires minutes to process one transaction; KSI can process billions per second. The KSI ledger scales at a constant rate of approximately 2GB per year; the Bitcoin ledger grows with the number of transactions and is already on the order of 20-30GB. While relying on similar principles as Bitcoin, KSI makes events widely witnessed without exposing confidential data allowing integrity of events, programs and configurations to be verified without reliance on burdensome infrastructure for secure keys.

KSI Blockchain Use Cases for Healthcare

KSI has numerous areas of application in the National Healthcare Arena. As stated above, loss of integrity in medical records could result in the loss of life from the administration of healthcare based on incorrect information. This assertion leads one to the conclusion that verifiable integrity of medical records is of paramount importance. KSI is specifically designed to impart authenticity and enable the verification of integrity of files and is therefore well suited for health and healthcare related applications.

With the KSI ability to sign digital content with minimal processing and storage requirements, we are able to validate the integrity of any digital record, for example, a prescription, database entry, or information system (IT) log entry, and determine its authenticity or a change in its authenticity. The value of blockchain to the health-care system is recognized through

establishing integrity of the data and health care records, providing auditability and transparency of these records over a distributed system, and maintaining the integrity through forensic quality auditing for the life of the record.

The following notional examples with health and healthcare research applications are provided:

1. Patient Records Integrity

   In an emergency, the difference between A and B blood type is life and death. KSI blockchain instrumentation enables users of the Electronic Health Records (EHR) system to be 100% certain of the accuracy of all retrieved records. We provide rapid deployment to complement existing EHR systems (Epic, Philips, General Electric, Carestream, Oracle, etc.)

2. Personally Identifying Information (PII) Compliance

   Healthcare Service Providers are required to ensure and prove their compliance with PII privacy clauses of various regulations. Black Lantern application server hardware with active anti-tamper capabilities enables you to protect PII against advanced persistent threats and insider threat actors while the data is being processed and stored. KSI blockchain enables an organization to tag, track and locate PII and its usage in real time.

3. Telehealth care Assurance

   Telehealth care can improve healthcare efficiency, availability, convenience and outcomes, but it presents new challenges in informed patient consent, practitioner credentialing and in malpractice liability. KSI blockchain is deployed for a complete, tamper-evident, end-to-end audit trail, to independently trace who did what and when, and the technology can be applied to video, audio and written communication recordings and logs.

4. Clinical Trials Reliability and Robustness

   Clinical trials reliability and robustness enables end-to-end assurance and proof of clinical trial data adhering to the Good Clinical Practice Directive 2005/28/EC, upcoming EU Regulation No 536/2014 and other regulations calling out for “reliable and robust data”. KSI can be deployed to complement existing collaboration and document management systems (SharePoint, Documentum, etc.), and provides means to discover and combat in-house clinical trial data tampering.

5. Healthcare Fraud Detection

   According to the Centers for Medicare and Medicaid Services, 5.8 percent of all Medicaid payments made in fiscal year 2013 were improper, representing $14.4 billion in Federal expenditures. KSI blockchain enables you to independently track and validate prescriptions and Medicaid payments through organizational and geographic boundaries.

Recognizing KSI’s unique characteristics, the Healthcare Industry can realize many business enterprise applications to enhance the mutual auditability of their cloud, development, and mobile platforms. Mutually auditable systems ensure that auditors/investigators have a preserved forensic state of the original system (or in this case data-at-rest reliability) from which to conduct a review or investigation.

KSI in Healthcare Demonstrated Performance

Guardtime KSI technology has demonstrated performance in an applicable environment at a national scale. The international parent of Guardtime Federal is Guardtime. Guardtime was founded in 2007, in Estonia, and a key product is assuring the digital integrity of the records used in the e-Goverment of Estonia or e-Estonia. The X-Road project is the backbone of e-Estonia. In this application all government records are signed with KSI signatures and this includes the national health care system. The Estonian health care system retrieves a variety of data products from different health care providers to enable any authorized facility to access patient records and other time critical information when care is needed. The national level of the program enables the application of big data analytics to assess trends and project resource needs.

This deployment of KSI in X-Roads, e-Estonia and the Estonian health care system enables individuals, their families and health care providers access to electronic health information in a secure, timely and reliable manner to support the health and wellness of individuals through informed, shared decision-making. Individuals and caregivers are enabled to participate in their health and care. The demonstrated example of KSI deployment in e-Estonia and the Estonian health care system suggests the ability of a potential KSI deployment in the US would meet the objectives of a system capable of exchanging electronic health information in a manner consistent with the objectives of the Nationwide Interoperability Roadmap. Given the demonstrated deployment in Estonia, deployment in the US should be low risk.

Since KSI has been demonstrated at the scale of a small nation, and since the KSI infrastructure readily scales to Internet level deployments, there is no reason to presume there is a gap in the application of the technology. Upon a decision to deploy, the KSI software development kit (SDK) would be exercised to integrate with existing health care community databases and tools to expose the data and effectively sign the desired elements. The degree to which integration is required would drive the number of software add-ons or program modifications. While these are all low risk the time required would scale with the number of interfaces. Infrastructure risk is also low, as it has already been demonstrated in Europe. Further, Guardtime Federal is investing in infrastructure in data centers across the US such that KSI will be available as a service accessible via the Internet for heath care applications.

Conclusion

There is no other sector where corruption-free data matters more than in Healthcare/Healthcare IT. Guardtime Federal's KSI Blockchain-based data integrity and assurance capabilities can be deployed to complement existing healthcare solutions, not to replace them, thus making implementation affordable. The value of KSI digital signatures is how it is applied to a customer's problem. Any type, format, or size of data can be signed and its integrity documented for use. This capability allows KSI to directly link to the Nationwide Interoperability Roadmap and healthcare related objectives. The KSI signing and verification process currently in use today, is scalable and controlled and easily integrated in systems for interoperability. The infrastructure using Black Lantern Security Appliances provides security from many threats (cyber and physical attack vectors) to offer non-repudiation, proof of integrity, irrefutable identity, irrefutable event time, longevity, and pedigree. This characteristic can be used to mitigate or prevent insider threats, fraud, or unwanted data loss. Some healthcare related use cases have already been developed and can demonstrate how to provide integrity for event logging, software authenticity, and data transactions. This leads to many opportunities for auditing, monitoring, configuration management, change detection and reporting on the integrity of data in development processes, engineering, operations, and maintenance of many systems in commercial, military, and healthcare markets.

Summary

Given the national mandate for preservation of life and assuring the highest quality of life, high quality health care has a strong demand for integrity of records. The loss of integrity in medical records could result in the loss of life from the administration of healthcare based on incorrect information. This assertion leads one to the conclusion that verifiable integrity of medical records is of paramount importance. This paper provides a case for using KSI Blockchain Technology for healthcare and health-related research. In the first of three sections, the paper provided a basic description of KSI technology describing the logical and mathematical processes as well as the security infrastructure necessary to offer the capability in a fashion that assures integrity of the process. The second section of the paper provided a discussion of how this implementation differs from other blockchain approaches. Finally, the last section proposed examples of how KSI may be useful for healthcare and healthcare-related research. This section addressed how KSI can be used to assure integrity of patient records, compliance of PII protection standards, provide tamper resistance of telehealth care information, impart authenticity verification into clinical trials reliability, and in healthcare fraud detection and prevention.