guardtime FEDERAL

Keyless Signature Infrastructure (KSI): Blockchain Technology for the Defense Industry

Kevin Zawicki
Director, Customer Solutions

16 Aug 2018

guardtime FEDERAL

Let’s start with an Example System: the JSF F-35

- Hardware production:
  - 1 Prime Contractor
  - <10 major suppliers
  - 10s of Ks of total suppliers
- Software:
  - 10s of systems
  - >>1M lines of code
  - >50 software suppliers
- Logistics:
  - >3000 individual aircraft
  - 3 variants
  - >10 countries

- Other Considerations:
  - Mission Planning and Data Files
    - A/C readiness
    - Software verification
    - Mission Planning and Authorization
  - Post-mission Data
  - Maintenance and Equipment Log Books
  - >5 Security Classifications (US)

guardtime FEDERAL

Cross Domain Enterprise Resource Management

Government Program Office

Prime Contractor

Other Government Offices

Physical and Logical Suppliers	Distribution	Production	End User	Information Suppliers
Contract Task 1 Task 2 Task 3 Task 4	Shipping Land Sea Air	Process Step 1 Step 2 Step 3 Step 4	Systems Operations Sortie Rate MTBF Use Rate Spares	Information Agreements Data 1 Data 2 Data 3 Data 4
Task 1 Task 2 Task 3 Task 4		Step 1 Step 2 Step 3 Step 4	People kkk Machines mmm Parts nnnn	Maps Currency 1/14/16 ATO Within 24 hrs Msn Data 4 X BDU- X Refueling Point Alpha
What is the status of my off-premise supplier deliverables?	Where in the world are my parts in shipment?	What is the status of my on-premise parts in production work flow?	Can I accomplish my intended mission?	Do I have the correct information?

Tracking of compliance and status accomplished by contract deliverables

No Off Premise Status, No common data language, Prime and Gov't PO struggles for insight

No cross enterprise tracking results in no confidence, problems discovered after the fact

guardtime FEDERAL

What is the Concern From the Government's (consumer's) POV?

- Authenticity - Am I consuming an authentic item?
  - For digital items (software, information), data integrity
  - For physical items, unique identifier relates it to its "digital twin"
- Provenance - Has it been produced according to an approved process?
  - Who produced it? When?
  - Manufacturing process followed?
    - Authentic sub-components?
    - Material sources?
    - Computer aided manufacturing files authentic?
    - Machines operating within tolerances?
  - Required QA testing accomplished?
  - Distributed through approved channels?

guardtime FEDERAL

What's the Problem?

- Business processes cross many boundaries – business-to-business partnerships, producer to customer, regulation and oversight authorities
- Audit and Reconciliation functions exists because there is no independent guarantee of the integrity of the process
- Compliance function exists because there is no way to enforce and prove the integrity of the process
- Fraud exists if the integrity of the process can be abused
- Security industry exists to detect and prevent abuse

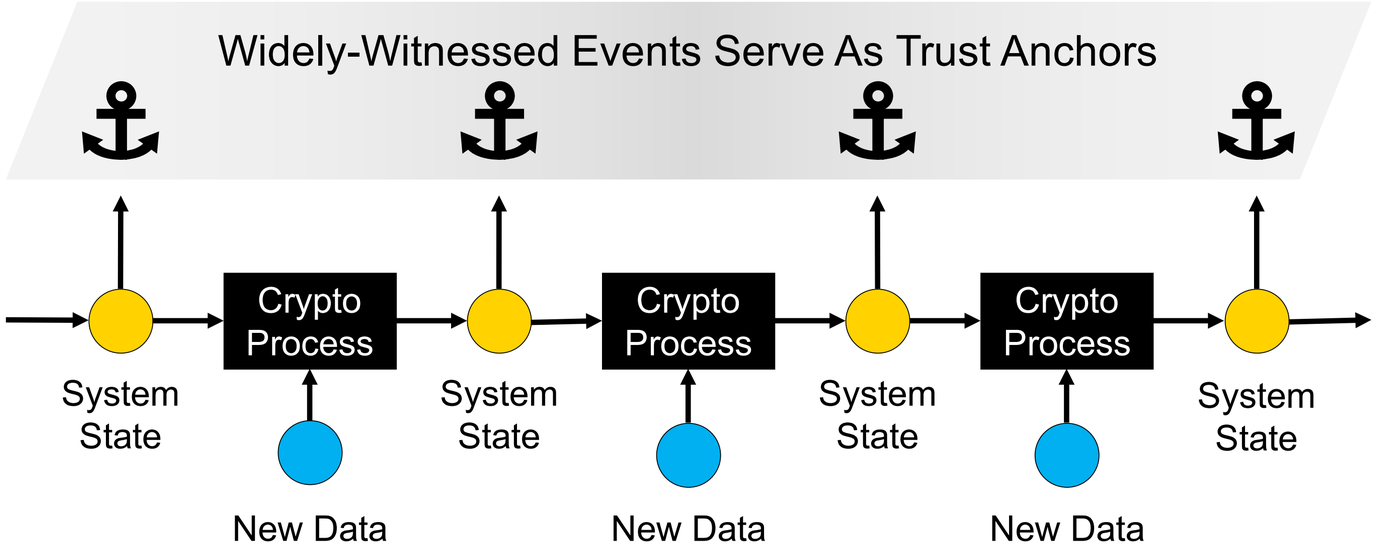
Digitize cross-boundary business processes while guaranteeing their integrity

guardtime FEDERAL

A Blockchain Can Provide The Needed Shared Trust Anchor

"Blockchain" – from Wikipedia

- A blockchain is a continuously growing, append-only list of records, called blocks, which are linked and secured using cryptography.
- By design, blockchains are inherently resistant to modification of the data -- Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks



Provides all participants with a shared (public) trust anchor.

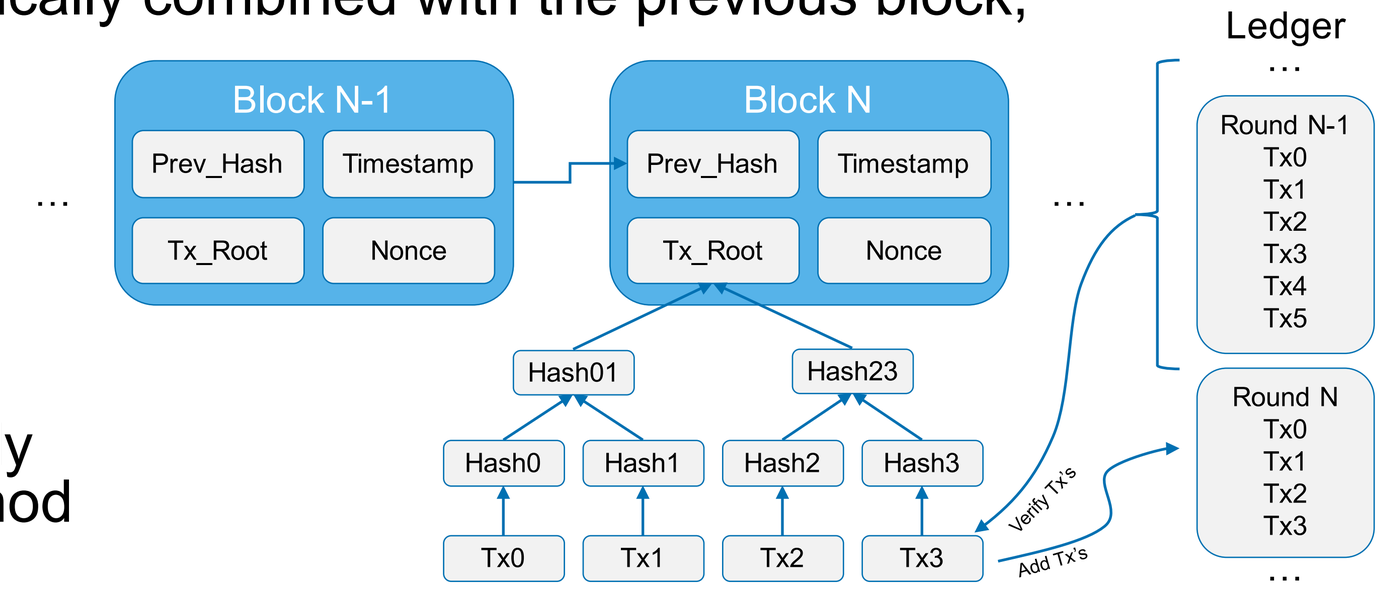
guardtime FEDERAL

Distributed Ledger Model – e.g. BitCoin

- A “distributed ledger” contains all the transactions ever recorded in the blockchain in a public database

- In each round, new transactions are first validated against the ledger.
- Each round, a group of validated transactions is hashed into a Merkel tree.
- The Merkel tree root is cryptographically combined with the previous block, resulting in the new Block.
- The new transactions are added to the ledger.

- The ledger grows according to transaction volume
- Bitcoin’s method to cryptographically link blocks is a “proof-of-work” method to achieve consensus

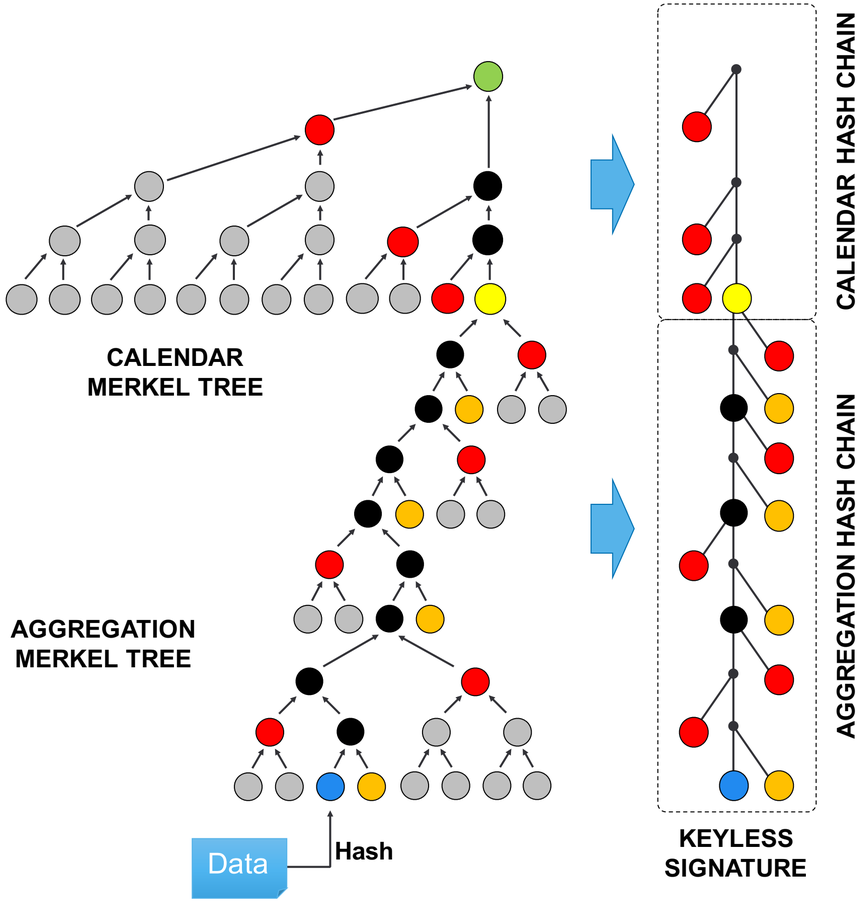


The public Distributed Ledger contains ALL of the data and IS the trust anchor.

guardtime FEDERAL

Proof of Participation Model – e.g. Guardtime Keyless Signatures

- Requestor hashes data at client machine and only the hash is sent to the network – keep the information private!
- Build a Merkel tree with the submitted hashes for each 1-second round.
- Resulting top hash is added as a leaf on a Calendar Merkel tree, cryptographically linking current round to previous rounds.
- Calendar Merkel tree is distributed publicly – it is the “blockchain database” – and its top hash is the trust anchor
- Merkel hash chains are provided to requestor; used to prove their data has participated in a particular round.



The Distributed Calendar contains NONE of the data; Calendar top hashes are the trust anchors.

guardtime FEDERAL

Model Comparison

Distributed Ledger

Public Data/Public Anchor

- ALL Data is stored in the public ledger
- Entire Database is the trust anchor
- Database grows with transaction volume
- Verification requires a copy of the (large) public database
- Every Participant sees ALL the data

Proof of Participation

Private Data/Public Anchor

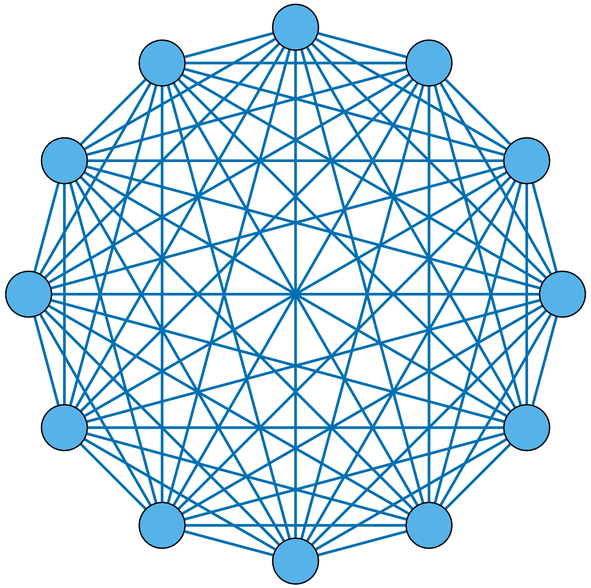
- NO data is stored in the public database
- Independent trust anchors every round
- Database grows linearly with time
- Verification requires data and signature; compare computation to small public anchor
- Data owner chooses with whom to share

- *What happens when you need to interact with many different network systems?*
  - *How to ensure Data Privacy?*
  - *How to maintain data provenance as information moves through boundaries?*
  - *How to add/remove system participants?*
  - *What infrastructure is required to verify data/transactions?*

guardtime FEDERAL

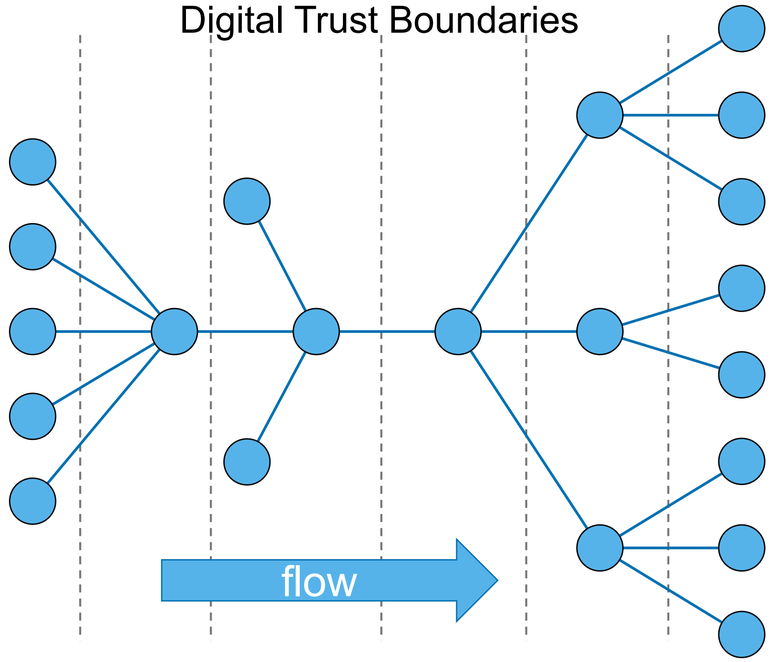
Is a Distributed Data Ledger really what the use case calls for?

Does the problem look like this?



Everyone needs to participate with everyone.

Or this?

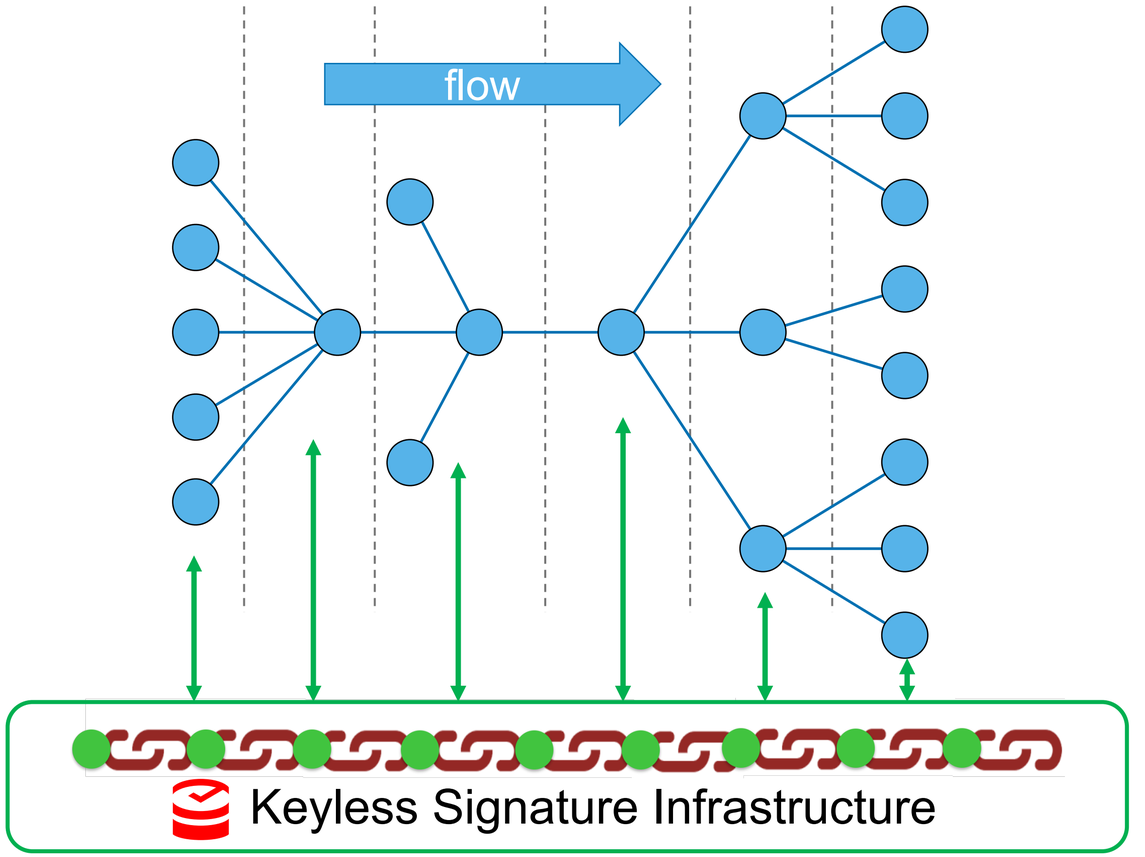


Interactions are limited and there is a flow to the process as it moves from one performer to the next.

guardtime FEDERAL

The Guardtime Approach: KSI-Backed Data and Process Integrity Enables Federated Execution and Distributed Verification

- Federated execution means that each part of the business process is owned and controlled by the party responsible.
- Distributed verification means that everyone can verify the data and that the overall process has been executed in accordance with pre-agreed rules.
- The benefits of this approach are scalability, performance, privacy, security and the ability to integrate with legacy systems while preserving existing accreditations.



KSI is an immutable, add-on, cross-boundary trust anchor that provides end-to-end life-cycle integrity for multiple use cases simultaneously

guardtime FEDERAL

How Is KSI Different From Other Blockchains?

Data itself is not stored in the system, only the cryptographic effect of its participation

- Requestor is provided with a cryptographic evidence token, a digital signature
- Signature allows a verifier to prove the Data affected the blockchain at a particular time
- Loss of Data or Signature cannot be recovered -- EVER

Participation is limited to authenticated entities

- Symmetric keys used to authenticate during signature generation allow server to establish identity of requestor
- Server adds ID of signature requestor as additional data to the system
- Allows verifier to cryptographically prove the identity claim in the signature through its effect on the system

Data to be participated is not validated – there is no data ledger!

- Any (authenticated) participant can get a signature for ANY data
- However, the signature will establish the “who” and “when” the data was participated
- Separates the ledger from the trust anchor - allows flexible integration of “blockchain”

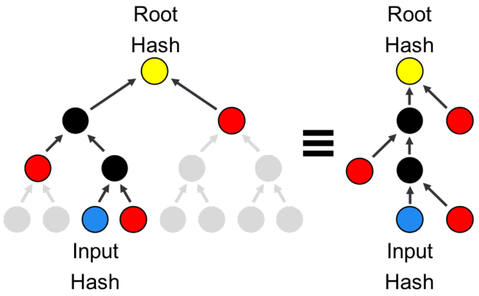
KSI cryptographically links the data to a temporal and immutable Trust Anchor

guardtime FEDERAL

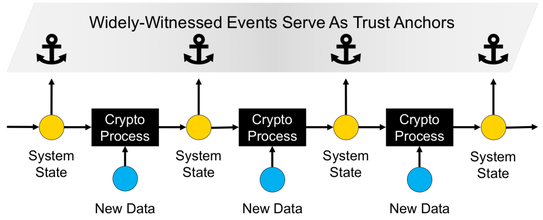
KSI Enabled by Robust and Proven Technologies

- Cryptographically **Secure Hash Algorithms**, e.g. SHA2-512
  - One-wayness prevents disclosure of private information
  - 2nd pre-image resistance prevents counterfeiting
  - They can be computed quickly on virtually any client

- Hierarchical **Merkle Trees** and Merkle Hash Chains
  - Enable aggregation of immense number of requests (10^{12+}) in each round
  - Enable long-term operation on quick cadence (1 round/second)
  - Calendar Database growth is linear with time at ~4 GB/year
  - Small signature tokens of 2-4 KB delivered after each round.



- Permissioned **Blockchain Database**
  - Calendar is widely distributed and top hash is periodically published
  - Identity of signature requestor becomes part of the blockchain
  - Can’t deny the past and can’t go back in time to register something



Anyone Can Do The Math!

guardtime FEDERAL

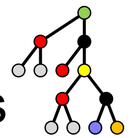
Guardtime KSI System

KSI Aware System

Provides

- Data Authenticity
- Immutable Time
- Signing Entity
- Scalability
- Security
- Resiliency
- Inter-operability
- Data Defense In Depth
- Data Provenance

Guardtime Component

- Keyless Signatures 
- Gateway
- Aggregator
- Core
- Black Lantern
- vAppliance
- Managed Services
- Link
- Sentry
- Broker
- Venture
- XDAL
- KSI Dockets

Foundational Area

- Crypto
- Cyber
- Attribution

guardtime FEDERAL

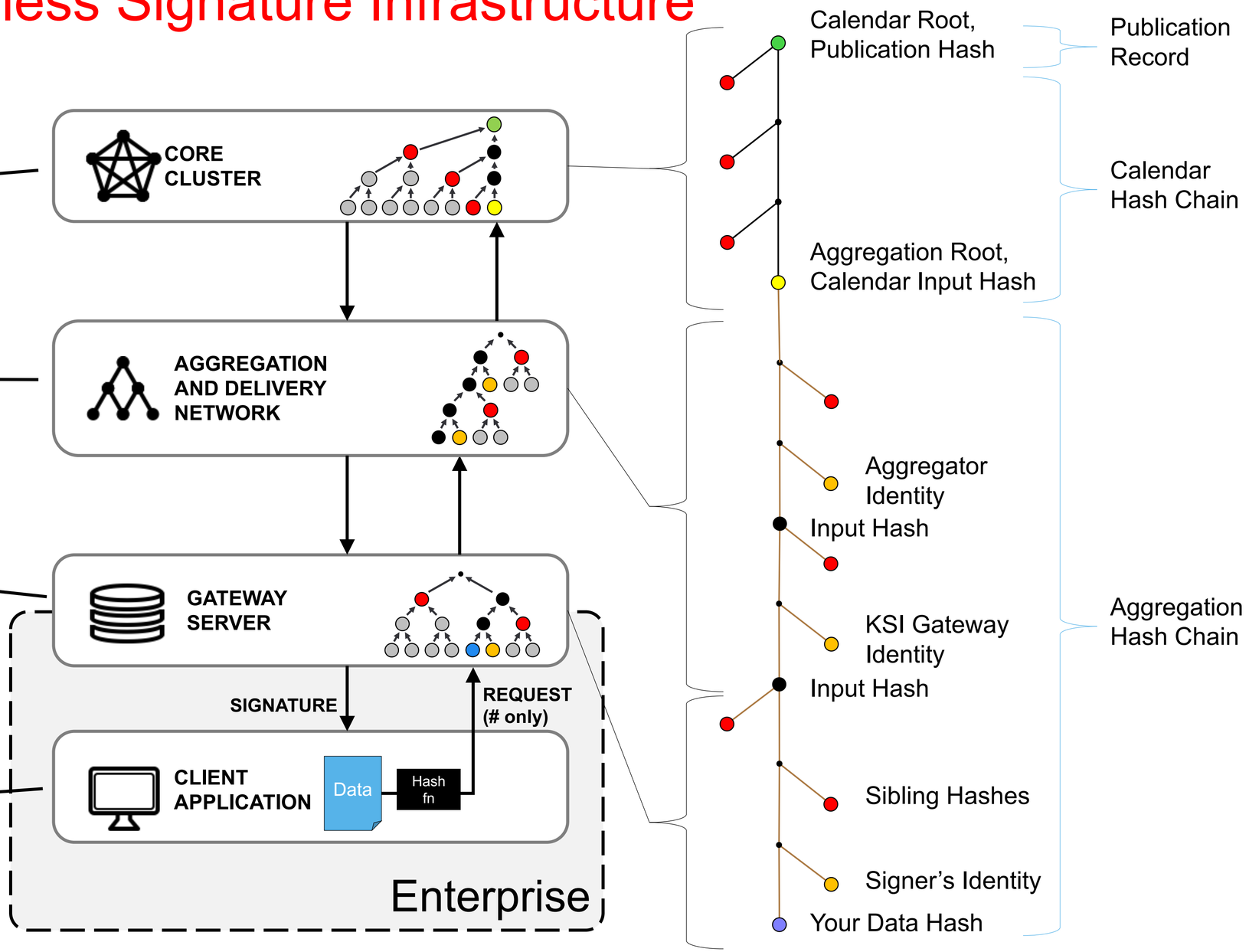
Guardtime Federal's Keyless Signature Infrastructure

Core Cluster creates the round's top root hash and durably stores it as a new leaf in the Calendar Block Chain.

The Aggregation and Delivery Network provides the scale and reach.

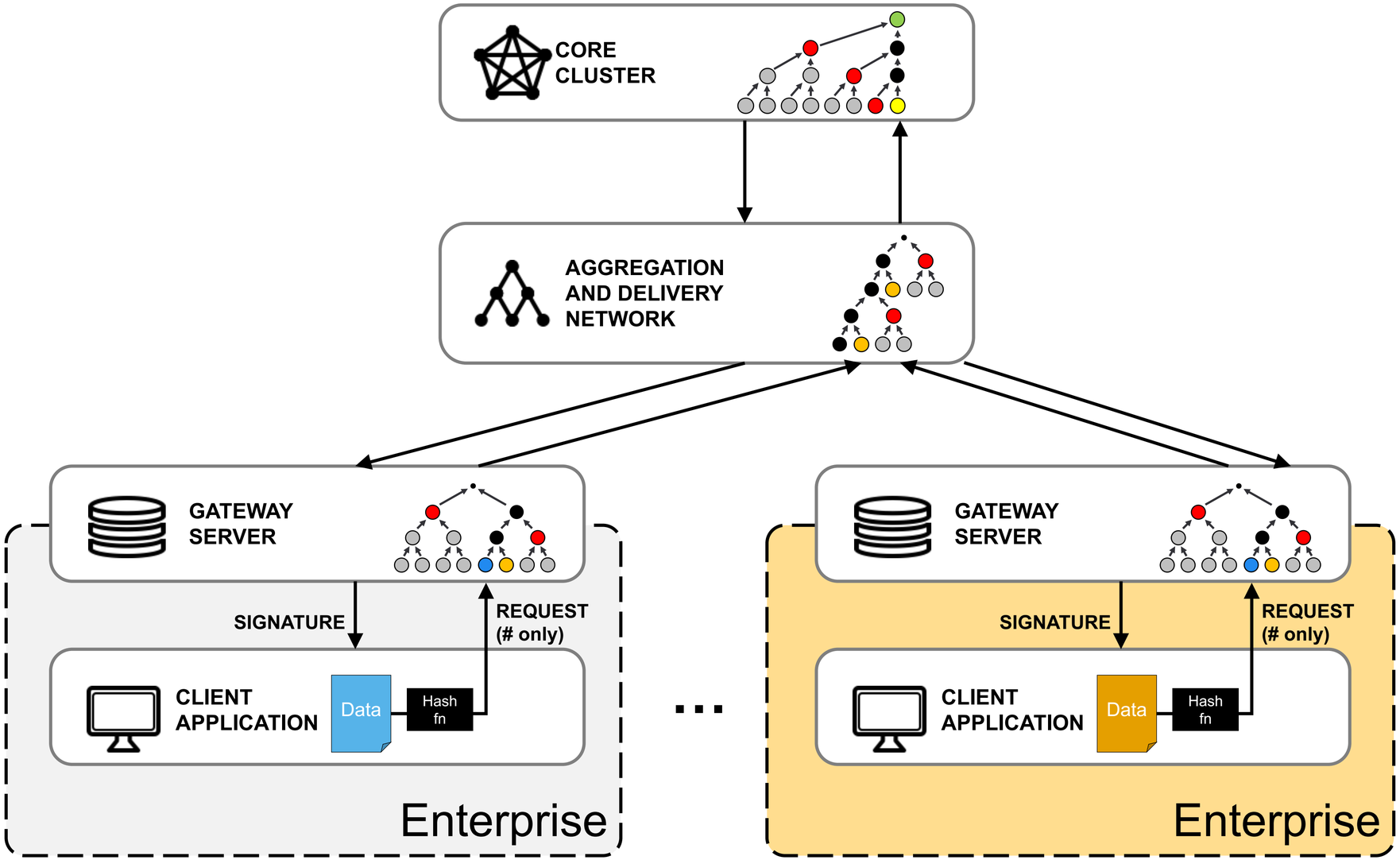
The KSI Gateway delivers the KSI signing service to client applications. (NIAP Certified Black Lantern)

KSI-enabled applications request signatures. User data never leaves the client machine – only cryptographic hashes of the data.



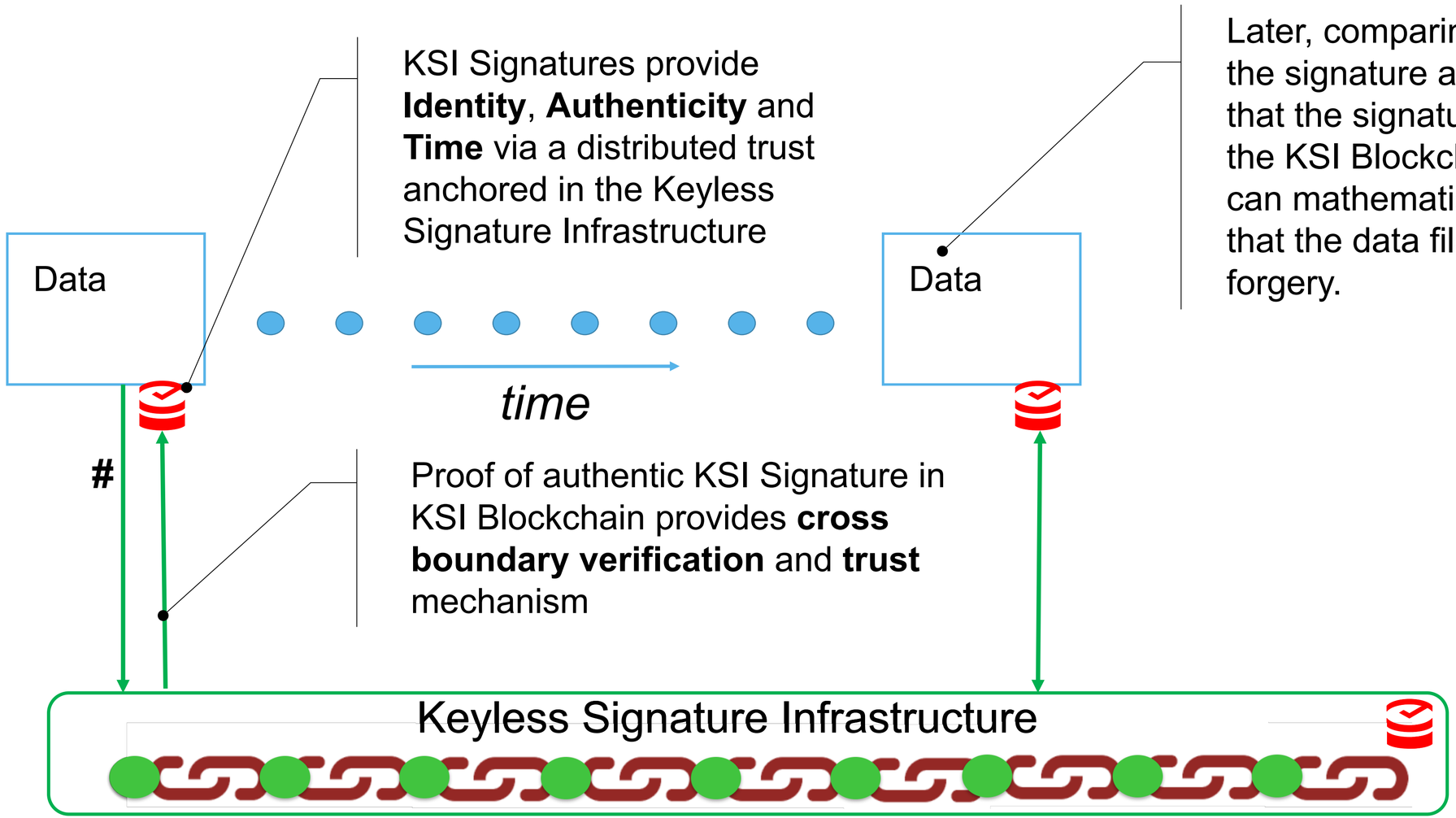
guardtime FEDERAL

Guardtime Federal's Keyless Signature Infrastructure



guardtime FEDERAL

KSI Signed Data – Logical Representation – Static File Integrity



guardtime FEDERAL

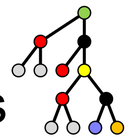
Guardtime KSI System

KSI Aware System

Provides

- Data Authenticity
- Immutable Time
- Signing Entity
- Scalability
- Security
- Resiliency
- Inter-operability
- Data Defense In Depth
- Data Provenance

Guardtime Component

- Keyless Signatures 
- Gateway
- Aggregator
- Core
- Black Lantern
- vAppliance
- Managed Services
- Link
- Sentry
- Broker
- Venture
- XDAL
- KSI Dockets

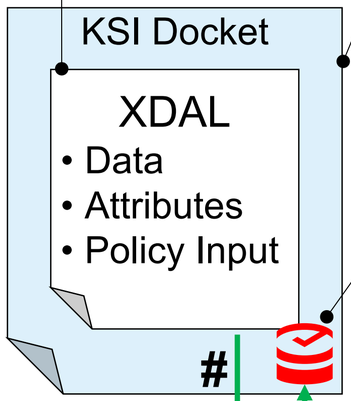
Foundational Area

- Crypto
- Cyber
- Attribution

KSI Dockets – Logical Representation – Provenance Capability

XDAL provides a unique, purpose built language for interoperability and validation

KSI Dockets provide a **standardized construct** backed by KSI Signatures. These constructs are based on the Guardtime eXensible Data Attribution Language for machine readable inputs to verification endpoints.

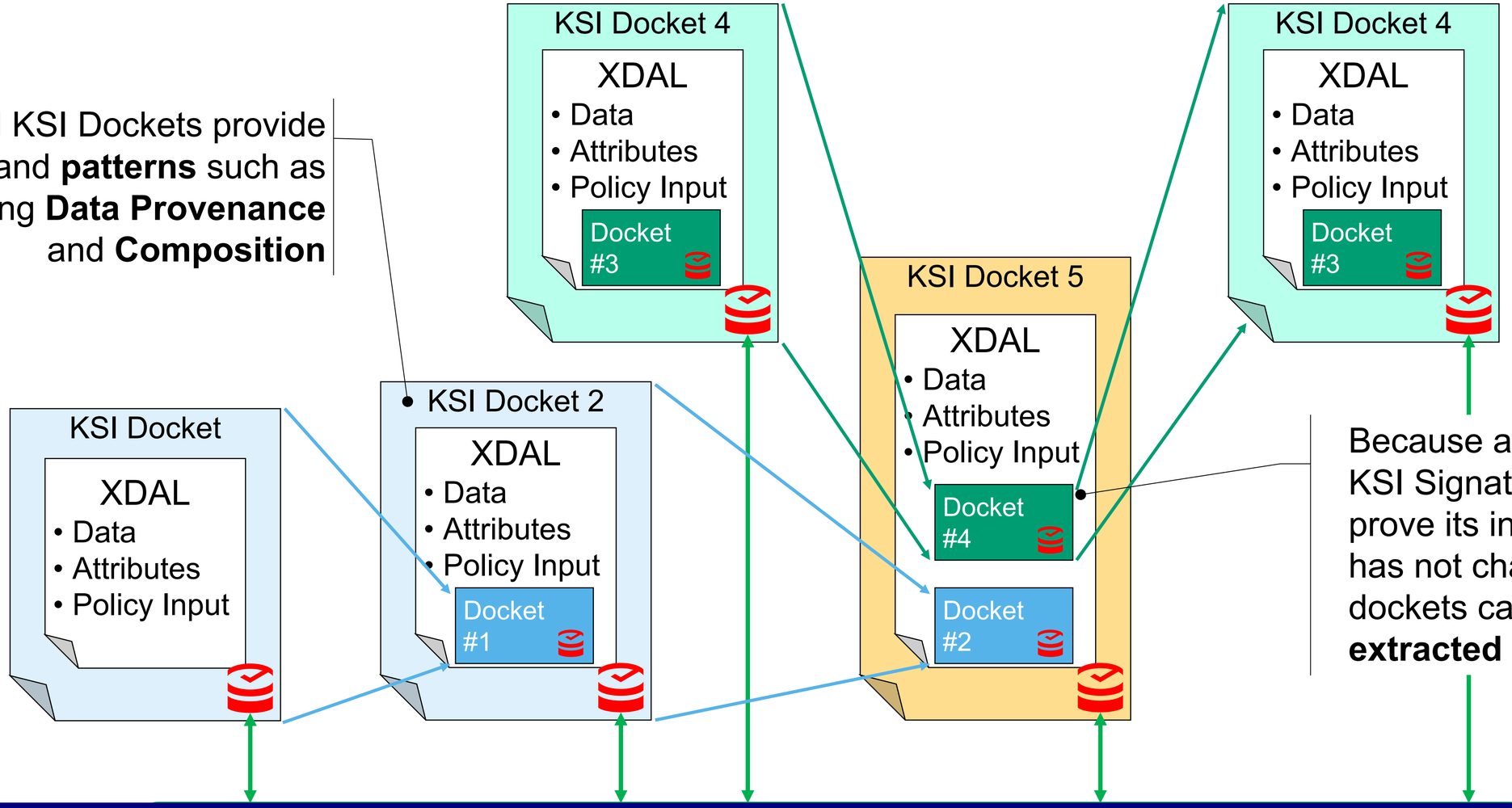


KSI Signatures provide **Identity**, **Authenticity** and **Time** via a distributed trust anchored in the Keyless Signature Infrastructure

Proof of authentic KSI Signature in KSI Blockchain provides **cross boundary verification** and **trust** mechanism

guardtime FEDERAL

KSI Dockets – Logical Representation – Provenance Capability



Nested KSI Dockets provide **logic** and **patterns** such as proving **Data Provenance** and **Composition**

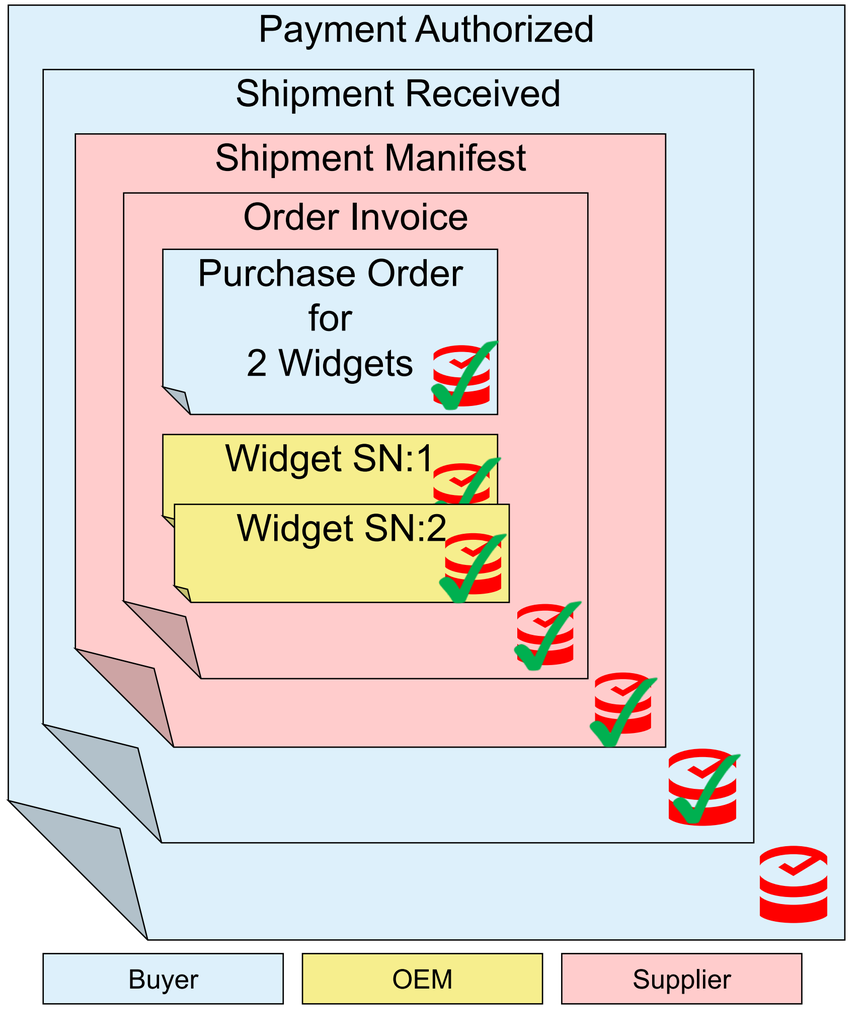
Because a docket's KSI Signature can prove its information has not changed, sub-dockets can be **extracted** later.

Nested Dockets are **self-contained microledgers**, with signatures created by users in **multiple domains**, but verifiable by anyone against the **common trust anchor**.

guardtime FEDERAL

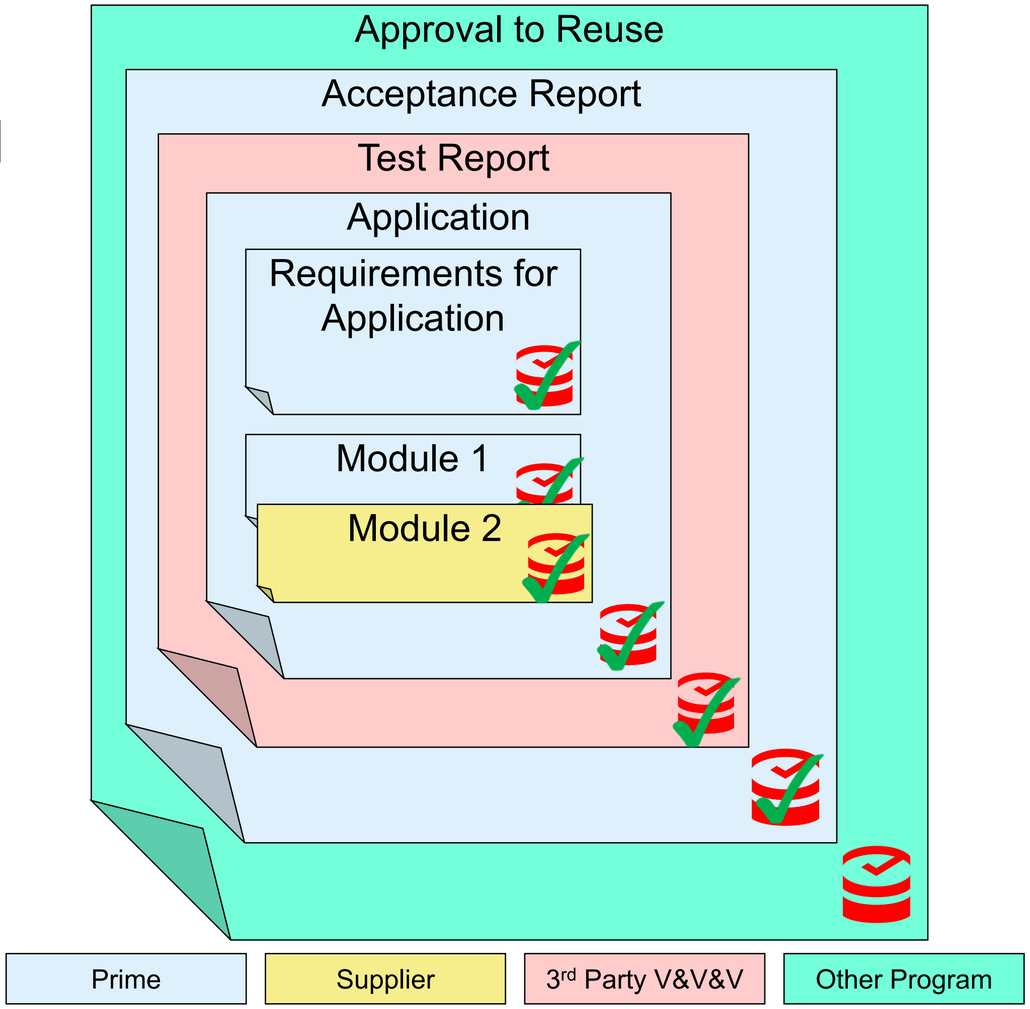
KSI Dockets Example – (Auditable) Physical Supply Chain

- Buyer creates Purchase Order; sends to supplier
- Supplier receives order, checks integrity
- Supplier has items, each with signed history from Orig. Equip. Manufacturer, checks validity
- Supplier creates Order Invoice, nesting dockets
- Supplier creates Shipment Manifest and ships to purchaser
- Shipment is received by Buyer – docket verified that Widgets satisfy Purchase Order
- Buyer verifies shipment receipt and authorizes payment



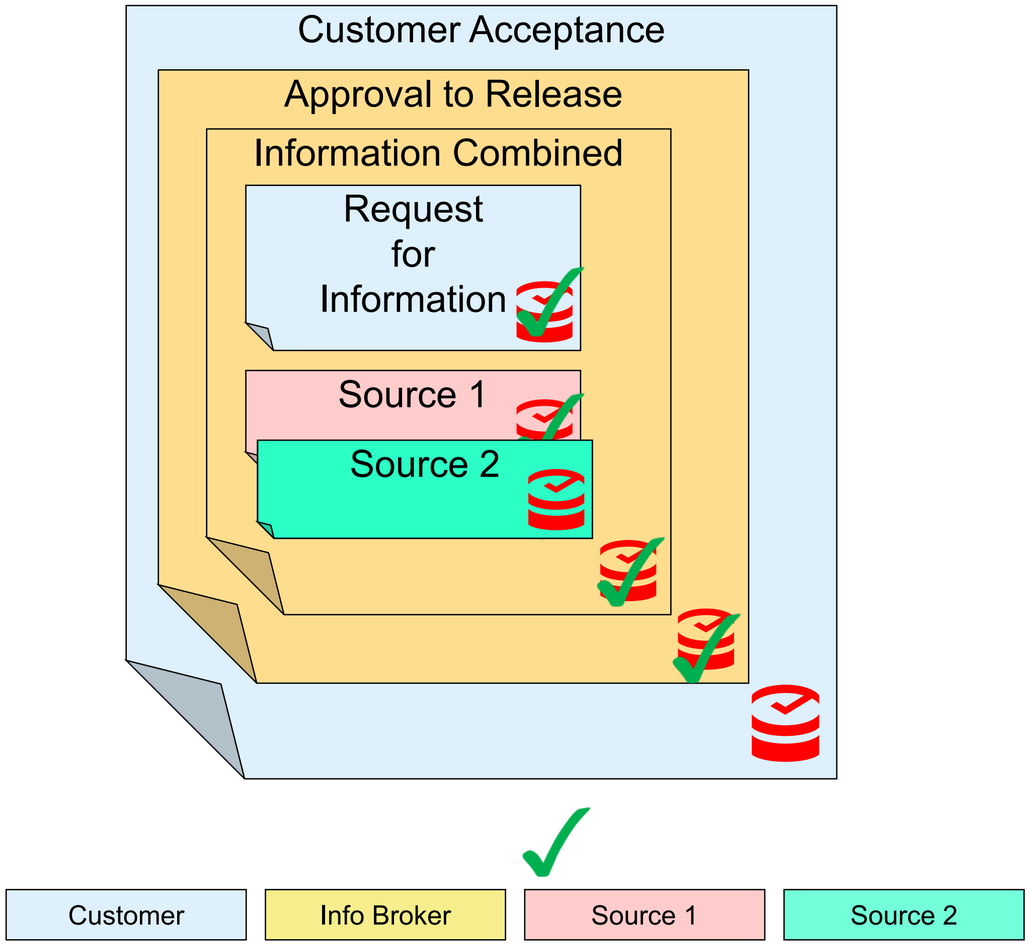
KSI Dockets Example – Software Supply Chain (SW Assurance)

- Requirements for an application are established and signed
- Modules created by Prime and Supplier(s) against verified Requirements
- Application is compiled from verified code blocks
- Third-party V&V and Vulnerability testing of verified Application
- Acceptance of verified SW for use in system
- Other systems can verify provenance and integrity of code, testing, and base requirements – limited re-testing required to leverage prior investment



KSI Dockets Example – Information Supply Chain (Cross Domain)

- Request for Information submitted by Customer
- Information Broker has multiple sources, verifies integrity of data
- Information is packaged by Information Broker
- Information verified and reviewed to ensure release is in accordance with policy; Approval is granted for Release to Customer
- Customer verifies and accepts Information
- Customer can securely Extract individual source material without compromising integrity or origination of the material – Verification can be accomplished by end user.



guardtime FEDERAL

Summary

1. Data itself is never sent to, or stored in, the KSI “blockchain.”
2. Requestor can only obtain a signature if they can authenticate to the system.
3. Requestor receives an evidence token that proves the Data affected the KSI in a particular round – includes the requestor’s identity cryptographically embedded!
4. KSI Signatures are SHA-based and “quantum resistant”
5. Verification is done by the end user – data, KSI signature, public trust anchor

6. KSI Dockets neatly package Data, attributes/context, KSIG -- and other Dockets
7. Nesting Dockets effectively creates self-contained micro-ledgers.
8. Existing business systems can easily ingest XML Dockets.
9. Established (accepted) processes can be imbued with integrity, increasing confidence, reducing costs, adding new opportunities

guardtime FEDERAL

Questions?

End of Slide Show