guardtime

Ensuring Healthcare System Integrity with Blockchain

Ivo Lõhmus

Program Manager

guardtime

Agenda:

Blockchain Based Integrity Assurance Concept

Keyless Signature Infrastructure overview

Integration with Estonian E-health Foundation & more

guardtime

Data Integrity

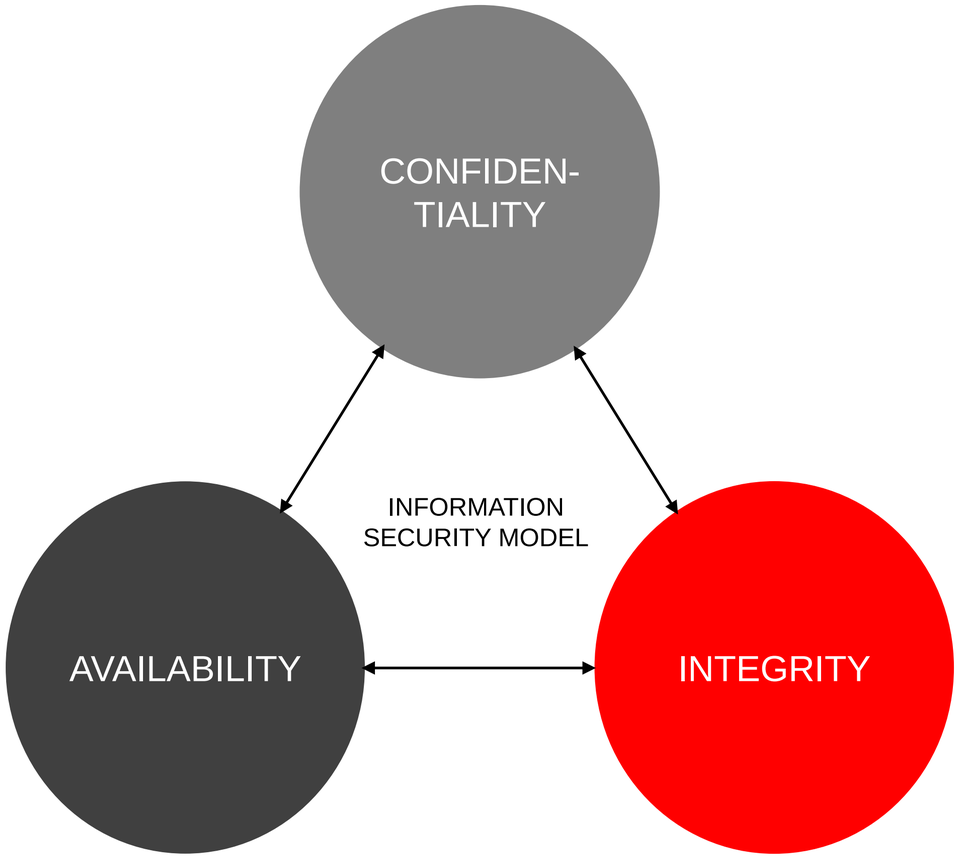
The root cause for ineffective cybersecurity is the lack of integrity of systems, networks, processes and data.

“The most serious national security threat looming in cyberspace may be the potential for vital data to be altered by cybermarauders”

– James Clapper, Director of National Intelligence (ODNI)

“The newest cyber threat will be data manipulation.”

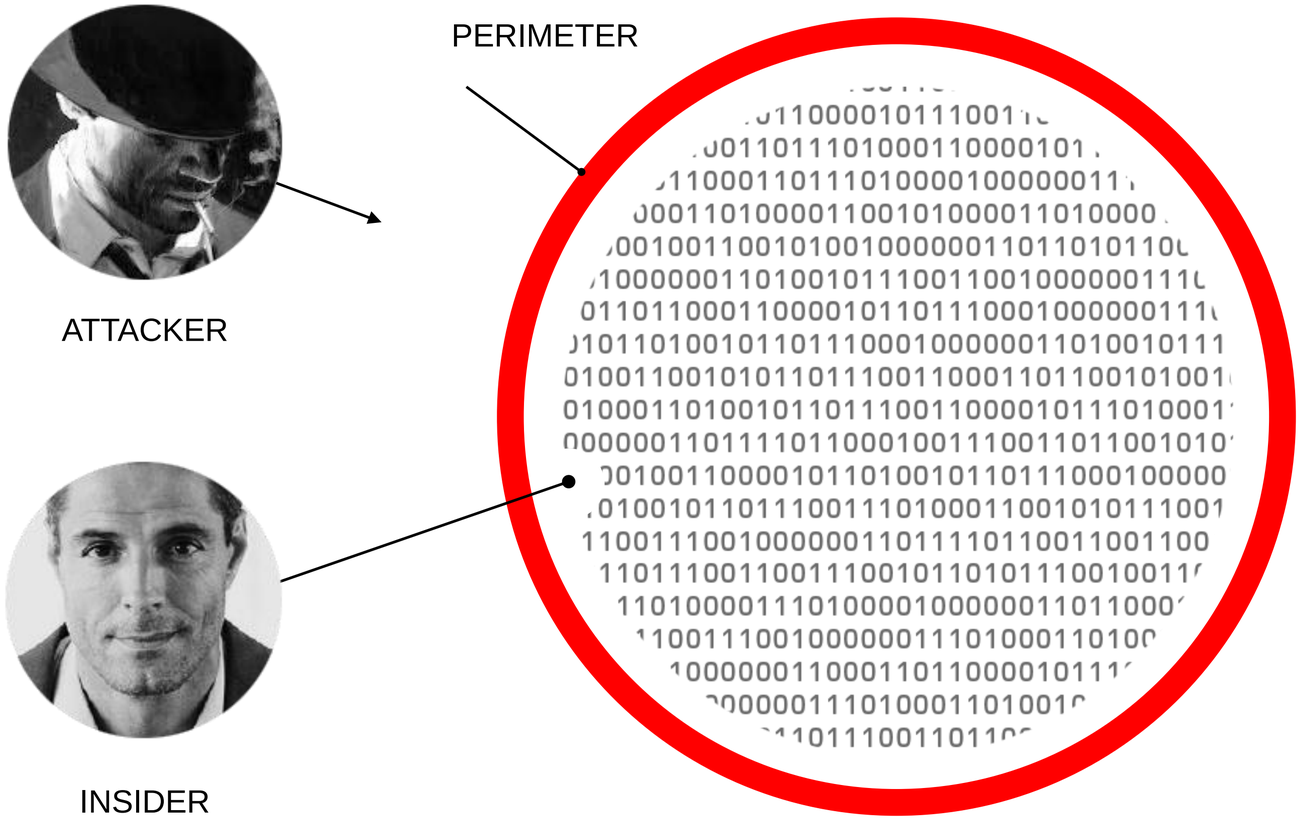
– Mike Rogers, Director NSA



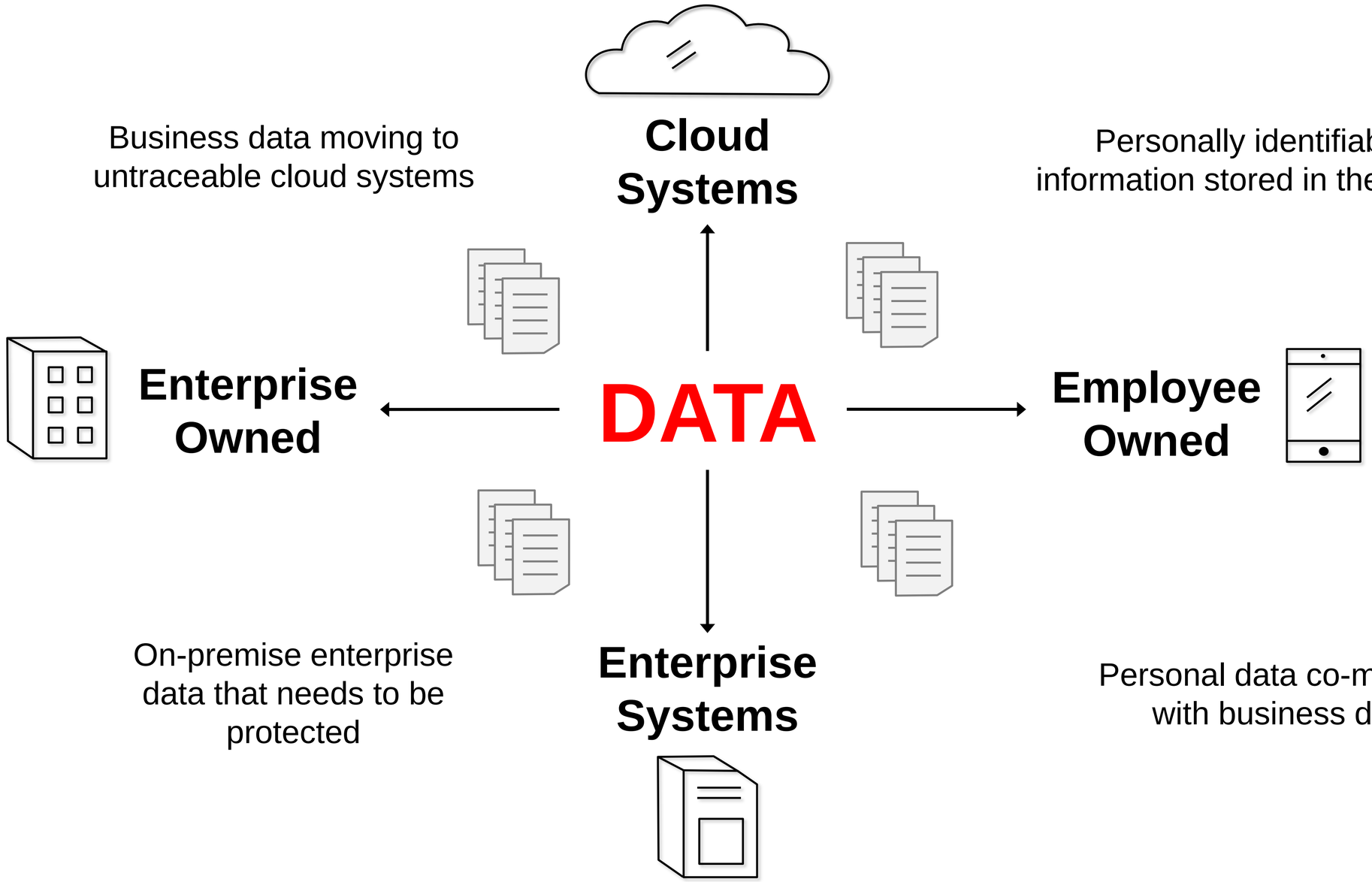
The Absence of Compromise

guardtime

The Problem: Traditional Approach to Cybersecurity



guardtime


Business data moving to untraceable cloud systems
Cloud Systems
Personally identifiable information stored in the cloud
Enterprise Owned
DATA
Employee Owned
On-premise enterprise data that needs to be protected
Enterprise Systems
Personal data co-mingling with business data

guardtime

The old guard of perimeter-based defense is ineffective and we need to compliment these solutions

---

It’s time to defend the DATA itself.

guardtime

Data Integrity Application in Cybersecurity

The practice of
verifying that

DATA

in your network
is not compromised


Firewalls


Configurations


Routing tables

Firmware


Data-at-rest


PaaS / IaaS

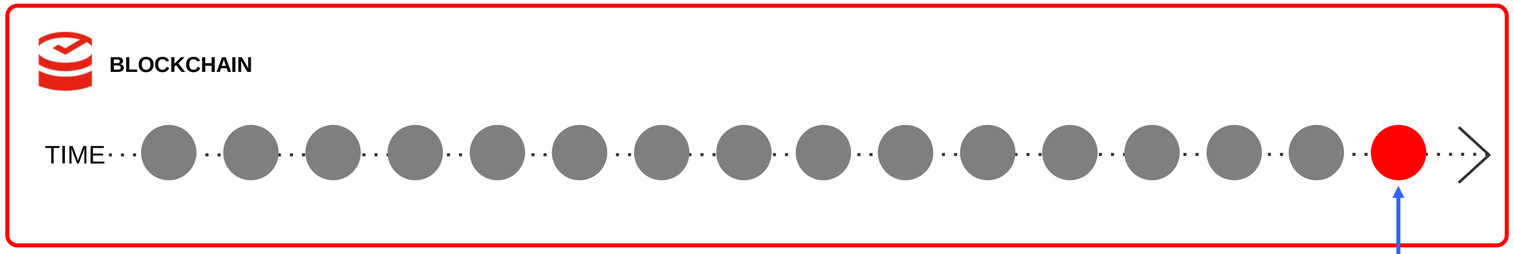

Virtualization

Event logs

…and other critical assets

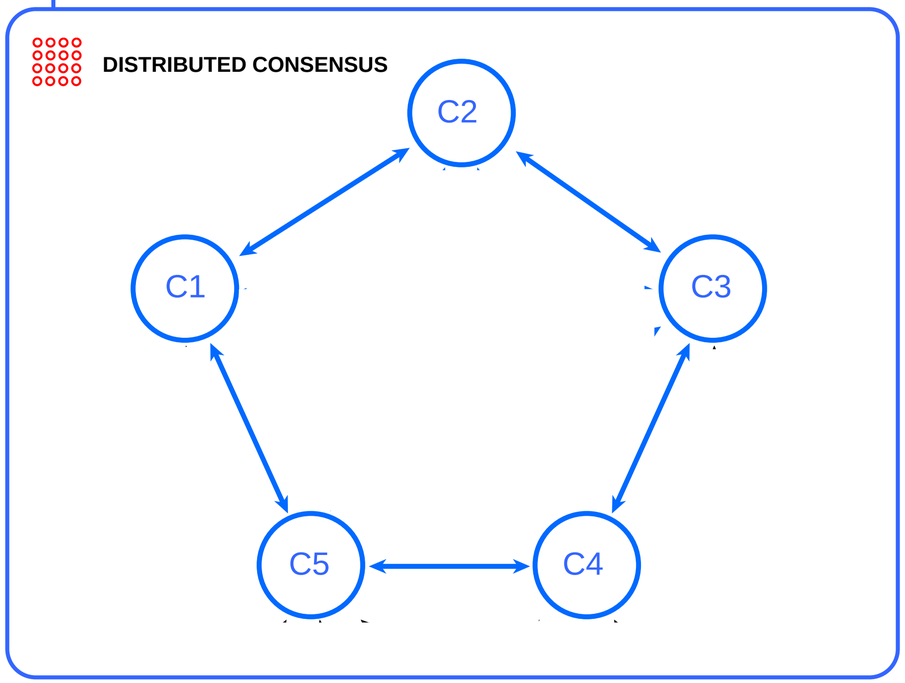
guardtime

Blockchain Principle



“Blockchain” is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering.

“Distributed consensus” is an agreement between different compute-nodes over what is a true or false record



As every client has a copy of the blockchain it is impossible to manipulate information and cover up your tracks. The integrity and provenance of information systems can be mathematically proven.

Bitcoin is blockchain-based, not vice versa!

guardtime

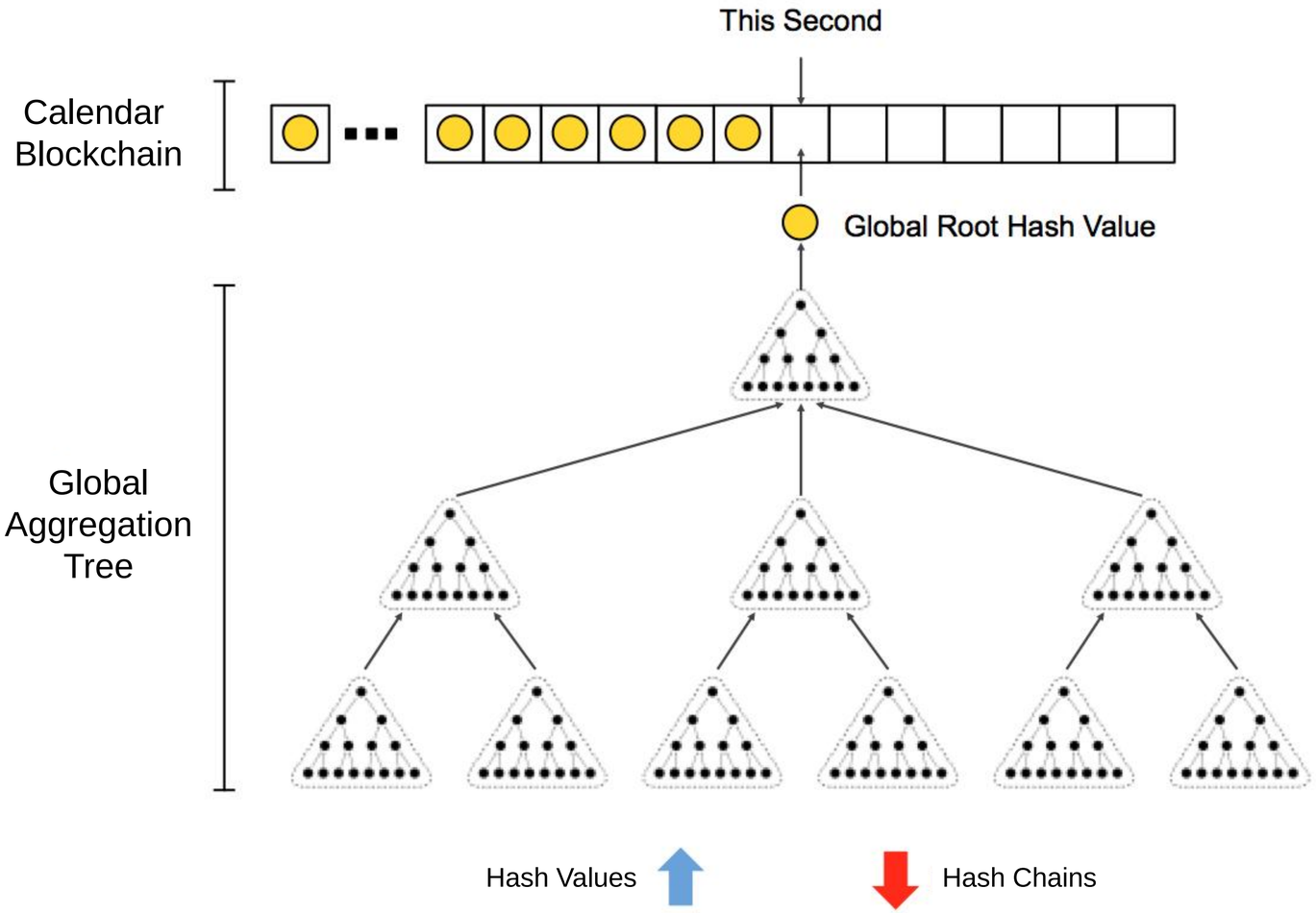
Introducing the Hash Calendar Blockchain

A global asynchronous Aggregation Tree summarizing all submitted Hash Values is built every second and destroyed after all clients have received their hash chains.

The same tree is never rebuilt.

Only the Global Root Hash Values of the Aggregation Tree are kept in a public Calendar Blockchain.

The Calendar Blockchain has exactly one entry for each second since 1970-01-01 00:00:00 UTC



guardtime

Signature Token

A signature token consists of:

- Hash chain from input data hash to global blockchain database
- Blockchian database hash chain
- Root hash value of the blockchain database tree that is periodically published.

guardtime

KSI Properties

KSI Signature provides:

- Signing time
- Signing entity
- Data integrity

KSI blockchain based asset authentication uses **formal mathematical methods** only, there are no secrets that can be compromised and conclusive proof of asset integrity is independent of any insiders or third parties.

The massive scale of the KSI enables authentication of **billions of data items** every second.

The KSI does not ingest any customer data – complete data **privacy is guaranteed** at all times.

Formal validation:

Tuesday, September 13, 2016 | ANNOUNCEMENTS

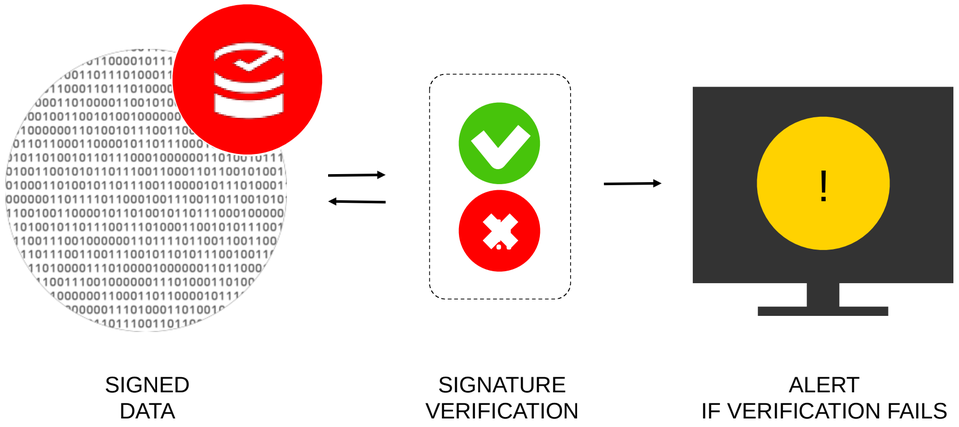
Galois and Guardtime Federal Awarded $1.8M DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System

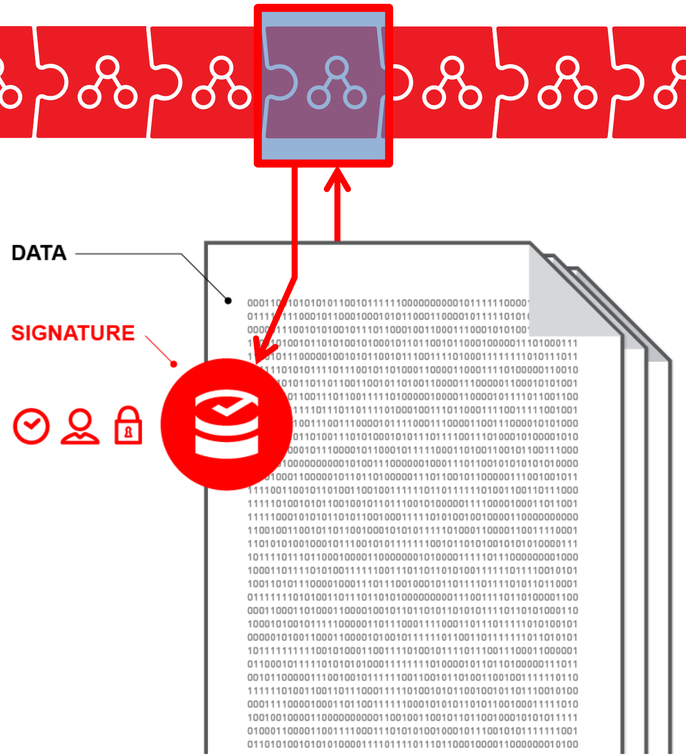
KSI is **quantum immune**, meaning it's security is not vulnerable to quantum algorithms run in existing or upcoming quantum computers, unlike i.e. RSA algorithm commonly used in PKI implementations.

guardtime

Solution to the Integrity Problem: Register Digital Assets in the Blockchain

KSI signatures, linked to the blockchain, enable the properties of data to be verified without the need for trusted third parties, keys or credentials that can be compromised.





guardtime

Integrity Backbone for Estonian eSociety

REPUBLIC OF ESTONIA
GOVERNMENT

Guardtime's KSI Blockchain is the **fundamental integrity substrate** for the Estonian e-Government systems that have 1,000+ citizen services and is ranked as one of the most advanced in the world.

Testing of KSI Blockchain in governmental systems started in 2008 and is in production use since 2012.

Today, Estonia has blockchain backed:

- Health-records
- Document registries
- Public database of laws
- Security infrastructure

guardtime

E-Healthcare in Estonia

Open information exchange platform; standardized schemas.

- Lab results
- Prescriptions
- Case history
- Medical certificates
- Specialist appointments
- Data feeds, e.g. for social insurance
- Patient portal.

X-road is the underlying message exchange platform. Encrypted database, identifying and medical data kept separate. ID-card based access only; security hardware where necessary.

Strong transaction log is auditable by every subject.

Managed by E-Health Foundation, founded by Ministry of Social Affaris and major medical institutions

guardtime

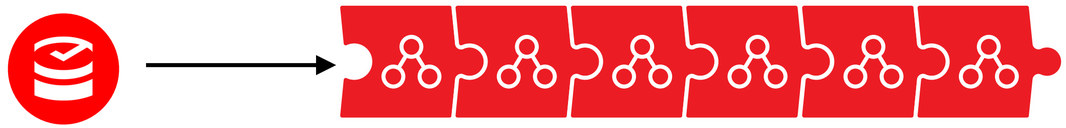
Initial integration with E-health Foundation

Goal is to solve several key problems for back-end healthcare record storage:

1. To produce independent and legally sound proofs of record and whole database for internal, external and regulatory compliance purposes.

2. To discover unauthorized changes, especially by insiders to the organziation, and report them in a timely fashion.

3. Achieve the above capabilities across extremely large systems with terabytes of data and millions of records



KSI BLOCKCHAIN

guardtime

1

Regulatory Compliance

Goal is to ensure ISKE T3 compliance

ISKE - Three-level baseline security system – defining requiements for confidentiality, availability and integrity.

ISKE is compulsory in organizations of state and local administration who handle databases/ registers.

T3 level integrity requirement: data source, manipulation and deletion must be legally provable. Data integrity, completeness and timeliness must be verifiable in real time.

T3 implementation in practice: hashchaining, signing and verifying all assets.

guardtime

2

Integrity assurance

Goal is to identify unauthorized changes in a timely fashion

Malicious actions by hackers or insiders that are mitigated:

- Unauthorized data manipulation
- Tampering with evidence of data manipulation
- Tampering with database backups

guardtime

3

Dimensioning requirements

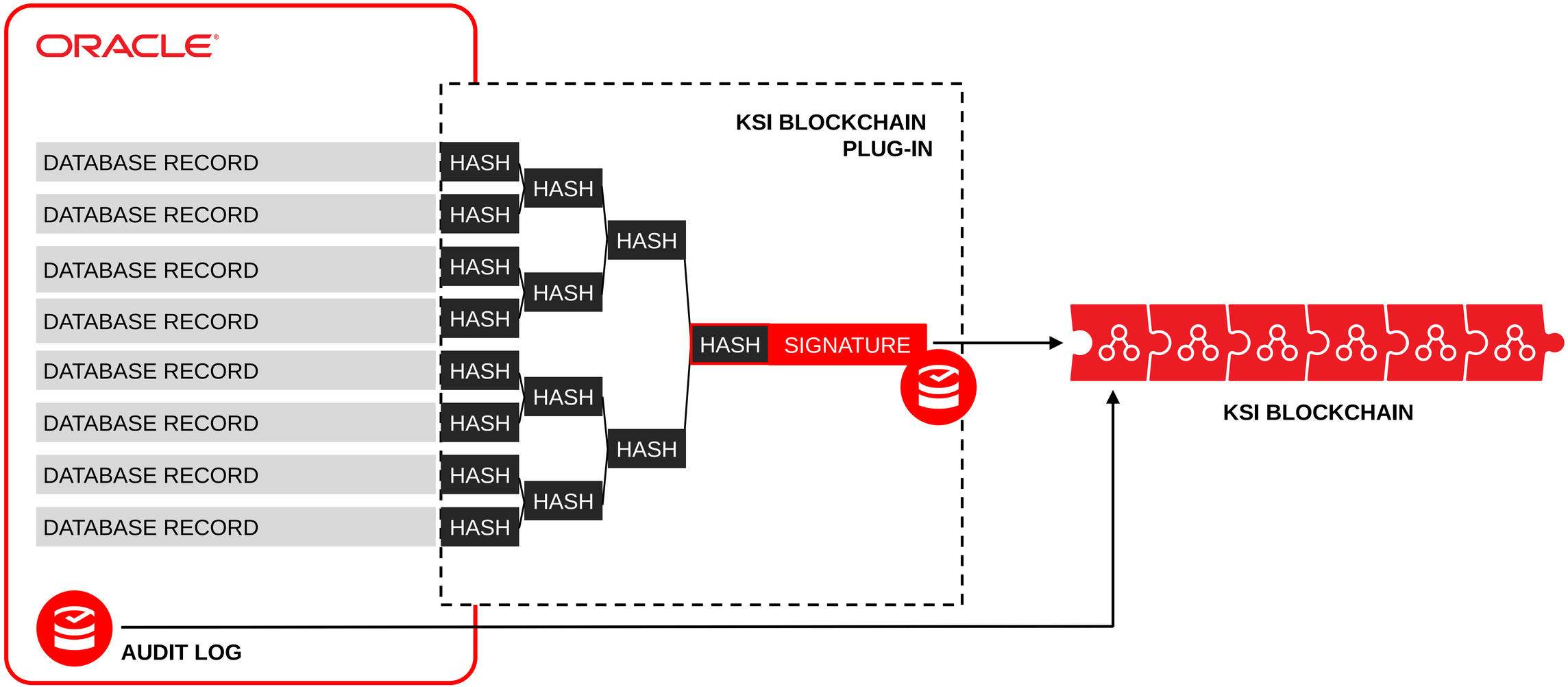
KSI integration must not cause additional overhead in E-health information system

Key dimensioning requirements:

- Tens of millions of database records must be signed
- Single record’s integrity must be provable in isolation
- Verification must be configurable (last day, last 30 days, whole database)

guardtime

Estonian E-Healthcare Oracle Database integration



guardtime

Securing E- Prescriptions

Use-Case Review

guardtime

e-Prescriptions: Overview

Core Problems Being Addressed

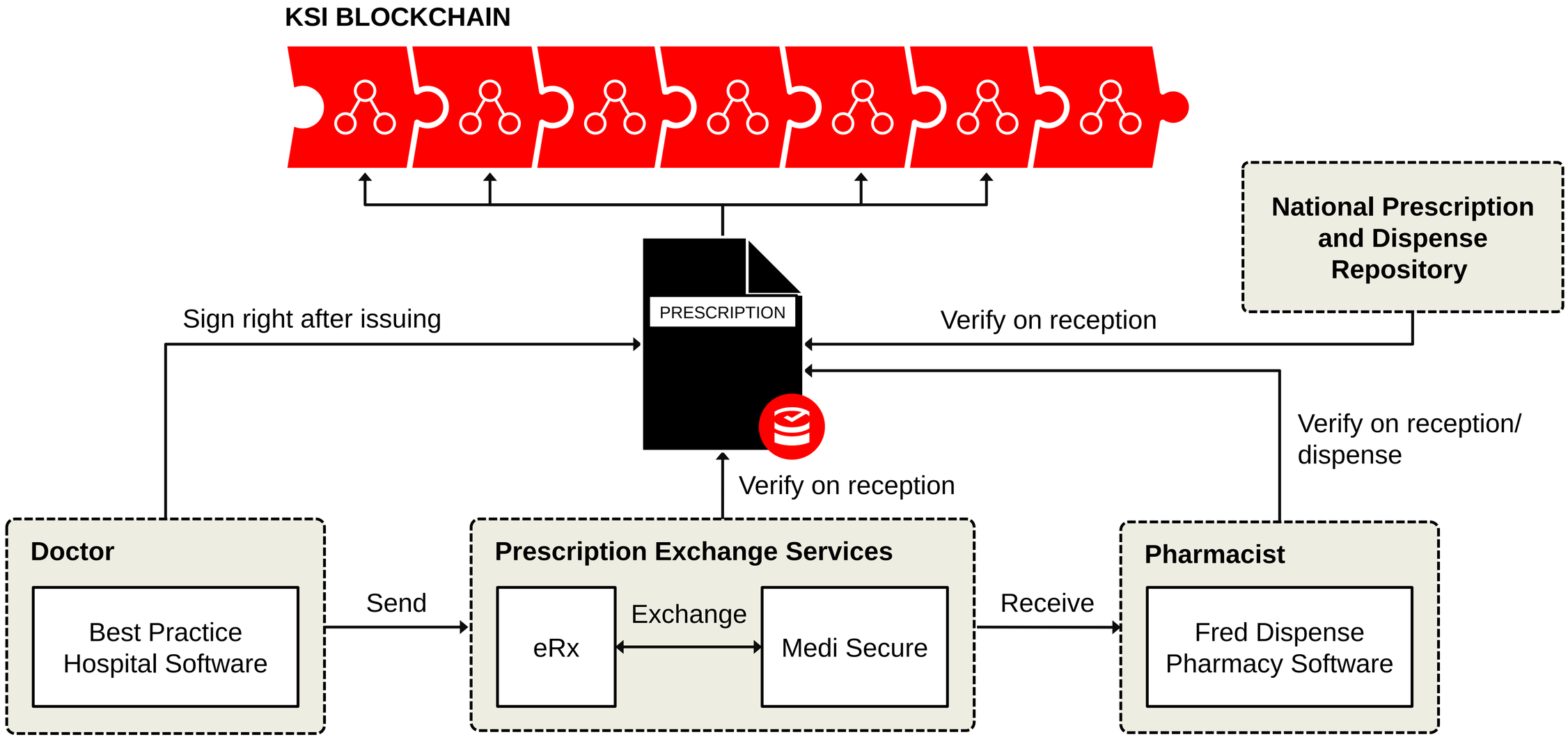
- Ensure integrity of prescription network as a whole
- Long-term integrity
- Legal aspects of paperless governance

KSI Solution

- KSI can protect e-prescription independent of the systems that process or store it
- Detect tampering with a valid e-prescription as it moves through the various systems
- Ensure consistency and integrity of dispense events of a e-prescription as it is being used
- Ensure the long term integrity of central e-prescription repositories and e-health records

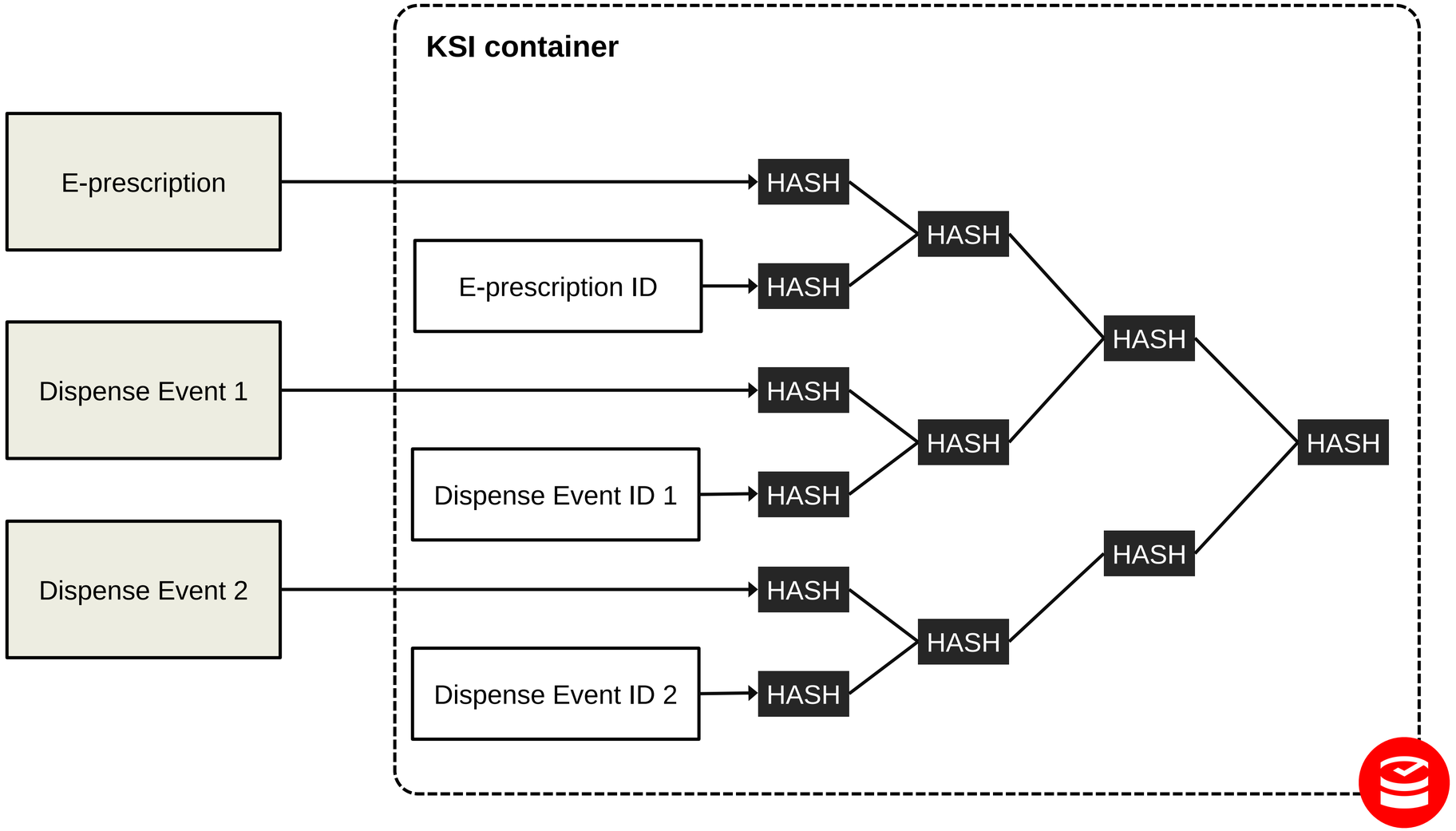
guardtime

e-Prescriptions: Architecture



guardtime

e-Prescriptions: Containers



guardtime

E-Health Integrations / Use-Cases Roadmap

- EHR long term archiving – provable integrity and timeline of medical events
- Telemedicine and remote care – verification of integrity of exchanged medical data
- Provably secure data handling at drug discovery and clinical trials

guardtime

Lessons Learned / Best Practices

Clearly define objectives:

- What kind of alerts are desired?
- What needs to be provable and to who?
- What are risk vectors?

Define Integration aspects:

- What is minimum/maximum granularity of data to be signed?
- If / how is data normalized?
- How often should data be signed?
- Where / how are signatures stored?
- What are verification policies?
- What are dimensioning aspects

Based on:

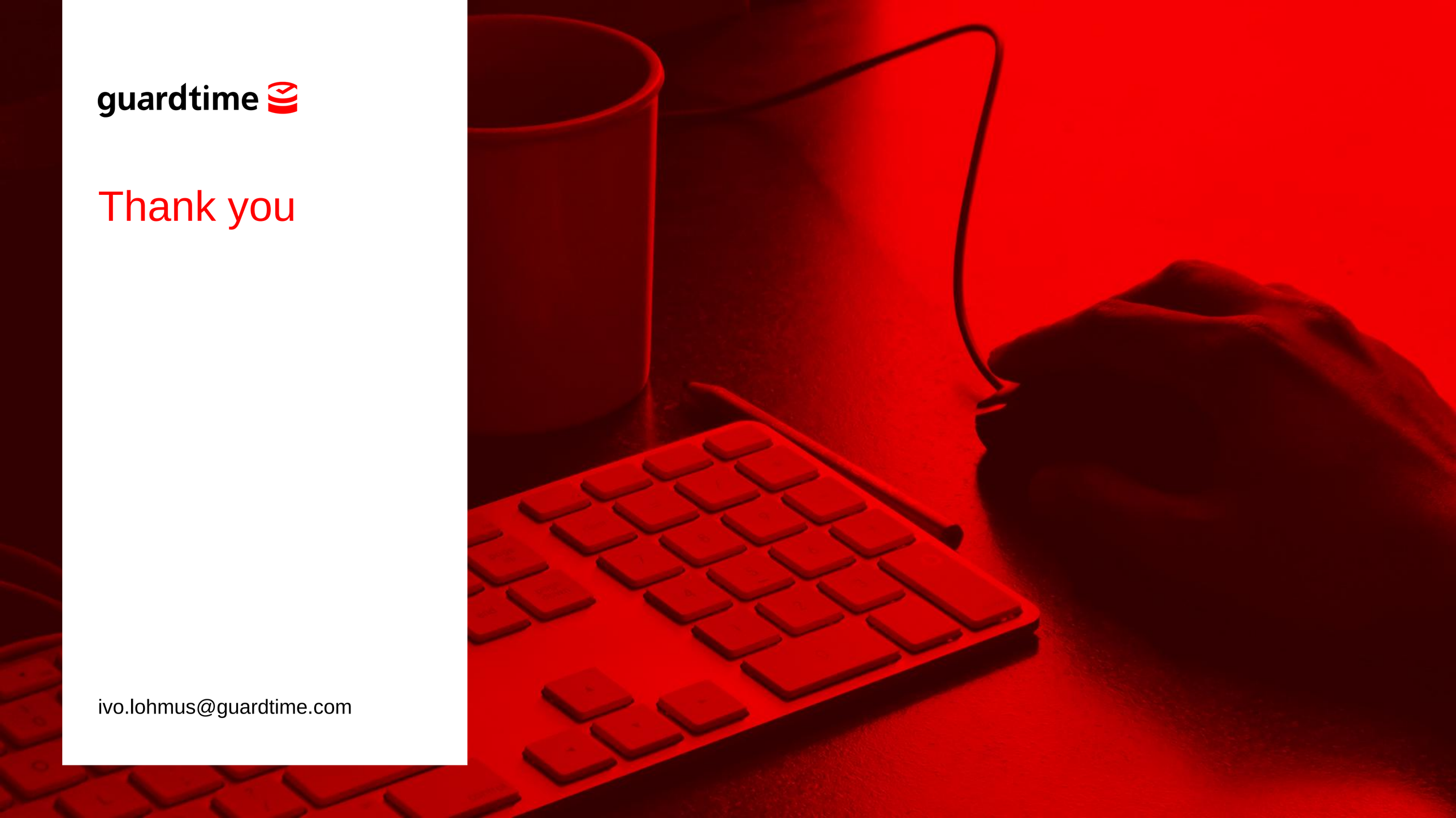
- Painpoints
- Risk analysis
- Regulatory Compliance

Best Practices:

- Sign as close to source as possible – follow business logic / data model
- Sign at immutable state
- Aggregate locally, consider hashing performance for large assets

guardtime

Thank you



ivo.lohmus@guardtime.com