Power Matters.

Microsemi

Improving Trust in the FPGA Supply Chain using Blockchain and Keyless-Signature Technology

Richard Newell
Senior Principal Product Architect, SoC Group, Microsemi Corp.
For the Cryptarchi workshop held in
Smolenice, Slovakia June 18-21, 2017

Improving Trust in the FPGA Supply Chain using Blockchain and Keyless-Signature Technology

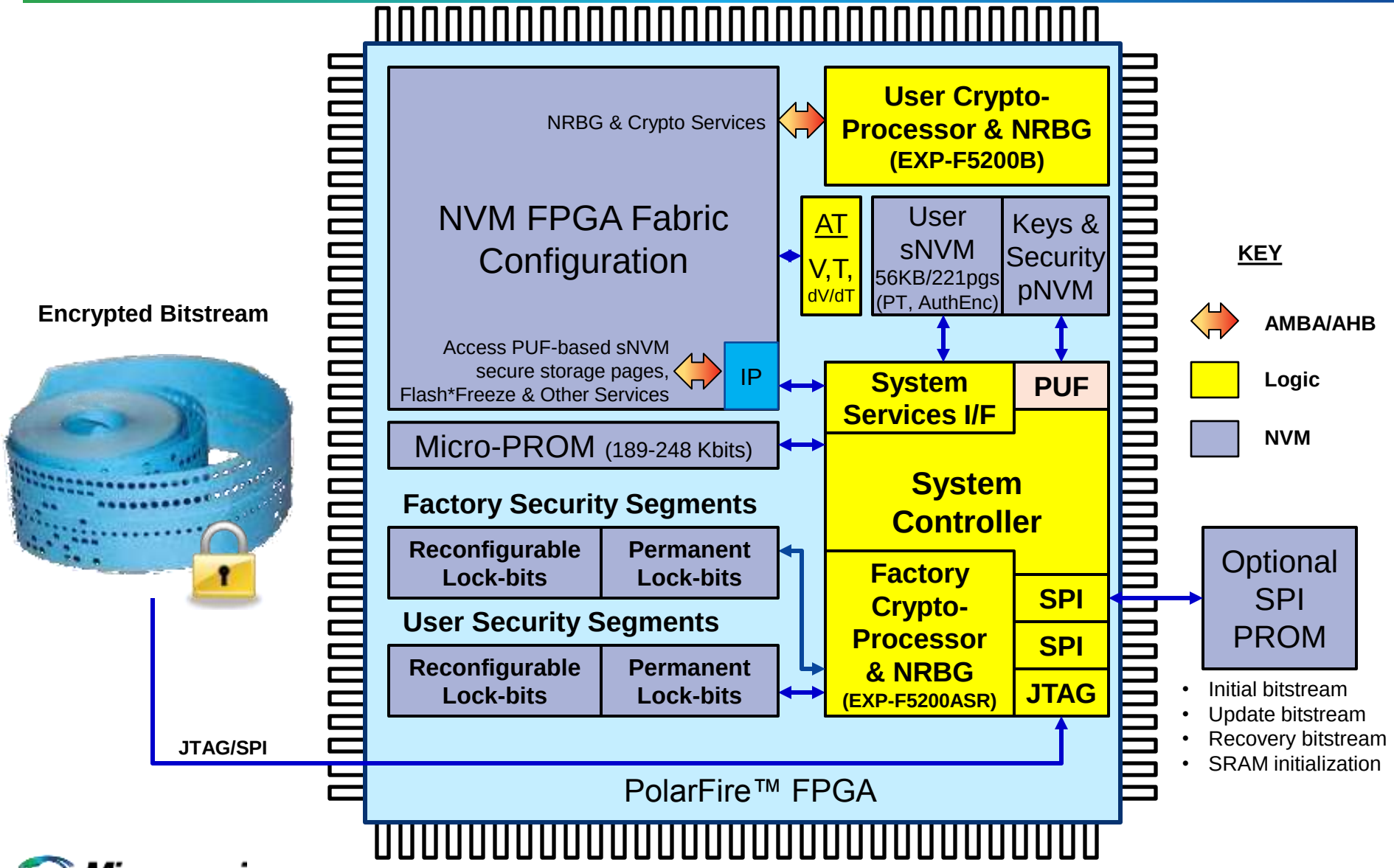
Abstract:

- Blockchain and Keyless Signature Infrastructure (KSI) technologies that only rely on secure message digests and need no secret keys can be used to provide additional assurances that non-volatile FPGA components and systems moving up the supply chain hierarchy from wafer test through to completed systems are trustworthy.
- This is done by providing cryptographic evidence of the FPGA's provenance using a verifiable time-stamped audit trail of key events in the FPGA life-cycle using blockchain and KSI technology, complementing existing traditional measures.
- System manufacturers using those FPGAs can keep appending to the extensible information container that represents the entire history of the FPGA (and eventually the system), strengthening trust in the system, preventing counterfeiting at all levels (component and system), and providing a strong verifiable identity for use in the final run-time application.

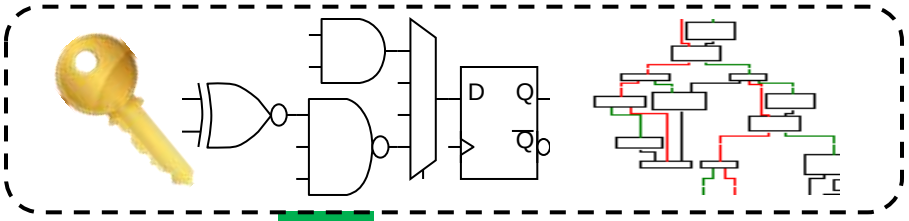
Current Microsemi FPGA Supply Chain Assurance Measures

Implemented and in production for SmartFusion®2, IGLOO®2 and PolarFire™ FPGAs

Simplified PolarFire™ FPGA User Security Model



Digital Certificate-of-Conformance (C-of-C)



- How to prevent insiders and rogue CMs from subverting security intent?
  - E.g., loading their own keys, security settings, or a design with a Trojan Horse?
- Answer: C-of-C detects any fraud

Bitstream

Digest

On-site check

?=?

(May all be the same)

$Digest_1$

$Digest_2$

$Digest_3$

Certificate of Conformance (C-of-C)

Secure check inside HSM

?=?

From Bitstream, S/N, & Key compute MAC and compare

MAC_1

S/N_1	MAC_1
S/N_2	MAC_2
S/N_3	MAC_3

Log File

Message Authentication Codes (MACs) are always unique for each device

Devices that fail programming are zeroized but still generate a C-of-C, if possible

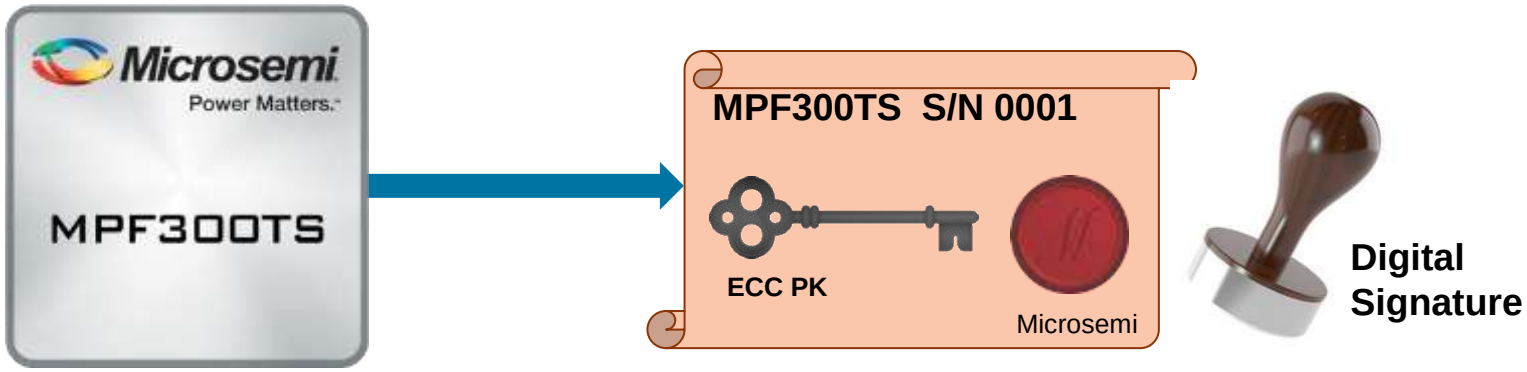
NVM Integrity:
PolarFire FPGA Digest Commands and Services

	JTAG/SPI Command	System Service
Bitstream, IAP, and UIC Authentication Services (external SPI Flash)		X
Export C-of-C tags (during bitstream pgm'g)	X	
Export Digests Stored During Programming (on demand)	X	X
Compute/Export Fresh Digests (on demand)	X	X
Compute/Report Fresh Status Flags (on-demand)	X	X
Compute/Report Fresh Tamper Flag (after Power-on-Reset)		X
Export Zeroization Proof (after zeroization)	X	
Device Integrity Flag (for new devices)	X	
sNVM Authentication (when page is read)		X

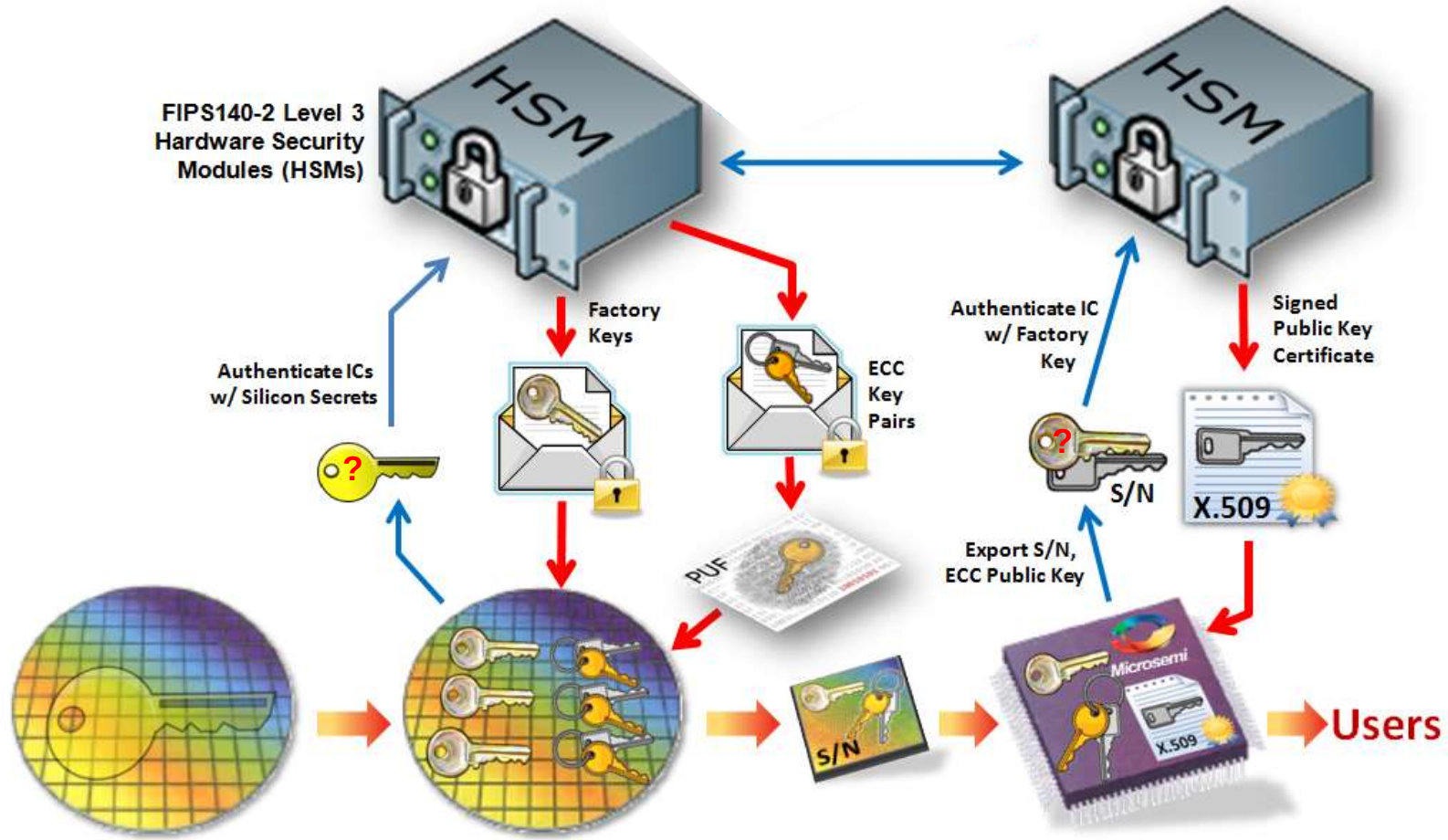
Up to thirteen SHA-256 digests or flags reported, ensuring integrity of the associated NVM

Supply Chain Assurance

- An X.509 conforming certificate digitally signed by Microsemi is stored in each PolarFire device's eNVM
- Certifies integrity and authenticity of contents:
  - Serial number and date code
  - Part Number
  - Includes device's ECC Public Key
- Key verification protocol binds certificate to secret key(s)
- Cryptographically assures customer that each device is…
  - Not counterfeit (nor overbuilt by our fab., nor failed test, etc.)

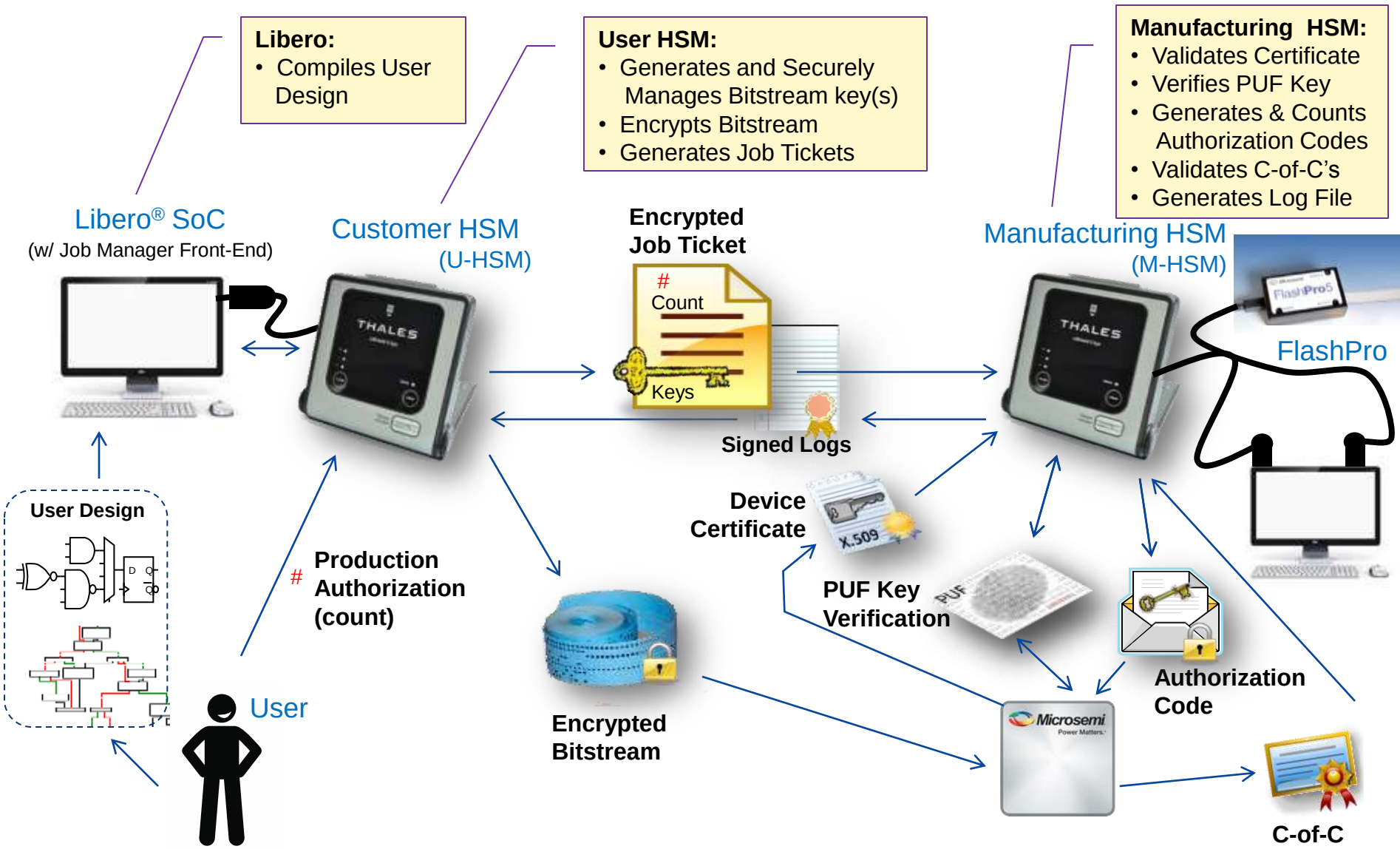


Microsemi HSM-based Manufacturing Flow



SPPS User Device Configuration Data Flow

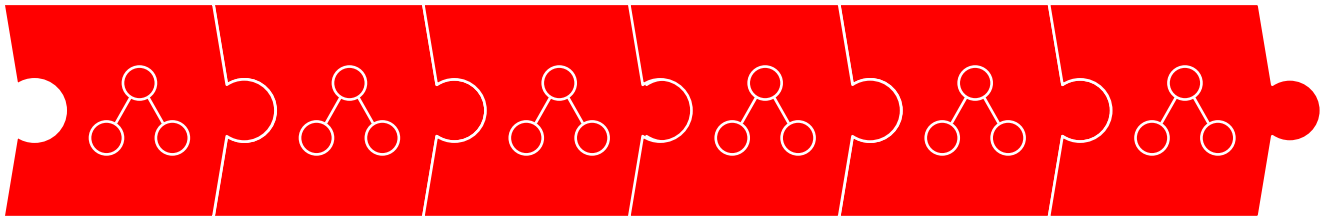
The Secure Production Programming Solution (SPPS)



Guardtime's Keyless Signature Infrastructure (KSI)

Blockchain

Each new block added to the chain includes a message digest (hash) of the previous block



The new block can also contain any kind of digital payload:

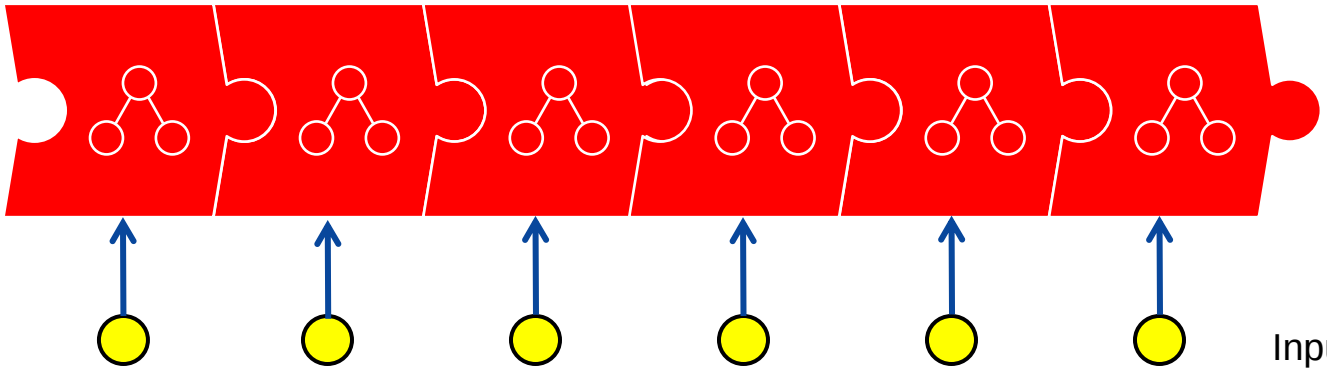
- Ledger entries (e.g., Bitcoin transactions)
- Contracts, documents to record
- Etc.

Public or Private Blockchains? Examples:

- Bitcoin is based on a public blockchain
  - "Proof of Work" entitles someone to add a new block (and earn a reward)
- The Guardtime private blockchain requires prior authorization to submit data to (no proof of work requirement)

GuardTime's Calendar Blockchain

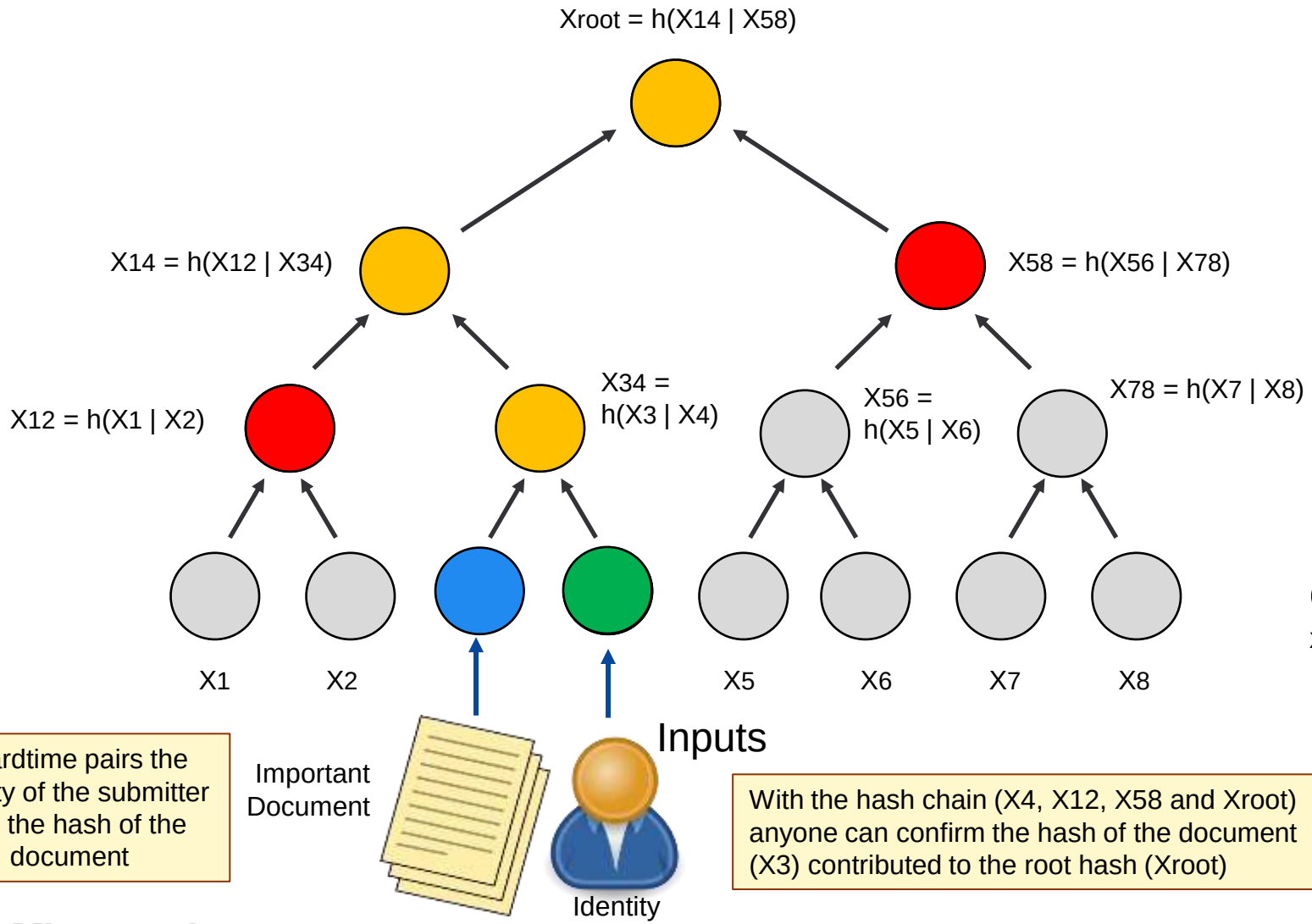
Adds a block once per second (since "Unix Time" began in 1970)



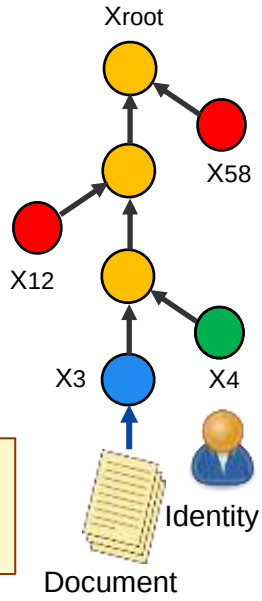
The payload for each added block consists of a single SHA-256 hash value (one per second)

(You will see where this hash comes from shortly)

Merkle Hash Tree Aggregates Inputs



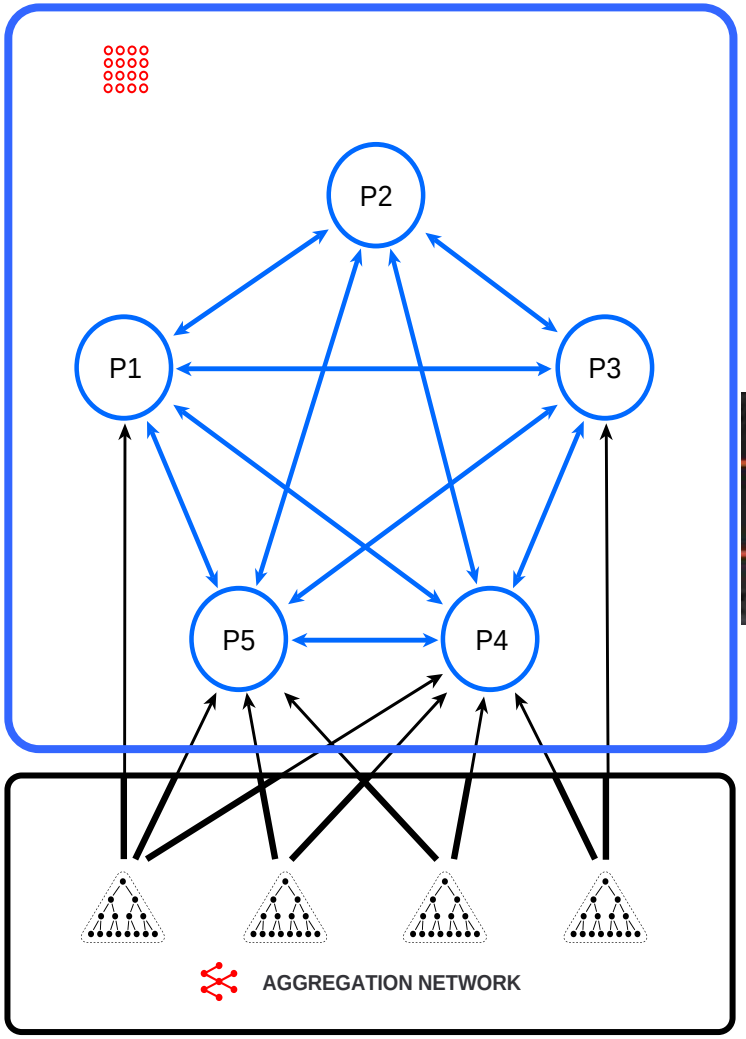
Hash Chain



Guardtime pairs the identity of the submitter with the hash of the document

With the hash chain (X4, X12, X58 and Xroot) anyone can confirm the hash of the document (X3) contributed to the root hash (Xroot)

Core Network for Distributed Consensus



The core network comprises multiple geographically distributed security-hardened servers: Guardtime's Black Lantern™ Security Appliance (HSM)

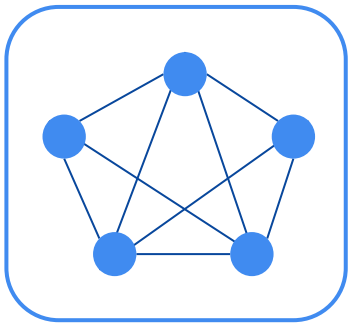
Core servers receive root hashes from the Aggregation Network (Merkle hash trees) and arrive at a consensus about the hash for each round (second), adding it to the calendar blockchain

Calendar Blockchain w/ Published Trust Anchor

WIDELY WITNESSED PUBLICATION
IN ELECTRONIC AND PHYSICAL MEDIA

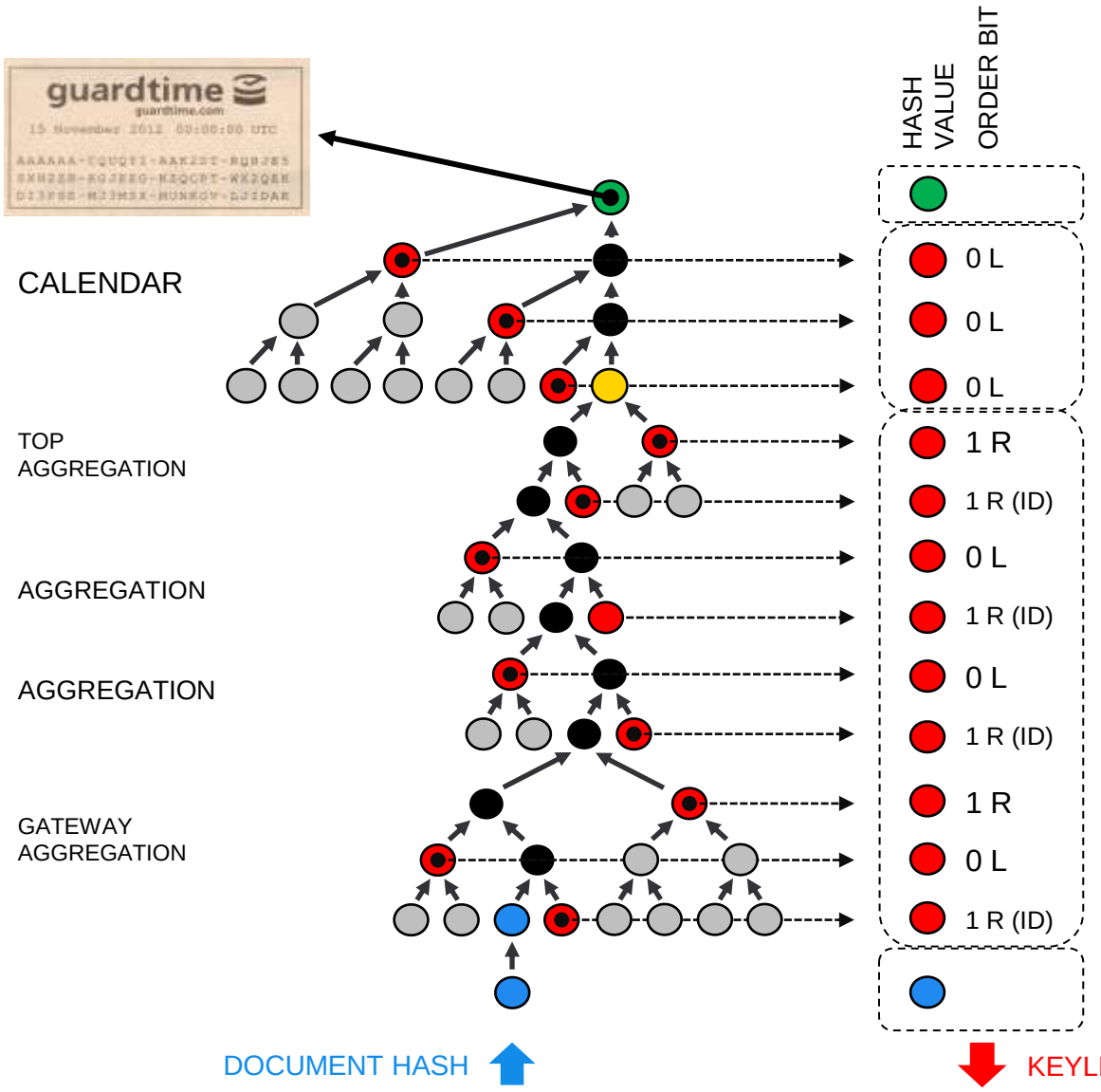
CALENDAR BLOCKCHAIN WITH ENCODED TIME

TIME



The consensus root hash becomes the payload
for the current “round” of the blockchain

Keyless Signature



KSI Signature Verification
PKI based Trust Anchor

Option 1 – Calendar Authentication Record (“Key-based” verification)

- The publication code in the signature is signed by the core node with a PKI certificate, and embedded in the KSI signature.
- If the PKI Signature is valid,
- And the PKI certificate is trusted, then
- The KSI signature is verified.

PUBLICATION HASH | SIGNING TIME | CORE NODE PRIVATE KEY | CALENDAR AUTHENTICATION RECORD EMBEDDED IN KSI SIGNATURE

KSI Signature Verification

Widely-witnessed publication based Trust Anchor

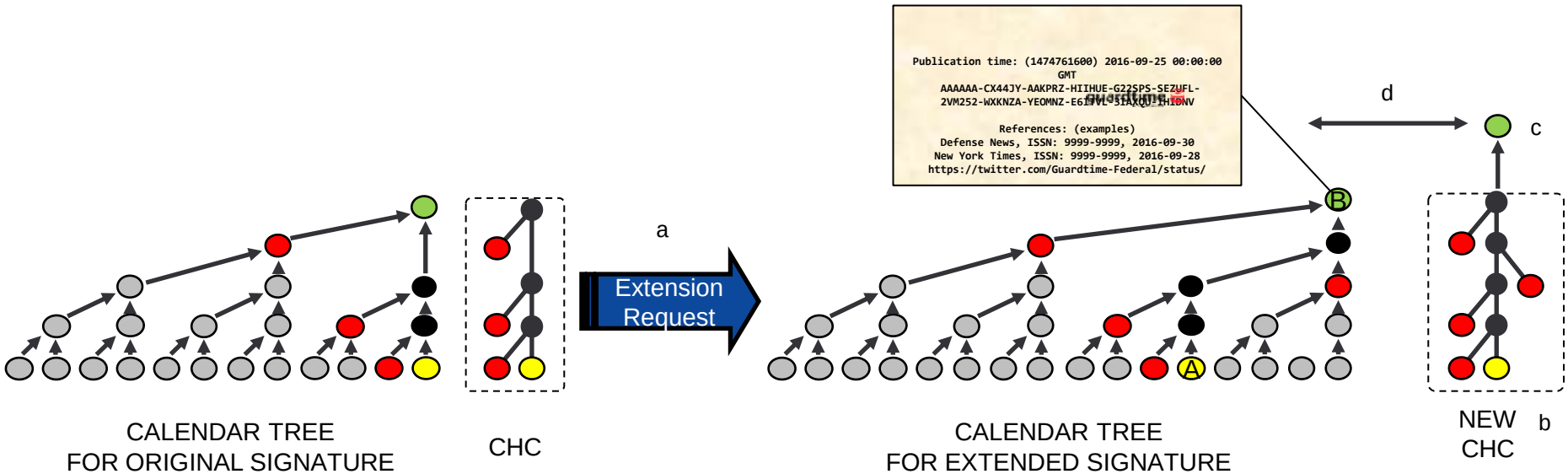
Option 2 – “Extend” the KSI Signature

a. Client requests extension of KSI Signature to later date/time.

b. Extender returns CHC required to get from Aggregation Top Hash (A) at signing time to Publication Hash (B) at later time.

c. Client calculates Publication Hash with Aggregation Top Hash and new CHC.

d. Client compares calculated publication hash to “widely-witnessed” value.



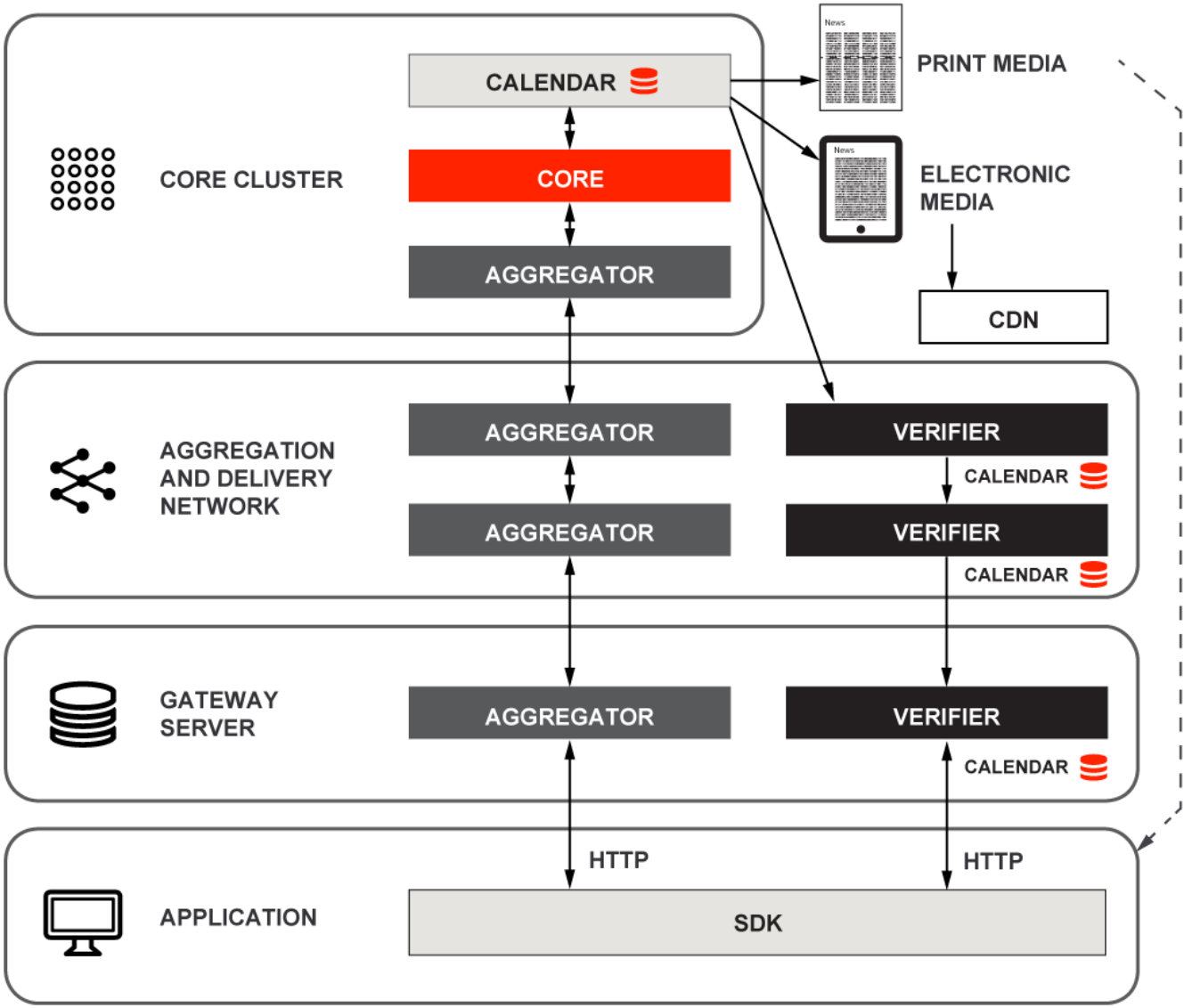
The Keyless Signature Infrastructure

Core Cluster
- Develops consensus and securely adds resulting leaf to the calendar blockchain each second

Aggregation Network
- Provides geographical reach and scale for the system

Gateway Server
- Customer facing server that provides signing and verification services (incl. calendar hash chain extension)

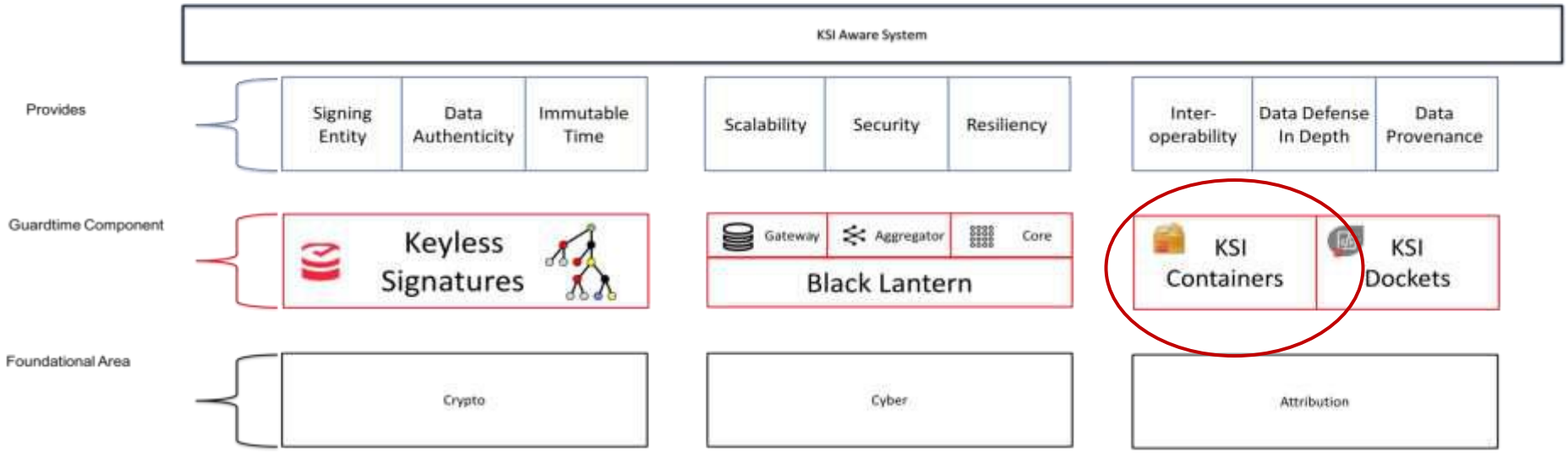
Applications
- KSI-enabled applications request signatures and perform verification.

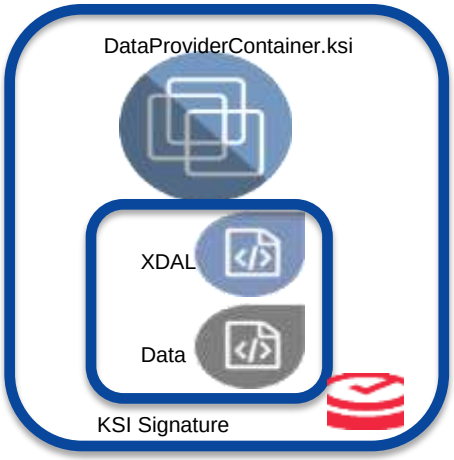


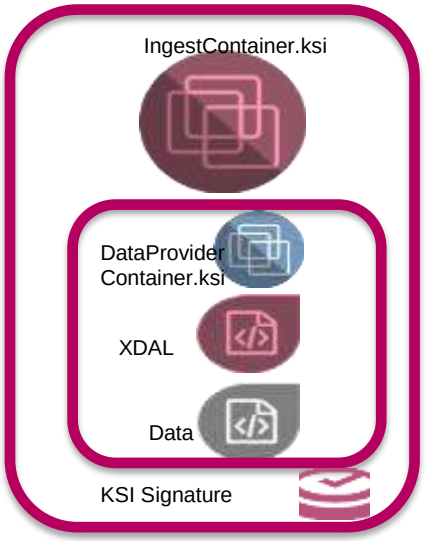
Discussion

- Privacy: KSI does not ingest any customer data; data never leaves the customer premises.
- Scale: KSI performance is practically independent of the number of clients or amount of data signed / verified. Proof of participation is provided in about 2 seconds of request and is not subject to “rollback.”
- Open Verification: For KSI Signature verification, one needs to trust publicly available information only - verification does not rely on trusted insiders or security of key-stores.
- Portable: Data can be verified even after crossing geographical or organizational boundaries or service providers.
- Offline: The KSI system does not require network connectivity for verification.
- Supports Real-time Protection: KSI Signature verification requires milliseconds, which allows clients to perform continuous monitoring and tamper detection.
- Long-term validity: Proof is based only on the properties of cryptographic hash functions and does not expire.
- Post-Quantum: The proof stays valid even assuming functioning quantum computers, i.e. does not rely on traditional asymmetric or elliptic curve cryptography.
- Carrier Grade: The KSI system architecture is able to deliver 99.999% availability.

KSI Containers
Extensible Data Attribution Language (XDAL)



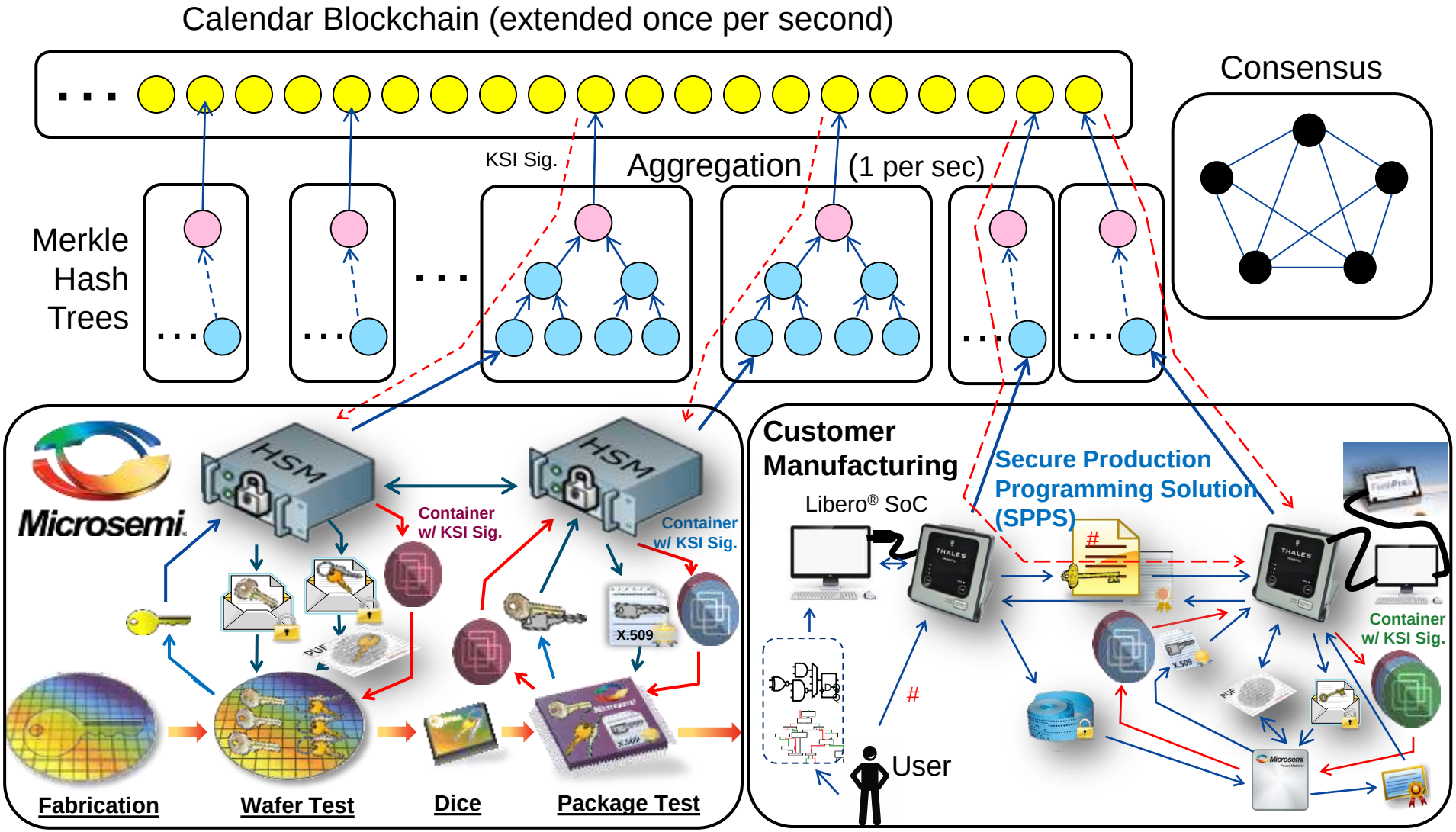




- Containers may wrap any type of data from a hash to a full video
- Containers can ingest other containers (nest-able)

Conceptual FPGA Supply Chain Provenance Application of KSI and XDAL Data Containers

Guardtime Keyless Signature Infrastructure (KSI)
Applied to Microsemi (& User) Trusted Manufacturing Flows



Blockchain records immutable audit trail of key events in device & system lifecycles, supplying provenance

Thank You!

Questions?

Richard Newell
richard.newell@microsemi.com
+1 408 643 6146