

Quantum Safe Code Signing

A case study in HSMs

Thales Trusted Cyber Technologies



Luna HSMs Protect Traditional and Emerging Technologies

Emerging

Traditional



Perform **post-quantum** crypto securely



Secure **5G** data



Secure **digital signatures**



Secure **PKI** root keys



Create secure digital IDs for **IoT** and **secure manufacturing**



Protect **Non-Person Entity** identities

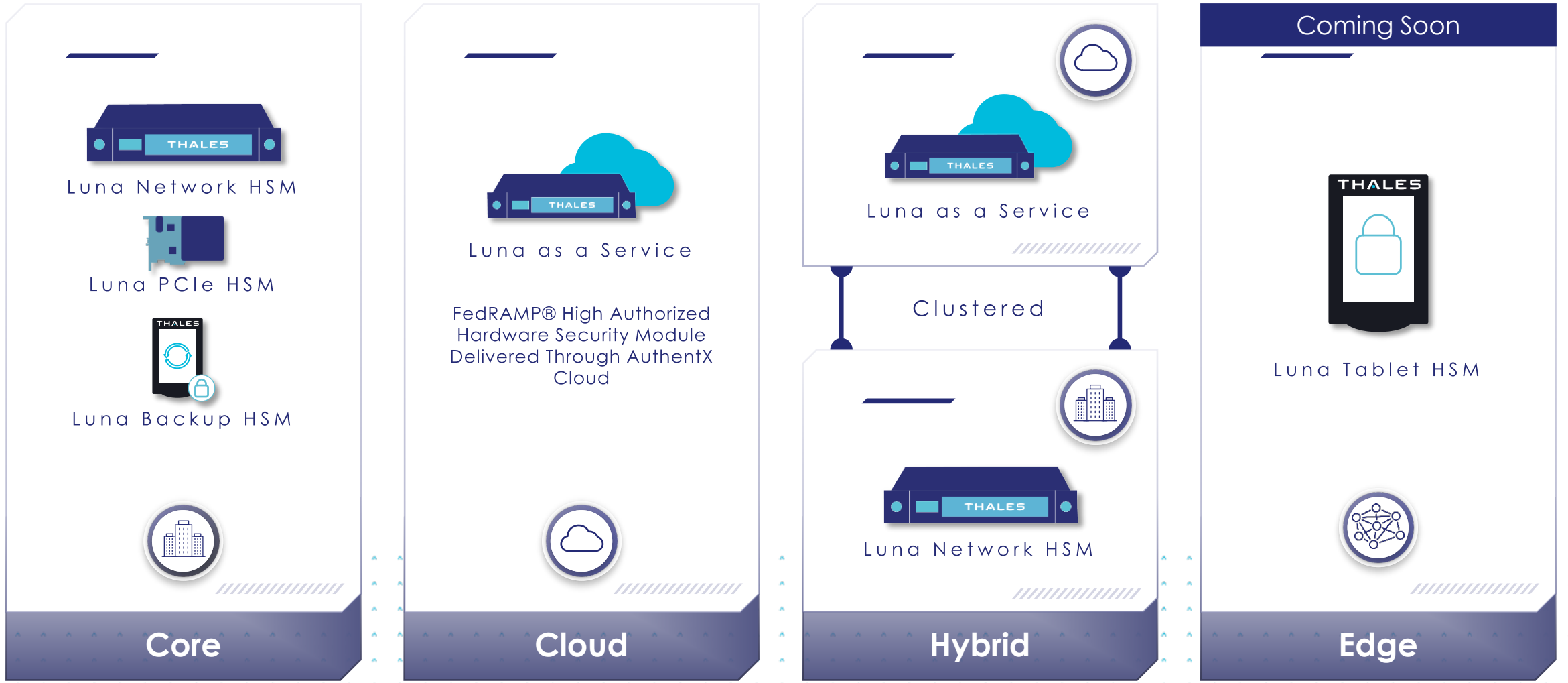


Ensure software integrity with **code signing**



Maintain key ownership in the **cloud**

Root of Trust Anywhere You Need It

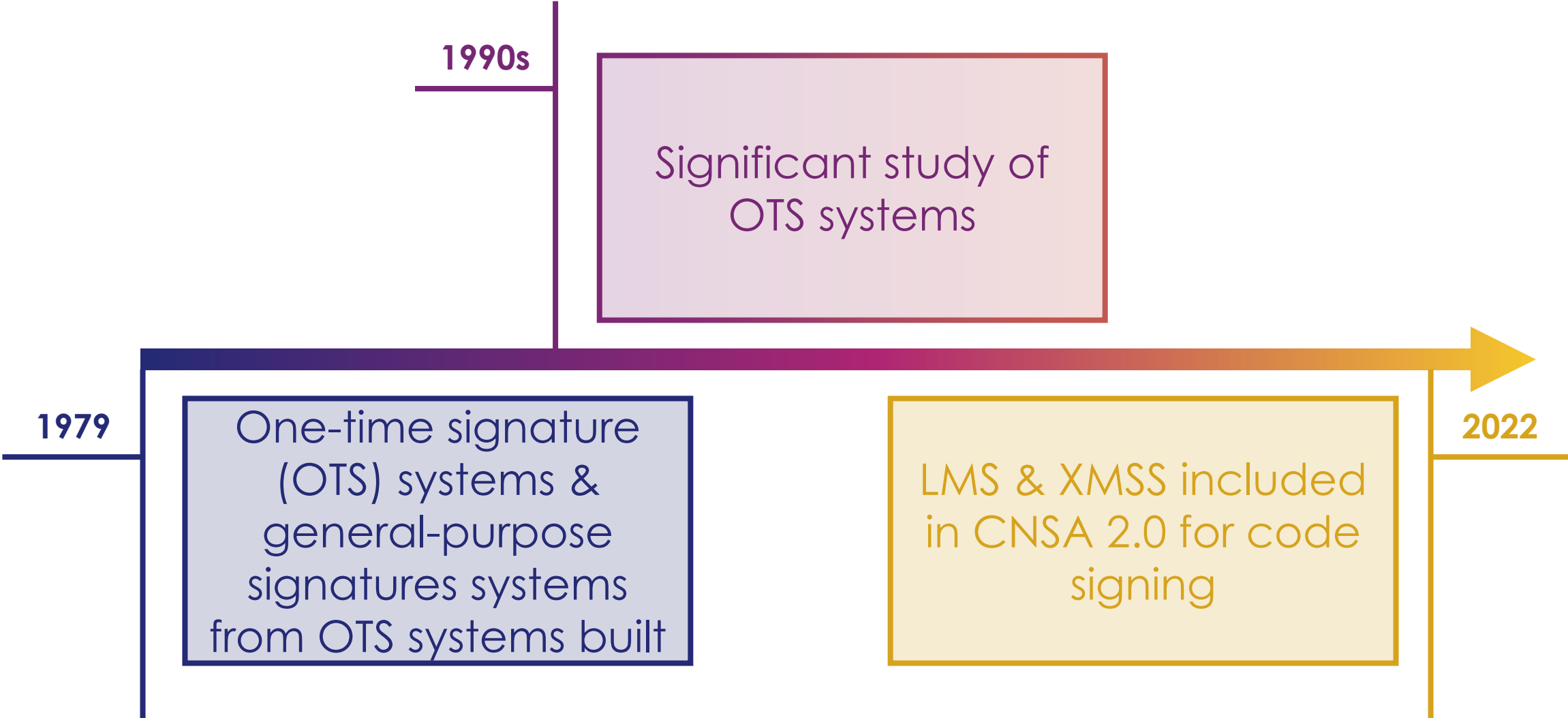


Stateful Hash Based Signature Schemes

An Overview

Thales Trusted Cyber Technologies

A Brief Timeline



Comparing LMS to Classical Algorithms

Public & Private Key Sizes



Quantum Resistant

Signature Generation, Verification Times



Advantages

Disadvantages



Signature Sizes



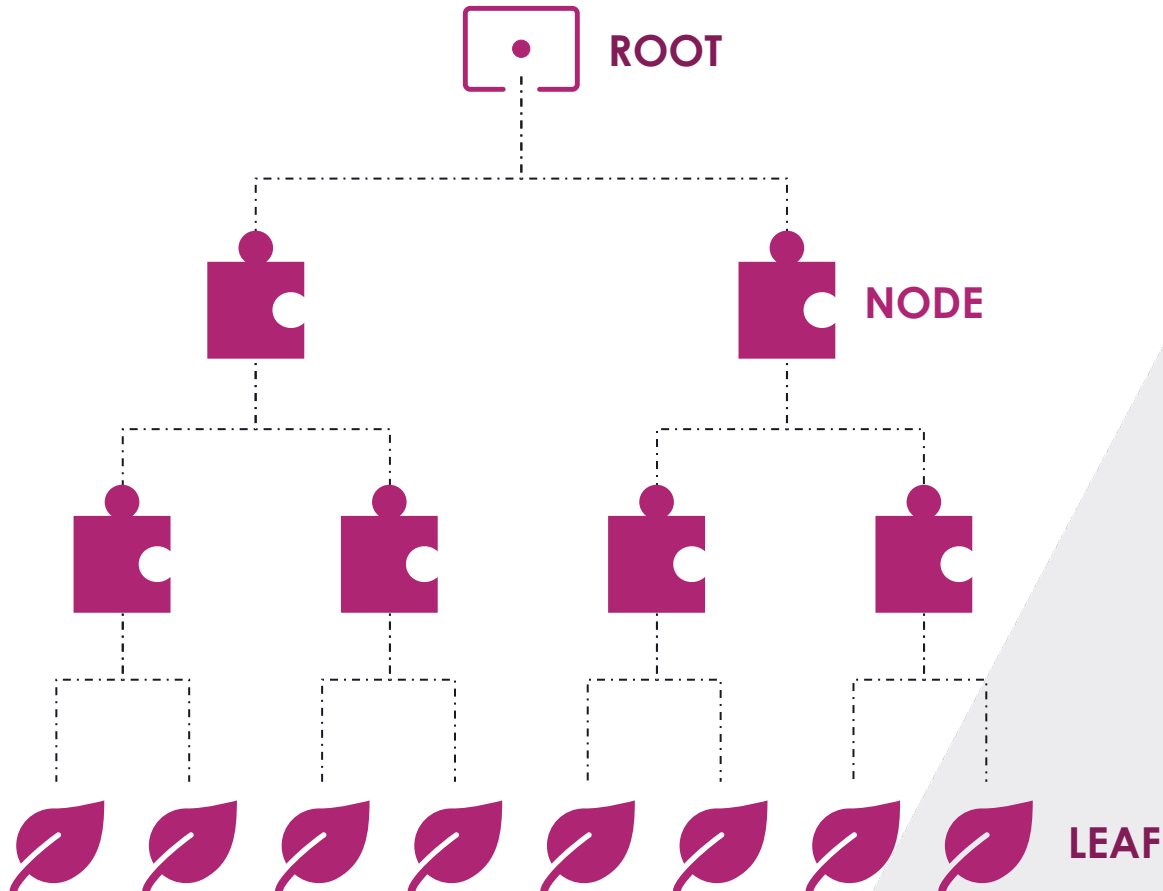
Key Generation Time

as compared to RSA & ECDSA

Comparing LMS to Classical Algorithms

| | LMS \ HSS 2-Tier (H10) | LMS \ HSS 3-Tier (H10) | ML-DSA Level 5 | SPHINCS+ 256 bits | RSA 4096 bits |
|------------------|---------------------------|---------------------------|-------------------|----------------------|------------------|
| Signature Size | 2,912 bytes | 4,368 bytes | 4,595 bytes | 49,856 bytes | 512 bytes |
| Private Key Size | 324 bytes | 324 bytes | 4,864 bytes | 128 bytes | 512 bytes |
| Public Key Size | 172 bytes | 172 bytes | 2,592 bytes | 64 bytes | 512 bytes |

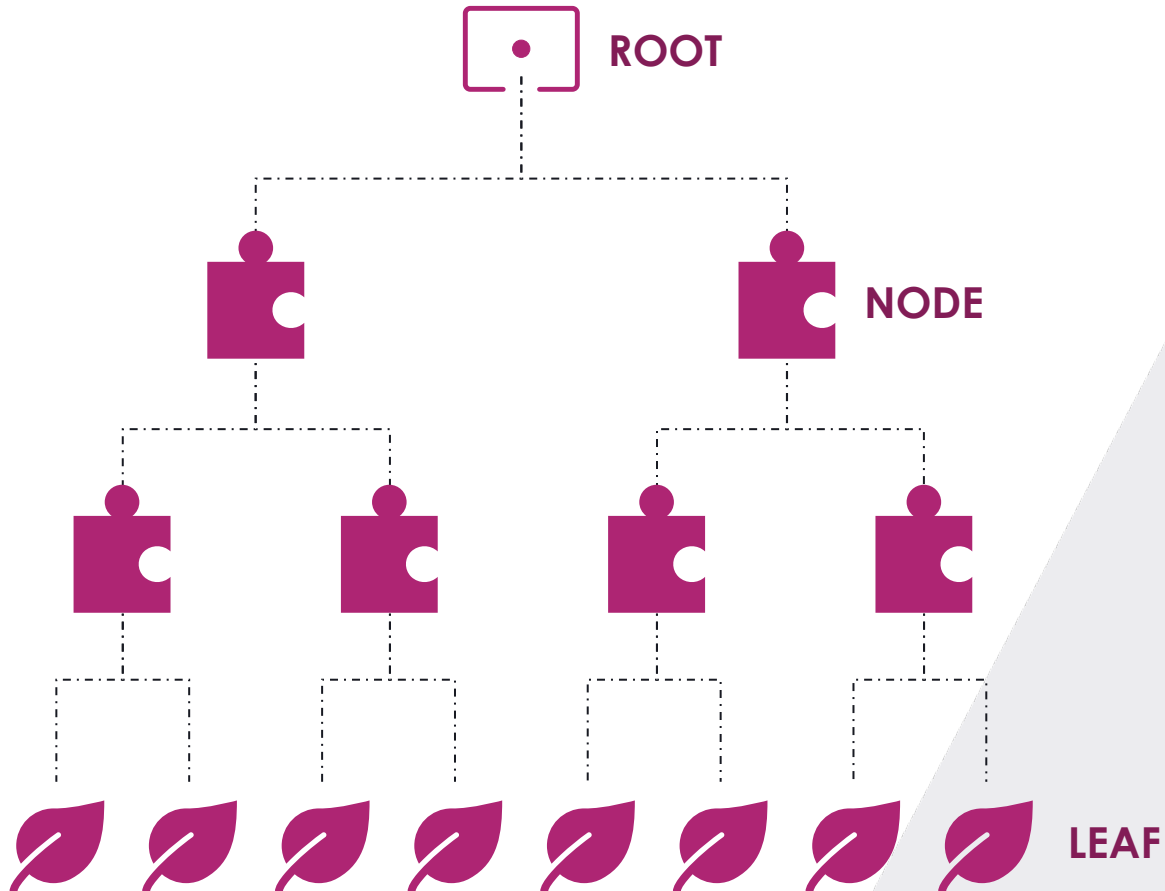
LMS Merkle Trees



An LMS system has the following characteristics:

- > The height of the Merkle tree
 - > Total OTS capacity = 2^h
- > Interior nodes of certain byte lengths
 - > Each a hash of its two children
- > A second-preimage-resistant cryptographic hash function (e.g., SHA256; SHA256-192)

LMS Statefulness



Statefulness

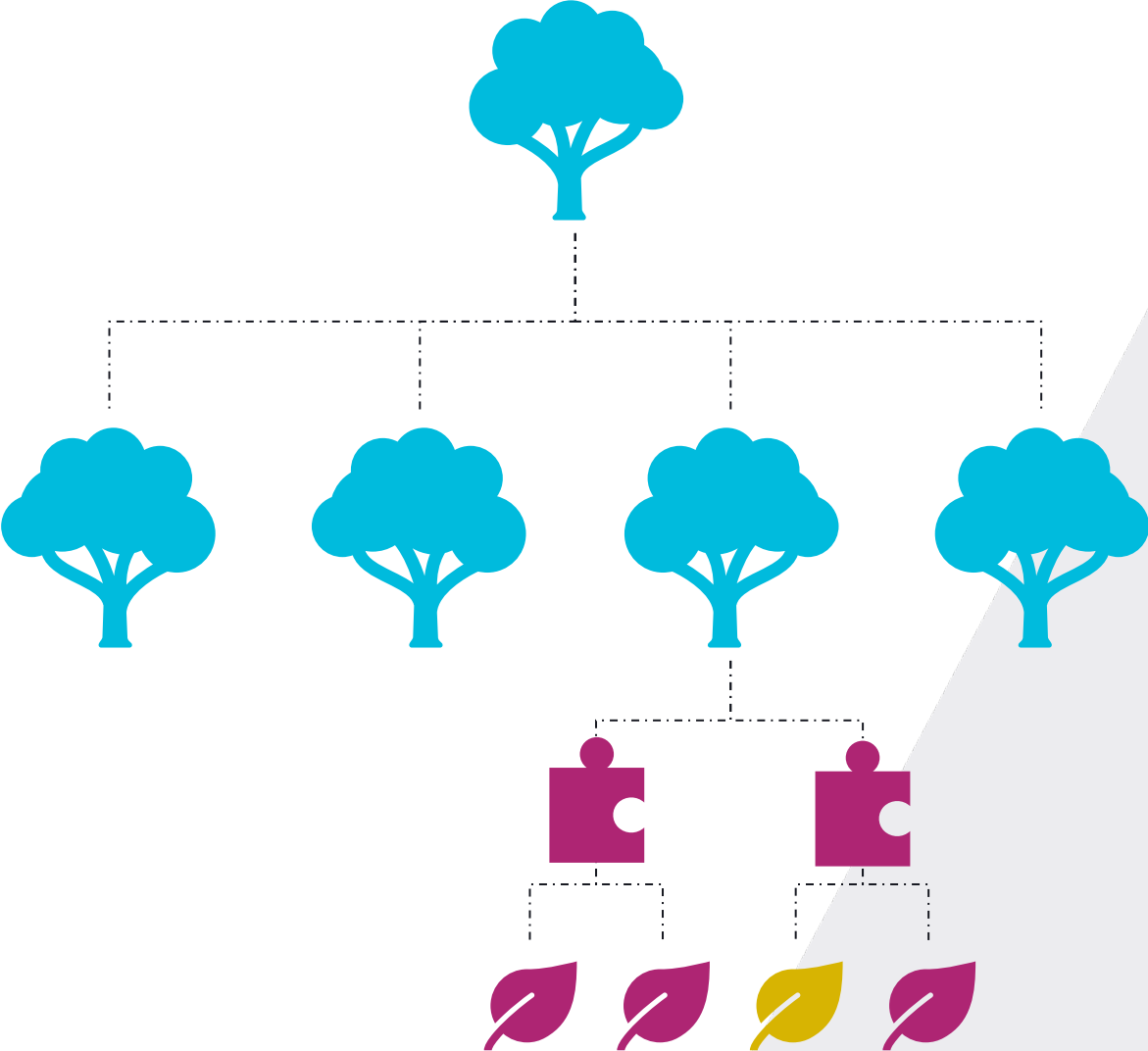
- > Tracking the index of used keys
- > Key reuse breaks security



- > SP 800-208 requires use of HSM to enforce indexing by single authority



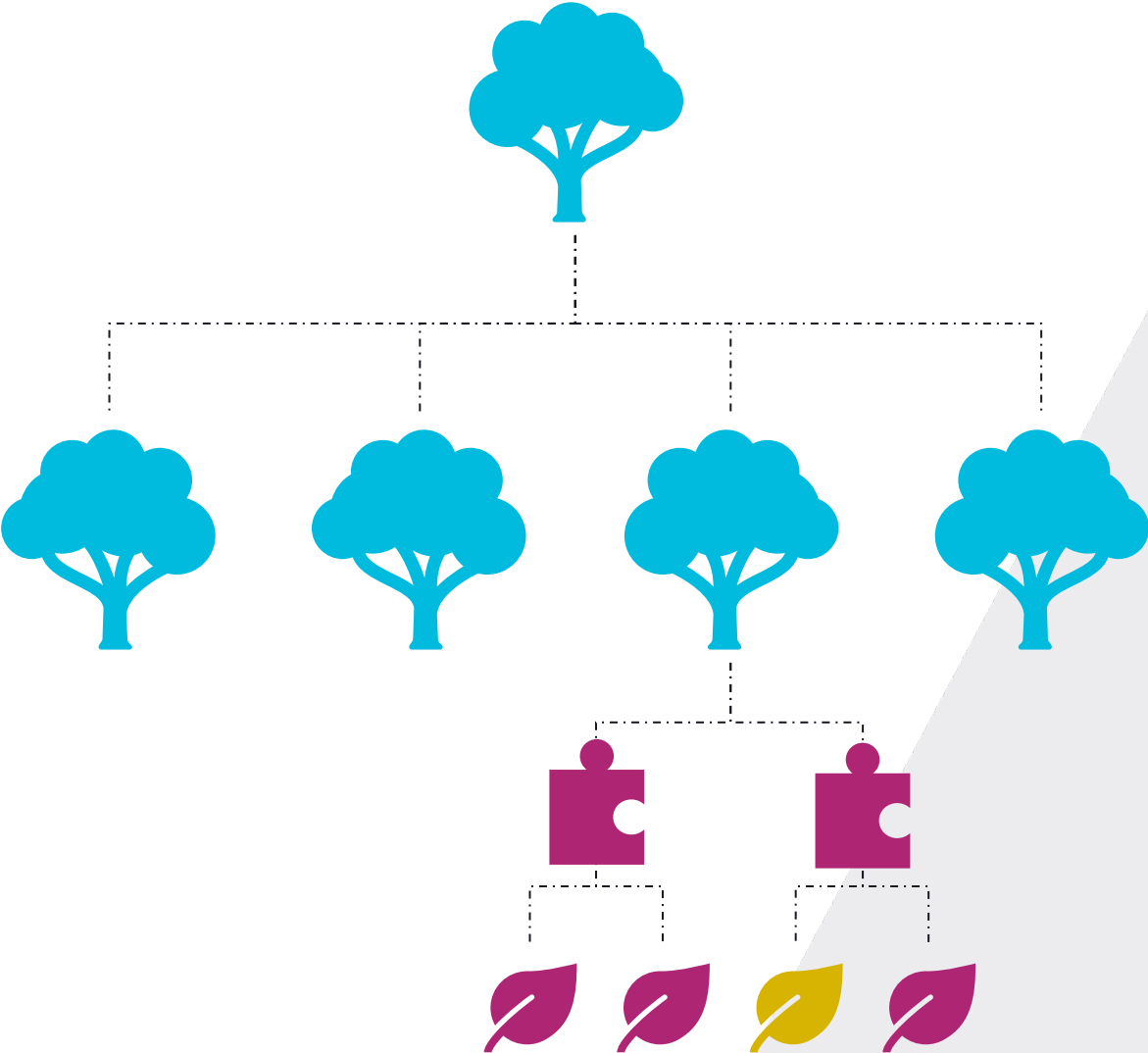
Hierarchical Signature System (HSS)



Hierarchical Signature System

- > Sequence of LMS trees
- > OTS private keys of parent sign Public Keys of children trees
- > OTS private keys of lowest tier children sign messages

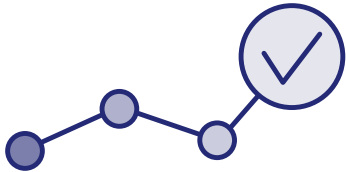
HSS vs XMSS



HSS Advantages over XMSS



x4 Faster
using SHA256

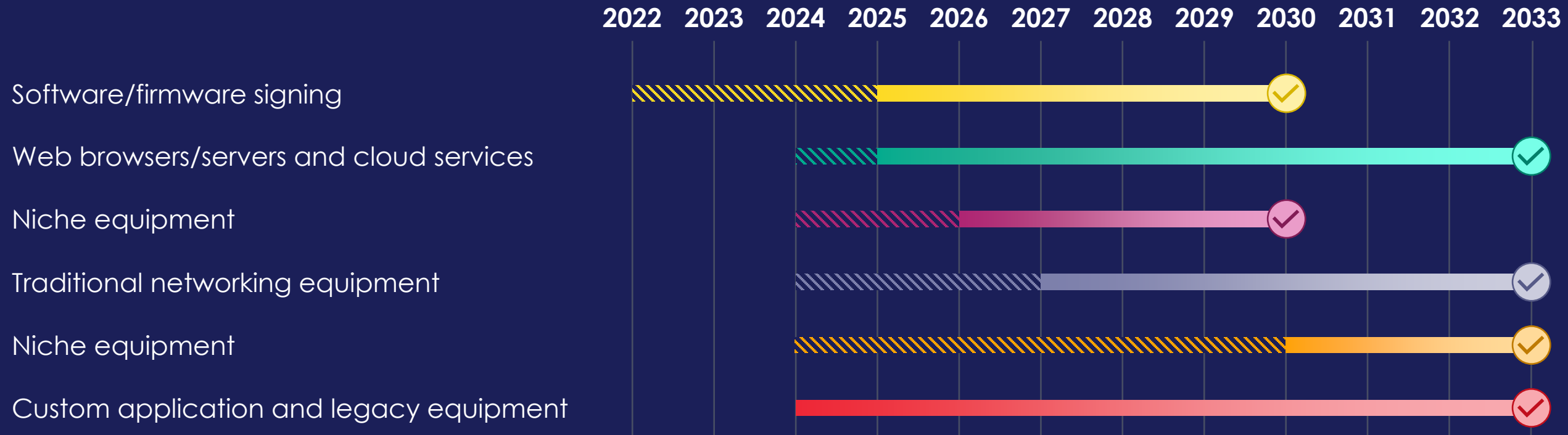


Simpler
Implementation

Why SHBS Schemes

Thales Trusted Cyber Technologies

CNSA 2.0



- CNSA 2.0 added as an option and tested
- CNSA 2.0 as the default and preferred
- Exclusively use CNSA 2.0 by this year

LMS & XMSS prescribed for use in **Software/firmware signing** as specified in NIST SP 800-208

Why Stateful Hash-Based Signature (SHBS) Schemes

Urgency

Firmware deployed now may be in service well after quantum threat becomes real

Standards

NIST SP 800-208 codifies standards for HBS

Other PQC algorithms will not be standardized until 2024

Cryptanalysis

HBS have been extensively researched

Potential performance impacts non-critical to software/firmware signing use case

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

Why Stateful Hash-Based Signature (SHBS) Schemes

Urgency

Firmware deployed now may be in service well after quantum threat becomes real

Standards

NIST SP 800-208 codifies standards for HBS

Other PQC algorithms will not be standardized until 2024

Cryptanalysis

HBS have been extensively researched

Potential performance impacts non-critical to software/firmware signing use case

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

Why Stateful Hash-Based Signature (SHBS) Schemes

Urgency

Firmware deployed now may be in service well after quantum threat becomes real

Standards

NIST SP 800-208 codifies standards for HBS

Other PQC algorithms will not be standardized until 2024

Cryptanalysis

HBS have been extensively researched

Potential performance impacts non-critical to software/firmware signing use case

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

The HSM Challenge

Thales Trusted Cyber Technologies



Managing State

Key Reuse

Reuse of One-Time Signature keys introduces cryptographic vulnerabilities into the signature scheme

NIST's Priority

Preventing key reuse is highest priority

External key storage or process-dependent controls insufficiently protect against key reuse

HSM Implementation

Similar to operating HSMs in Cloning (no private key export) mode

Additional challenges in redundancy and backups

HSM Challenge

SP 800-208 requires implementation in HSMs

Private Keys cannot be copied in anyway

- No cloning among multiple HSMs
- No backups

SP 800-208 describes two methods by which to achieve redundancy

- Scenario 1: End points configured to accept keys from independent roots
 - Scenario 2: Use of hierarchical trees distributed across HSMs

Example Deployment

Thales Trusted Cyber Technologies

HSS Example Deployment – SP 800-208 Compliant

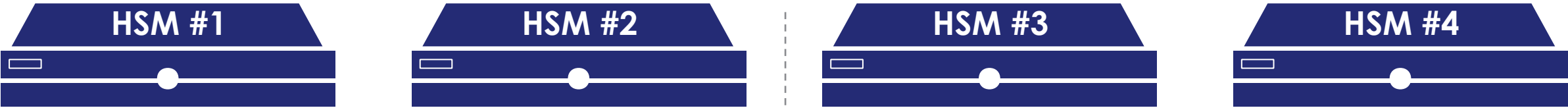
Vendor Requirements

- ▶ The vendor has **four (4)** product lines
- ▶ Each product line must have an independent PKI root
- ▶ Each product will accept firmware signatures from a only a single root
- ▶ Signature sizes cannot fluctuate over the lifespan of the products
- ▶ The vendor averages **one (1)** signature per workday per product
- ▶ Each product line has a lifespan of **25 years**
- ▶ Thus requiring **6,500 signatures** per product, **26,000 total**
- ▶ The vendor has **four (4)** Thales Luna Network HSMs in two (2) regions
- ▶ Redundancy must accommodate loss of **3 of 4** HSMs

Proposal #1 The Basics

Thales Trusted Cyber Technologies

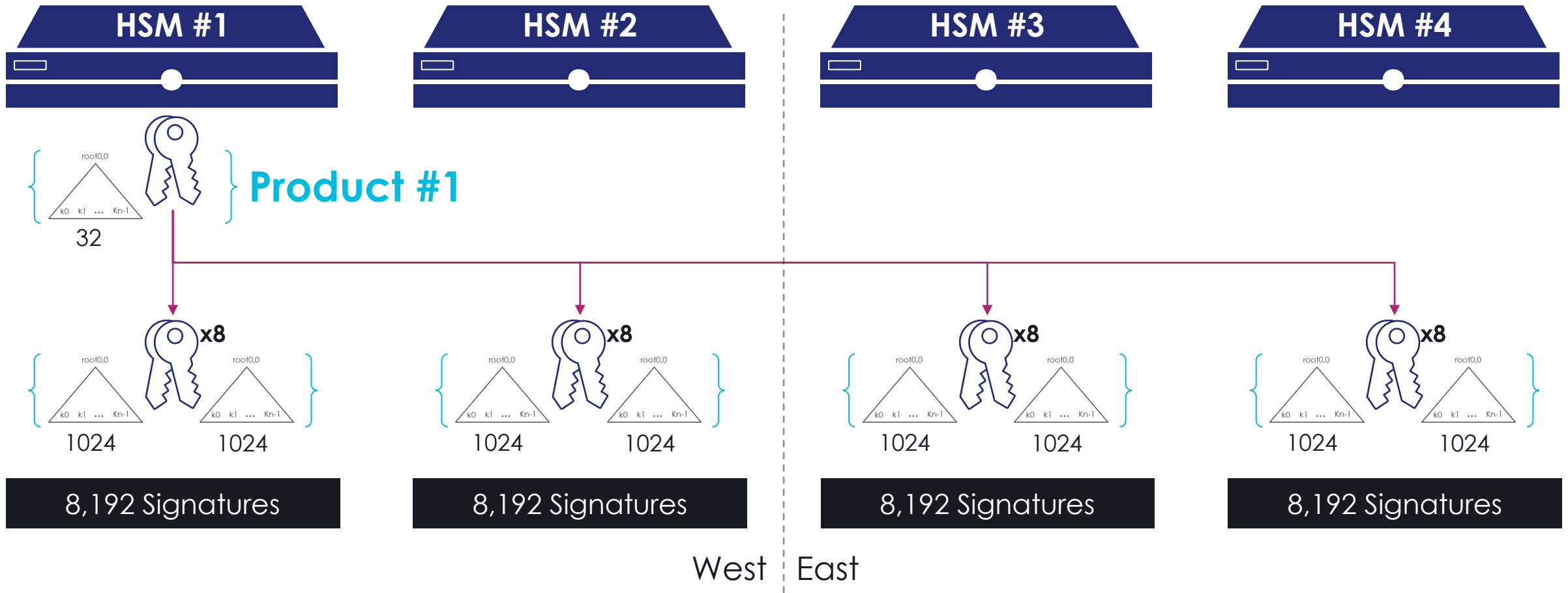
Proposal #1: Setup



West | East

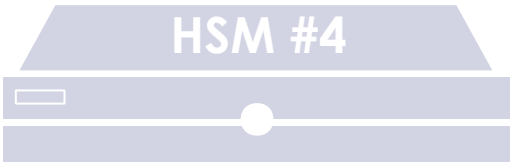
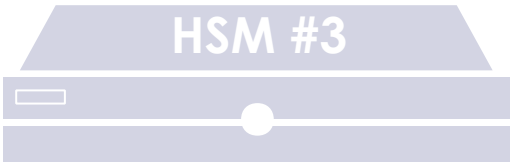
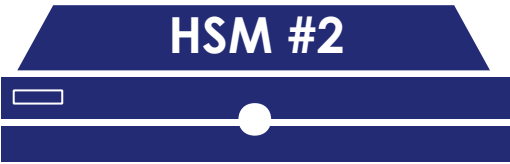
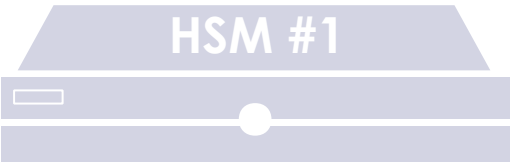
Root Key created for each Product

Proposal #1: Setup

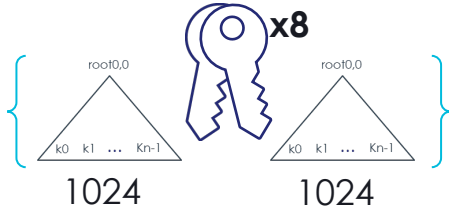


Root Keys used to sign Signing Keys (x30) for each product, distributed across all 4 HSMs

Proposal #1: Loss Tolerance



Per Product



8,192 Signatures

8,192 Signatures

8,192 Signatures

8,192 Signatures

West | East

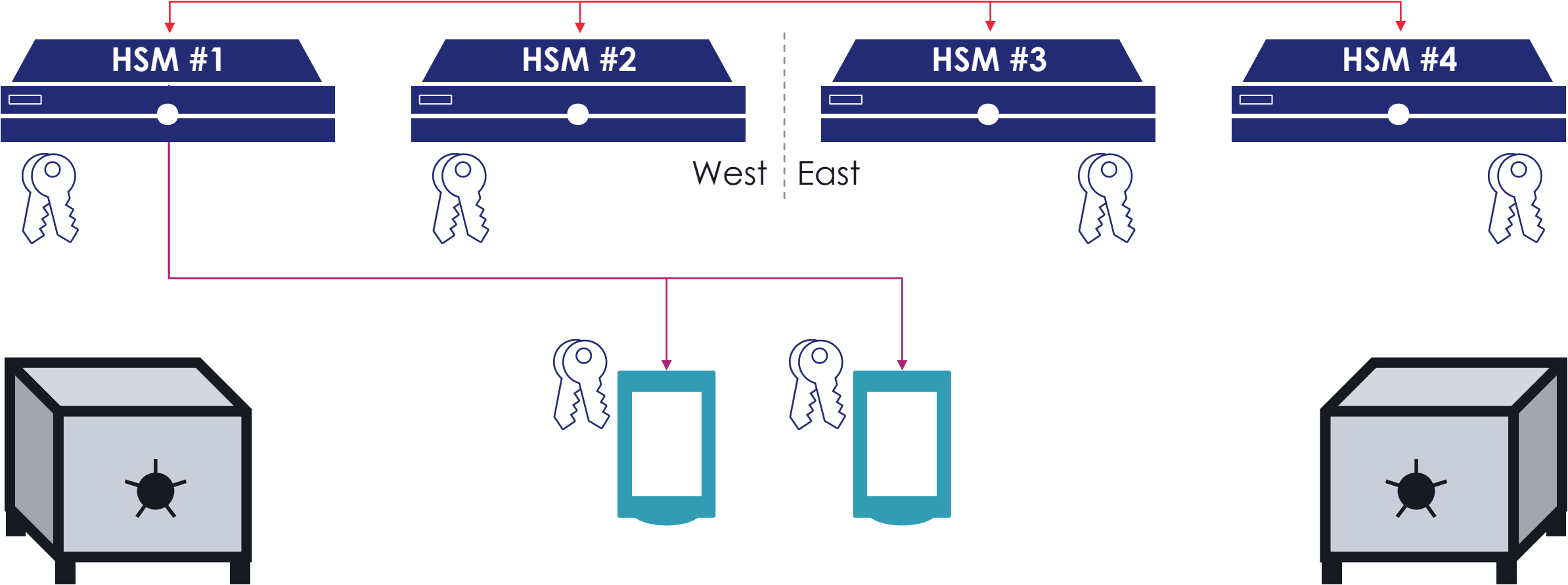
Solution tolerates loss of any individual HSM (up to 3 of 4)

Proposal #2 Offline “Backups”

Thales Trusted Cyber Technologies

Offline Backups – Stateless Keys

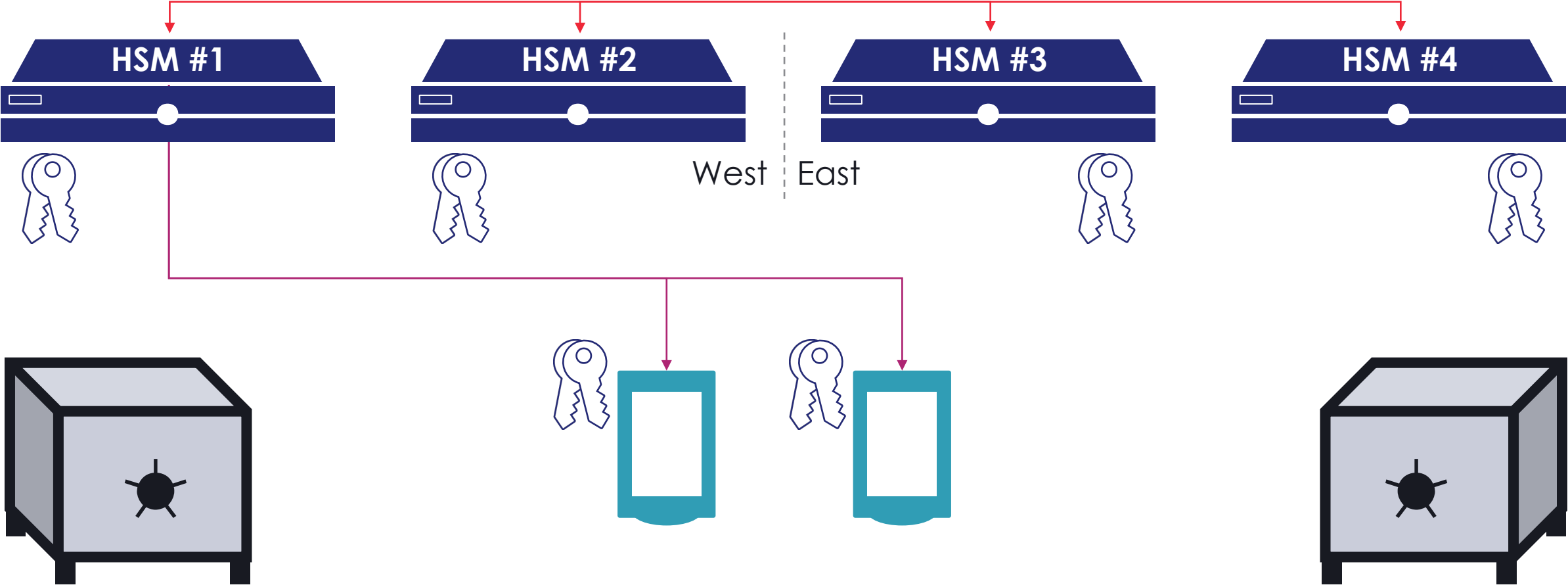
HA Group



Stateless keys are replicated among HA group members & cloned to Backup HSMs

Offline Backups – Stateless Keys

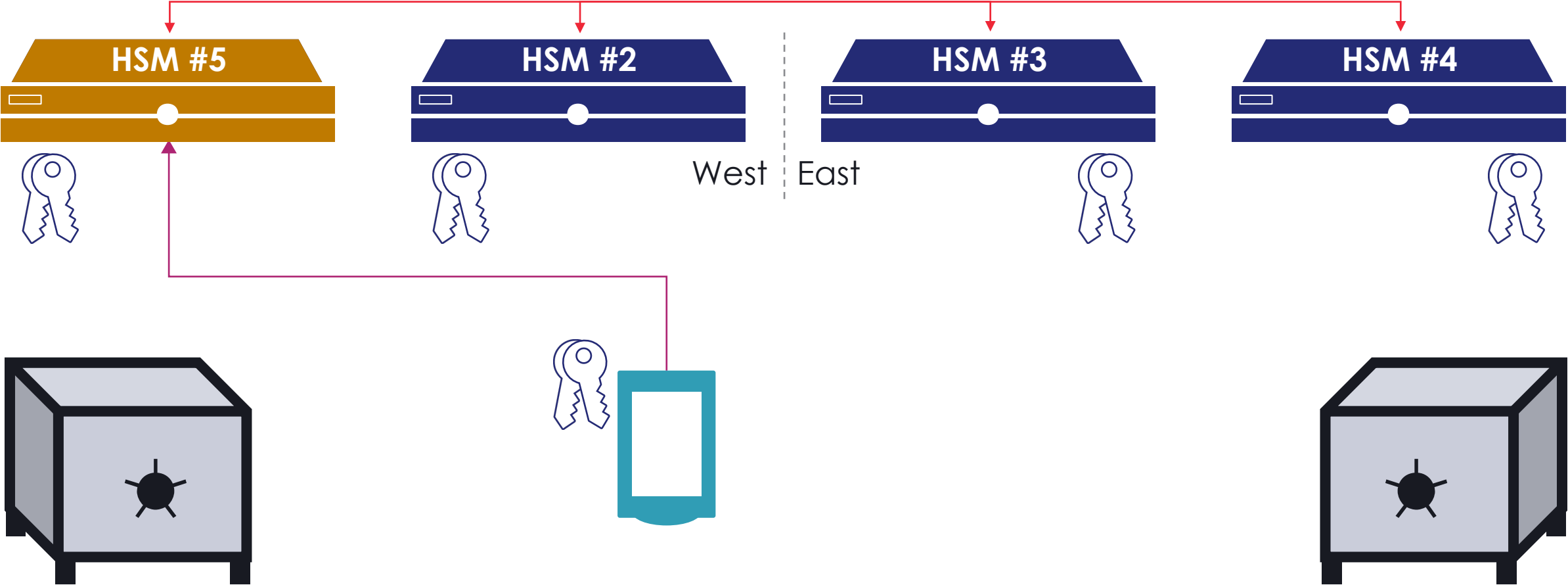
HA Group



Backup HSMs stored offline

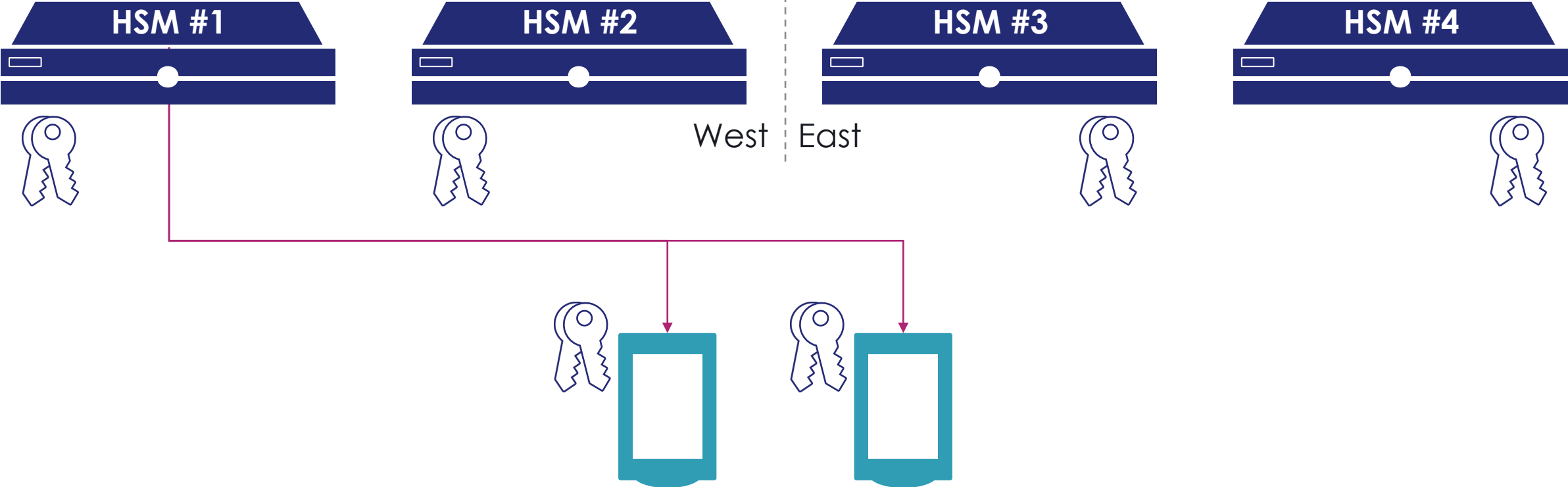
Offline Backups – Stateless Keys

HA Group



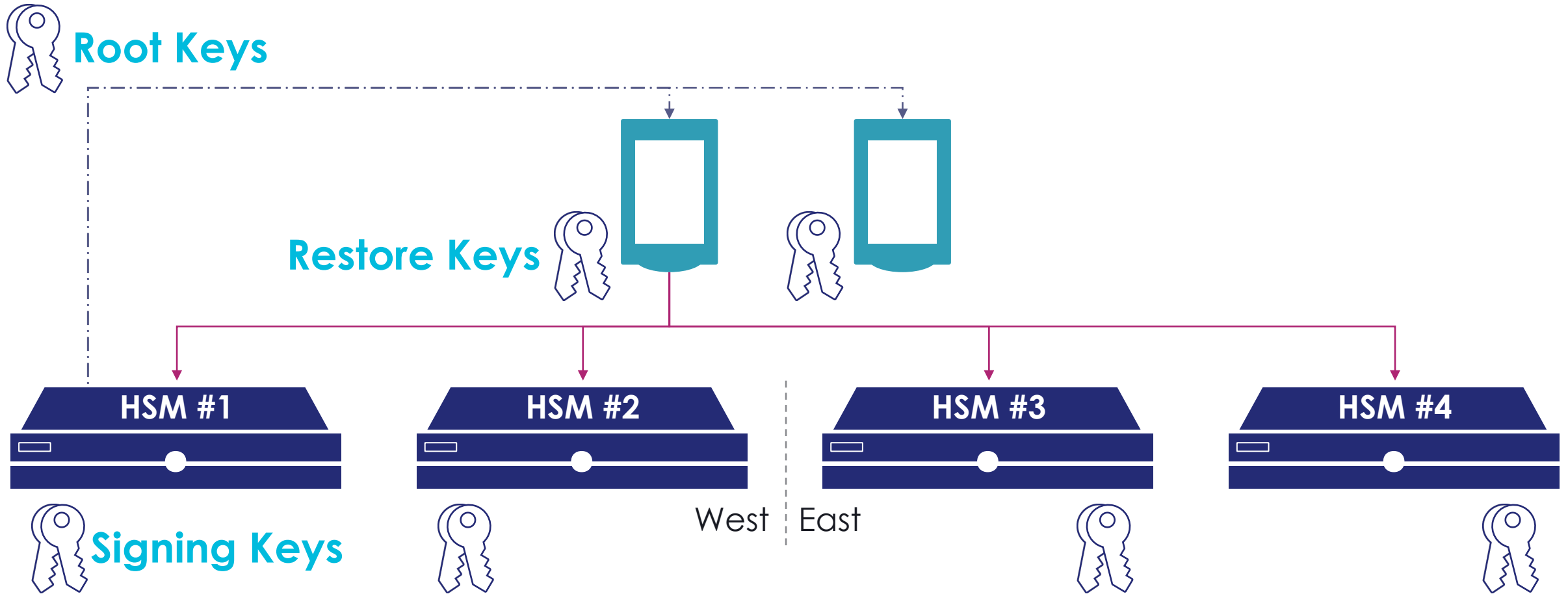
In the event of HSM loss or generation upgrade, key can be restored by HA Group or offline Backup

Offline “Backups” – Stateful Keys



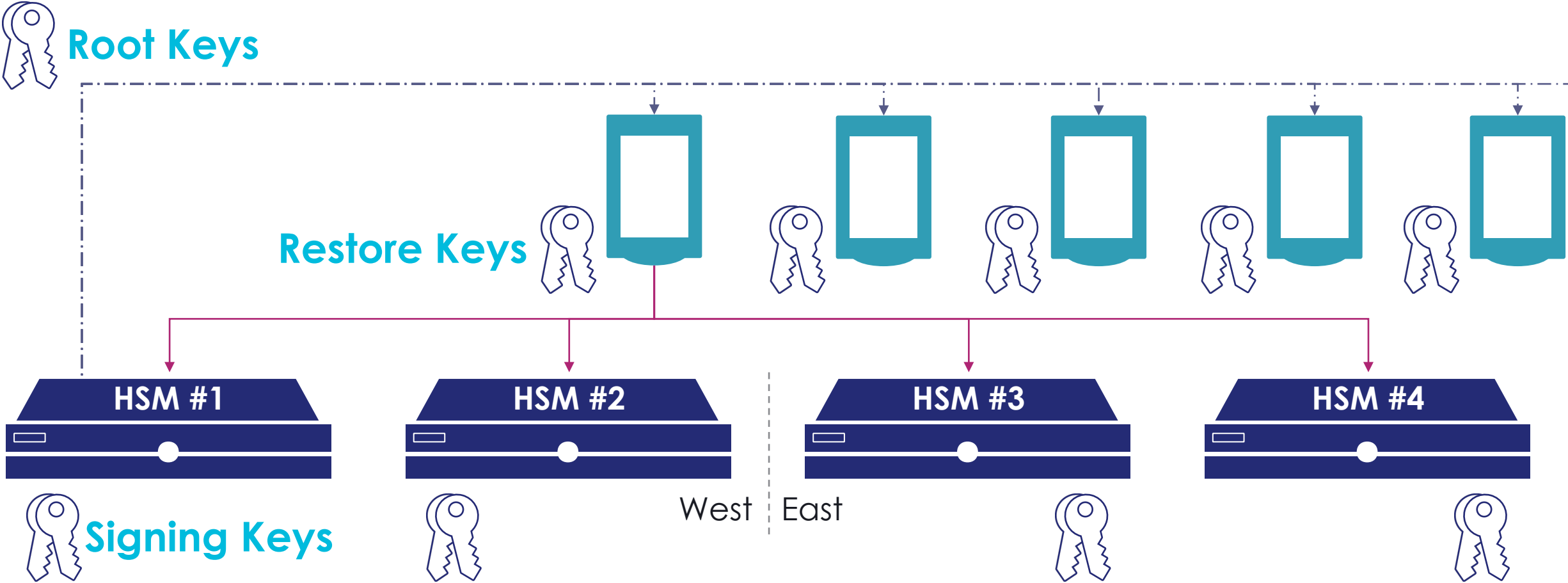
For stateful keys, invert this architecture...

Proposal #2: Offline “Backups” – Setup



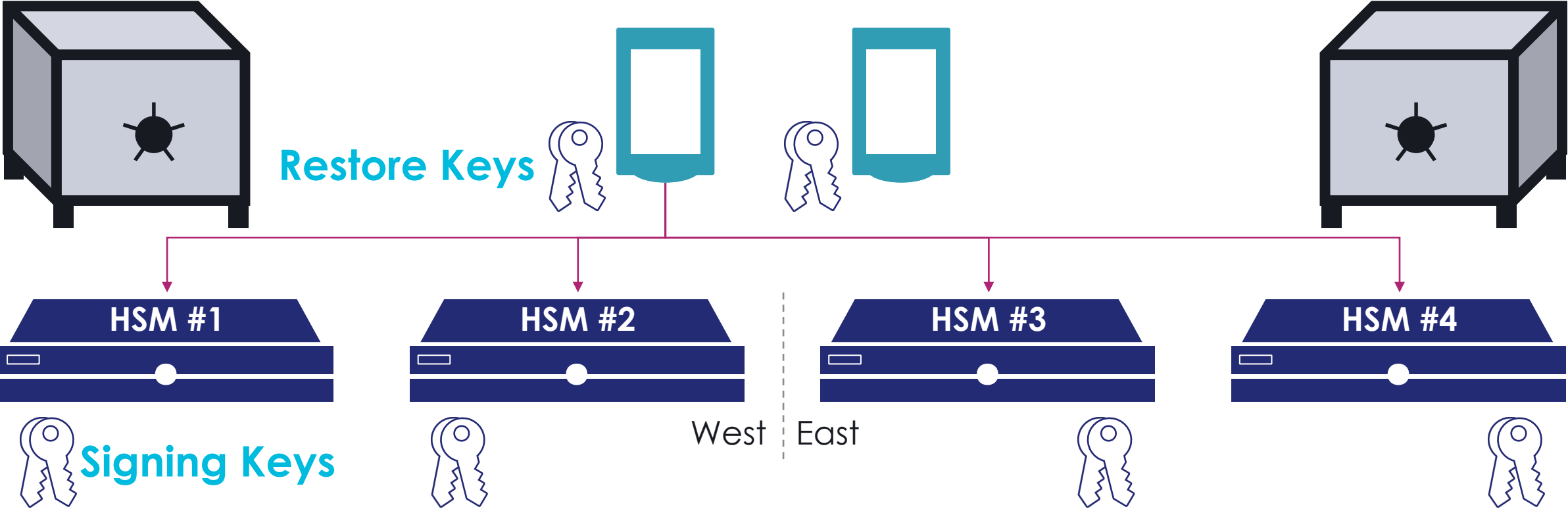
Generate Root Keys on HSM #1, Restore Keys on USB HSMs, and Signing Keys as before

Proposal #2: Offline “Backups” – Setup



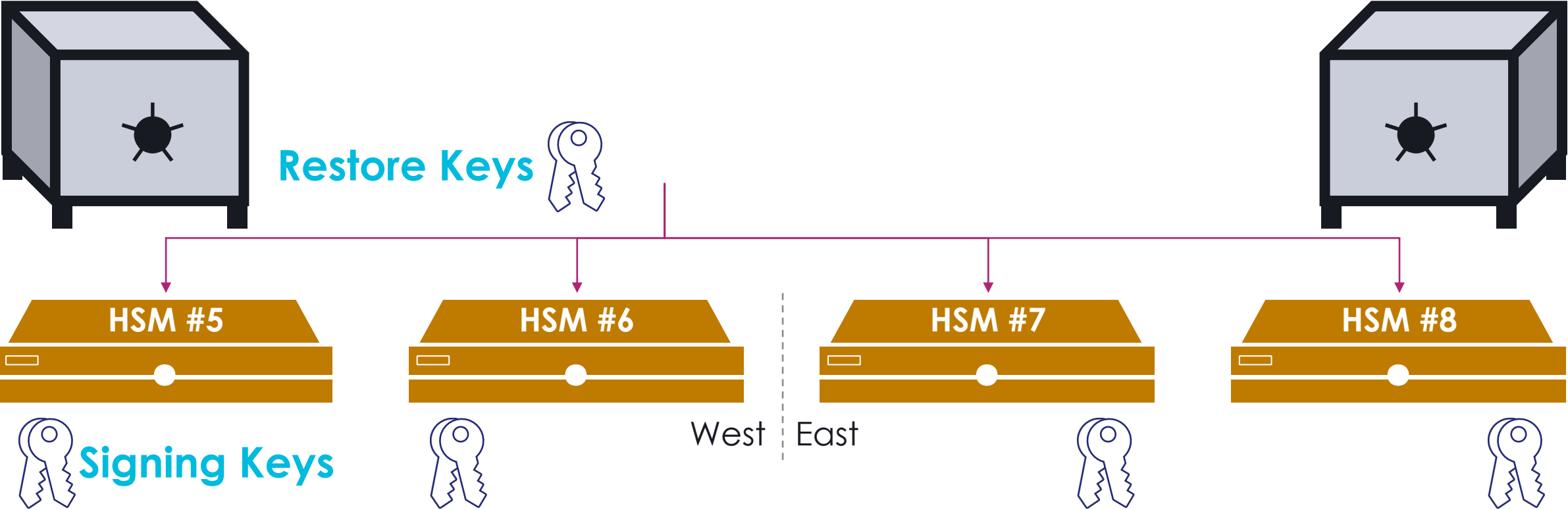
Use Root Keys to establish desired quantity of “backup” USB HSMs, then discard

Proposal #2: Offline “Backups” – Setup



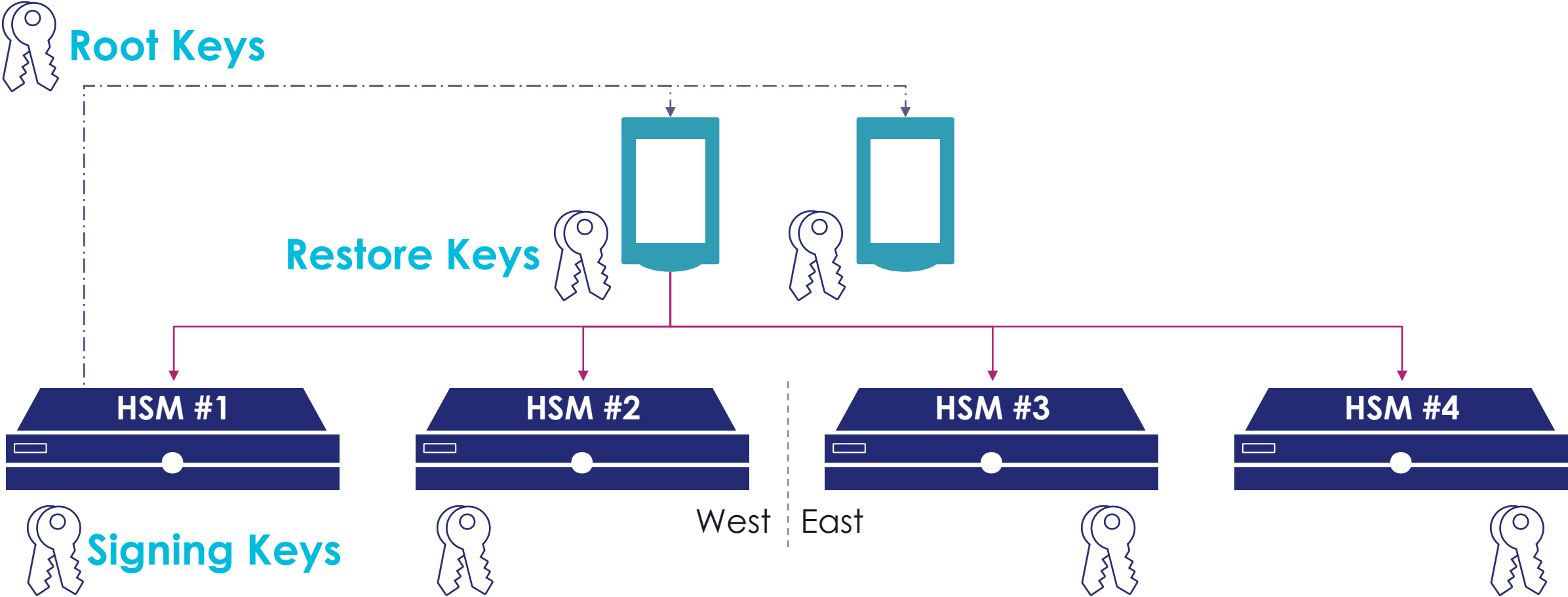
USB HSMs can be stored and treated like a typical Backup HSM device

Proposal #2: Offline “Backups” – Loss Tolerance



New Signing Keys can be spawned by Restore Keys to recover from loss or add new HSMs

SP800-208 §7.1 Compliant Solution





Thank you!

Evan Pelecky

Product Manager
Cryptographic Key Management

 **443-484-7076**

 **evan.pelecky@thalestct.com**