Post-Quantum

Cryptography Conference

Stateful Hash based Signatures: Practical Enhancements and Lessons learned

Volker Krummel
Chapter Lead PQC at Utimaco

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

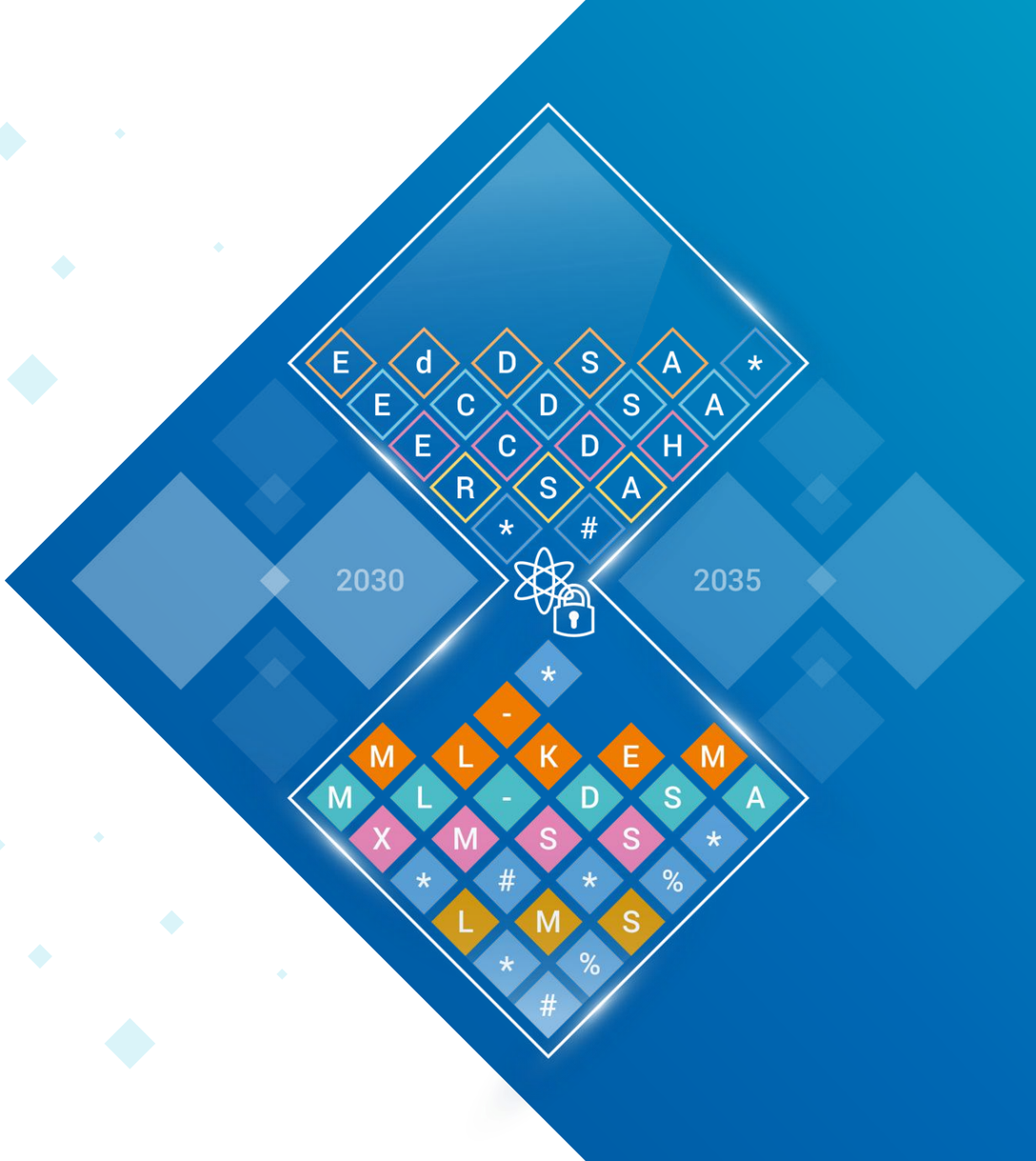
October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

utimaco®

The Better Choice for Trust in the Digital Society

Stateful Hash based Signatures – Practical Enhancements and Lessons learned



Dr. Volker Krummel

Chapter Lead PQC - Utimaco

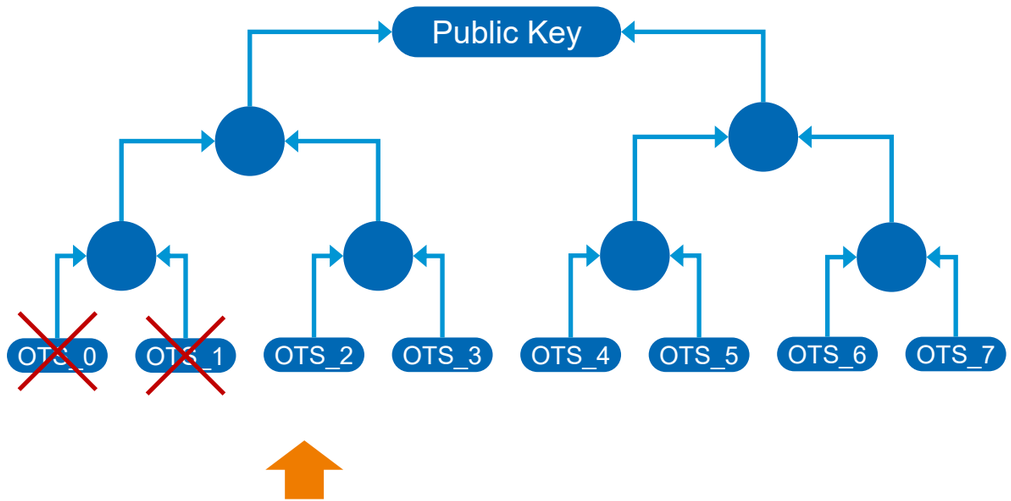
Kuala Lumpur, October 29th, 2025

- Recap: Stateful Hash based Signatures
- Recap: OTS Preserving Framework
- Automation
- Performance Improvements

Stateful Hash based Signatures - Recap

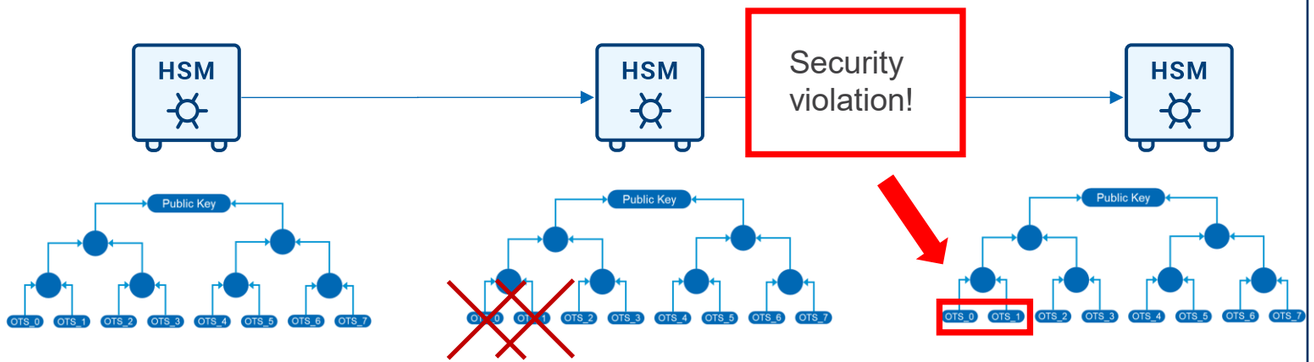
Scheme based on One time Signatures (OTS)

- Pure OTS impractical: too many public keys
- build up a tree structure → single public key

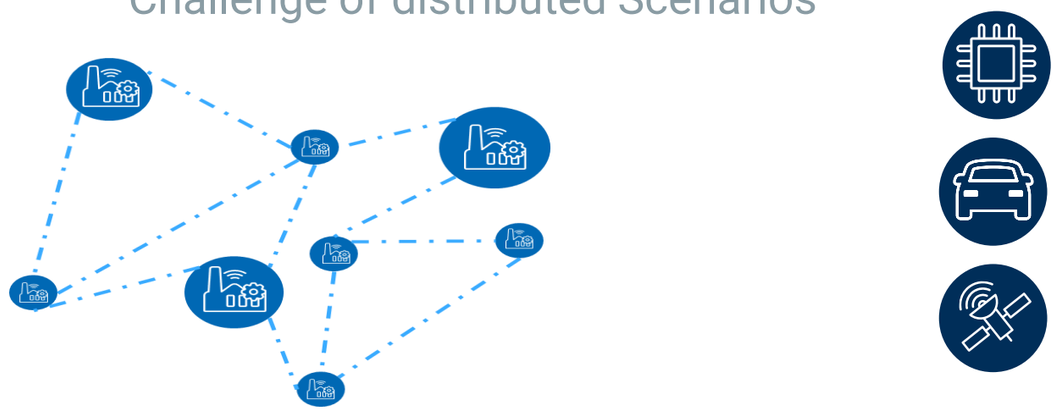


- State handling: Keep track about which OTS private key was already used
- Limited number of signatures

Backup & Restore breaks Security



Challenge of distributed Scenarios



Design Principles for an OTS preserving framework

Design Properties of a Secure State Handling Architecture

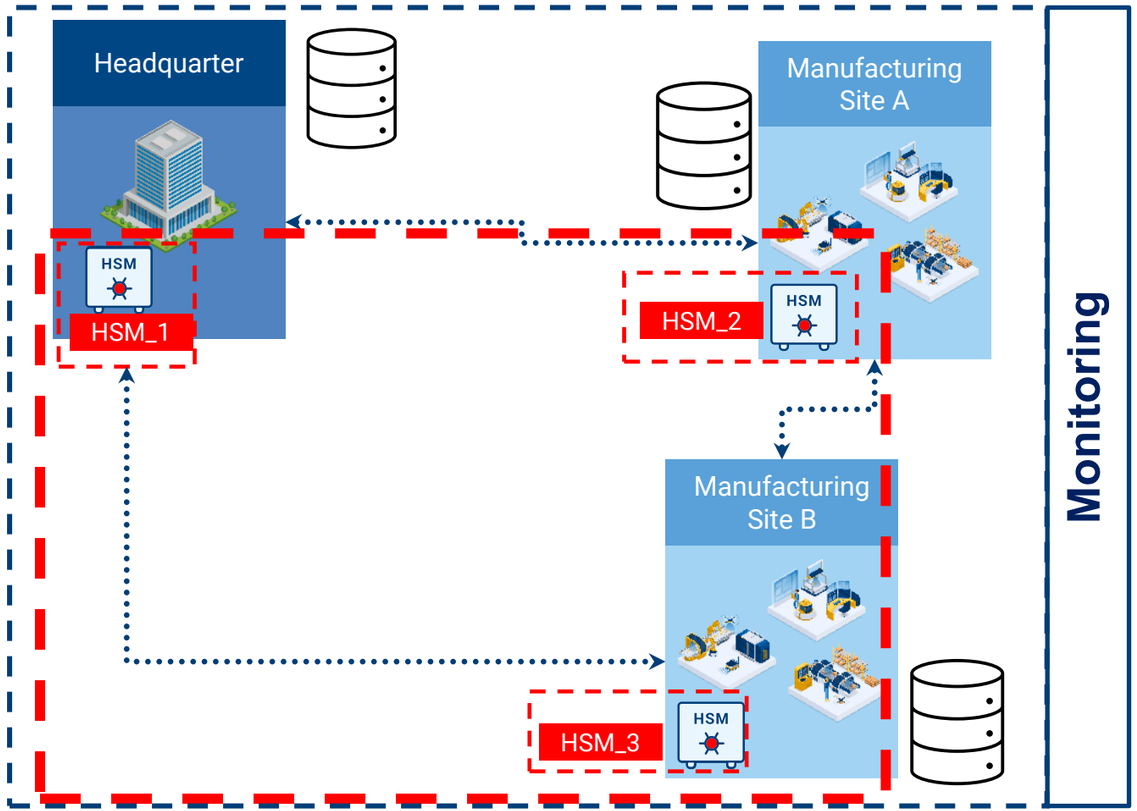
Security View

- **Comprehensive security design** - All security should be managed inside of an HSM.
- **Separate key information and state information** - knowing a key vs. using a key
- **Authentic and confidential end-to-end transfer of key and state information** - Do not use algorithms with less maturity.
- **Establish a reliable trust relationship between the HSM instances** - Allows a highly flexible and secure transfer even during operating in the field.
- **Prevent replays** – protect the freshness

Operators View

- **Prepare for offline data** – allow external storage of transfer messages (until delivery)
- **Asynchronous** - no need for direct (real time) communication between HSMs
- **No static setup** - flexible adaption of trust relationship
- **No Master – Slave** – avoid single points of failure
- **Generic** – no dependency to algorithm / key generation method

OTS Framework in action – Recap



Setup Phase

- Setup Trust relationship

Operating Phase

- OTS preserving Communication
- Local State Management
  1. Generate keys
  2. Distribute keys and state
     1. Add / remove HSM from Trust relationship
     2. Attacks blocked, e.g., Replay key transfer
     3. Risk of faulty app exhausting all keys

Trust boundary — Logical connection (network, portable storage, …) — External key storage (optional)

Security of the OTS-Framework

- Security notion of **OTS-preserving**
- Security Proof of OTS-Framework in the Universal Composability Model (UC-Model*)
- guarantees strong security properties (especially OTS preserving)
- allows a holistic security analysis
- for any adversary
  - protocol execution to indistinguishable from public simulator


Universally Composable Security:
A New Paradigm for Cryptographic Protocols*

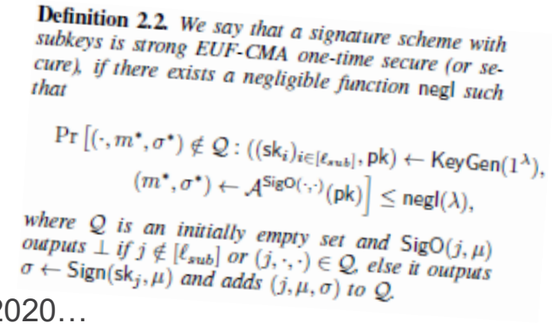
Ran Canetti†

February 15, 2020

Abstract

Keywords: cryptographic protocols, security analysis, protocol composition, universal composability.

- UC-Proof Status: proof finished, to be submitted
- White Paper “OTS-Preserving Framework” to be published soon


Definition 2.2. *We say that a signature scheme with subkeys is strong EUF-CMA one-time secure (or secure), if there exists a negligible function* negl *such that*

$$\Pr\left[(\cdot, m^*, \sigma^*) \notin \mathcal{Q} : ((\mathsf{sk}_i)_{i\in[\ell_{sub}]}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(1^\lambda), (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{SigO}(\cdot,\cdot)}(\mathsf{pk})\right] \leq \mathsf{negl}(\lambda),$$

where $\mathcal{Q}$ *is an initially empty set and* $\mathsf{SigO}(j,\mu)$ *outputs* $\perp$ *if* $j \notin [\ell_{sub}]$ *or* $(j,\cdot,\cdot) \in \mathcal{Q}$*, else it outputs* $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_j, \mu)$ *and adds* (j, μ, σ) *to* $\mathcal{Q}$.

* Canetti2000: Ran Canetti, **Universally Composable Security: A New Paradigm for Cryptographic Protocols,** 2000-2020…

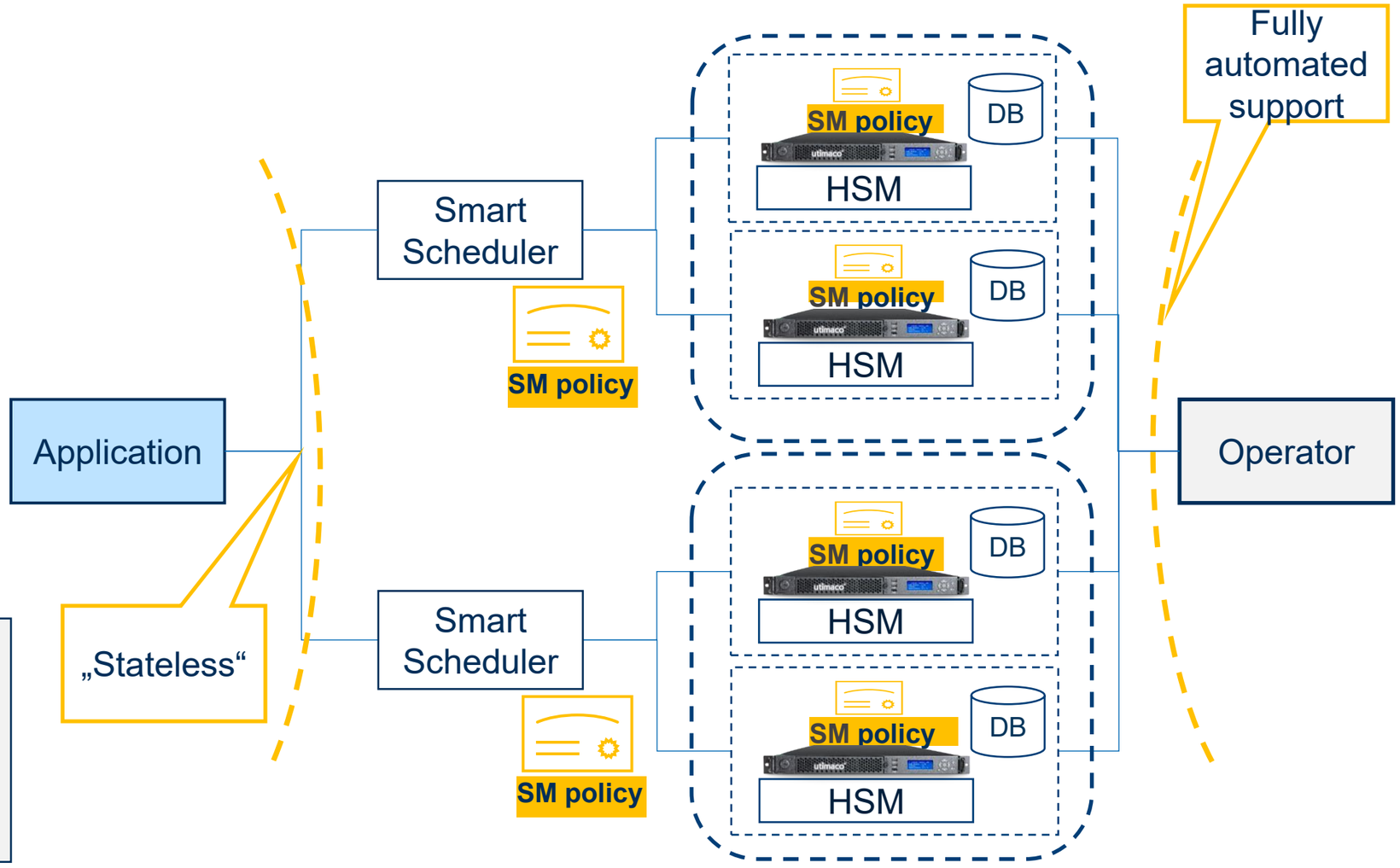
Secure and Transparent State Handling

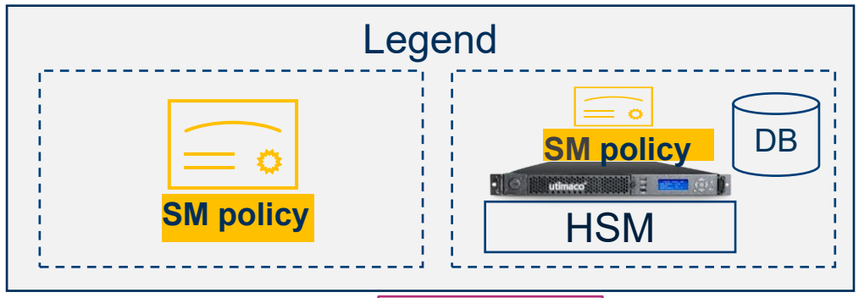
utimaco®

State Management Policy

- defines rules for state management
- based on OTS preserving framework

- application view: like stateless
- operator view: full flexibility & automation





Improvements

Key Generation

Sequential key generation

General Flow

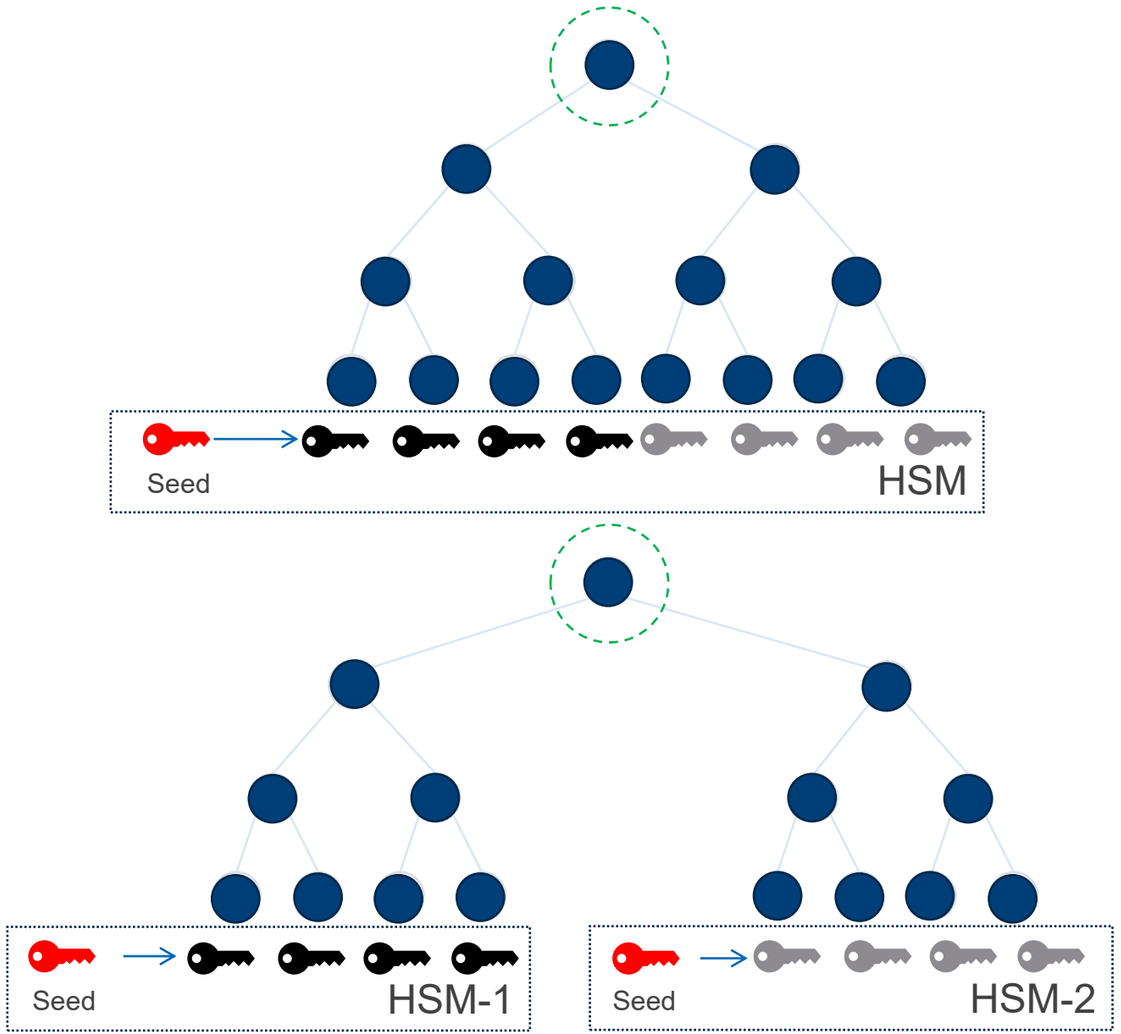
1. Select Algorithm / Parameter Set
2. Generate Seed
3. For all OTS
    1. Generate OTS
4. Generate Public Key

Distributed key generation

General Flow

1. Select Algorithm / Parameter Set
2. Generate Seeds (in parallel)
3. For all OTS
    1. Generate OTS
4. Generate Public Key

Parallel

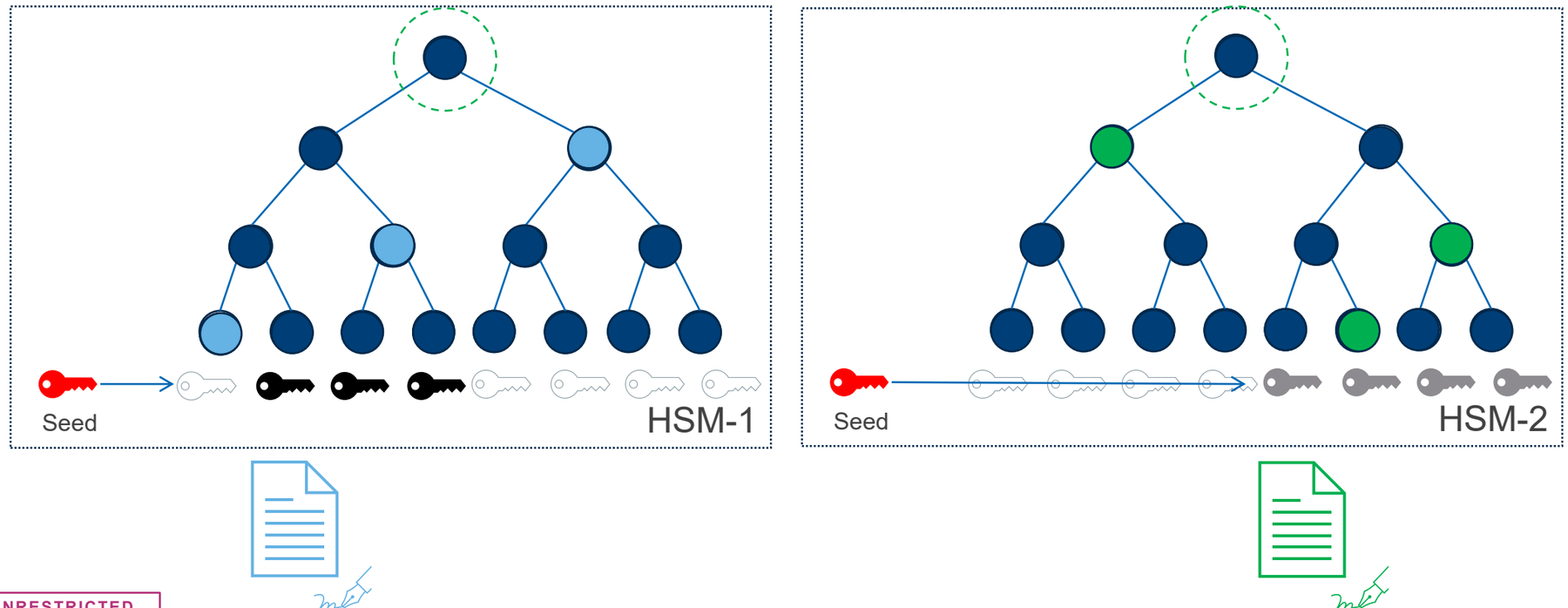


Signature Generation

Distributed Signature Generation

General Flow (independent on each HSM)

1. Select key according to current state
2. Generate OTS Signature
3. Compose Signature with AuthPath

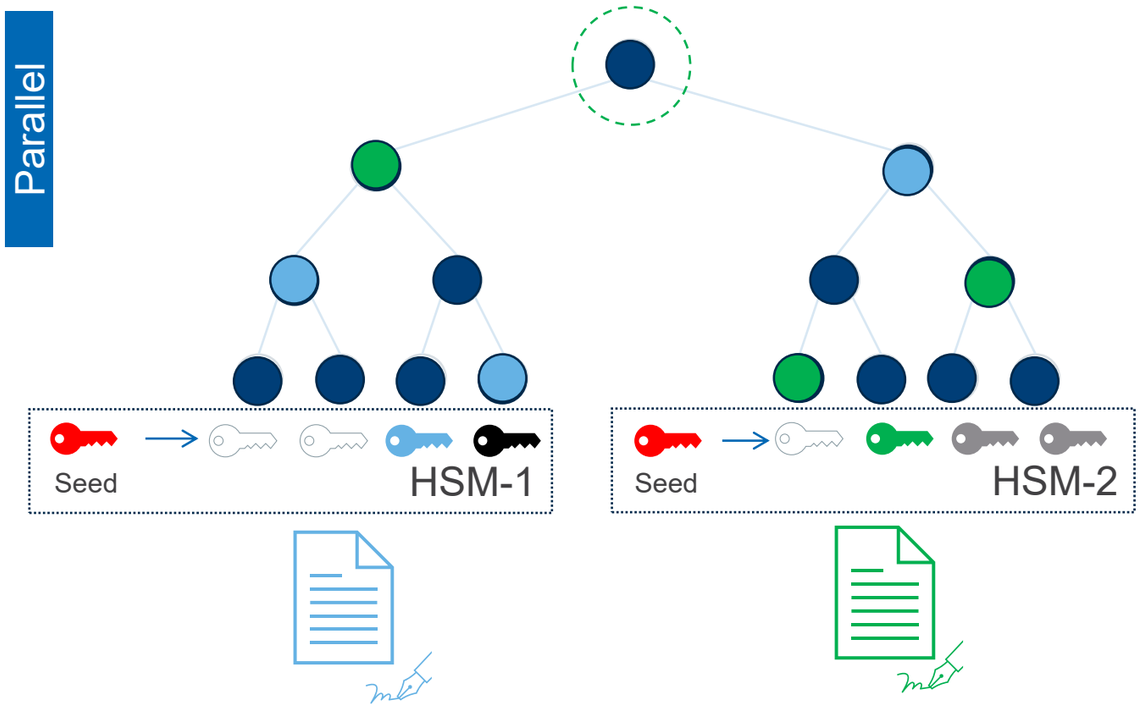


Signature Generation

Distributed Signature Generation with Tree Outsourcing

General Flow (independent on each HSM)

1. Select key according to local state
2. Generate OTS Signature
3. External Signature Enhancement with AuthPath



Advantages

1. Speed – only compute Private Key Operations on HSM
2. Speed – always have all Auxiliary Data precomputed
3. External Storage vs. Computing Time

Adressing the Challenges ...

- OTS Preserving Framework-Security ✓
- State Mgmt - Process Overhead ✓
- Performance Key Gen ✓
- Key Mgmt / Data Management ✓
- Limited Number of Signatures
  - Go for SLH-DSA (FIPS 205) ✓
  - Proper estimation ✓
- Regulatory (NIST SP 800-208)

Time for Your Questions

Q&A

Any further feedback: hsm@utimaco.com

  UNRESTRICTED

utimaco®

Thank You!

Headquarters
Utimaco Management Services GmbH
Germanusstrasse 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web utimaco.com
E-Mail info@utimaco.com

Utimaco IS UK Limited
Midshires House
Midshires Business Park
Smeaton Close, Aylesbury
United Kingdom, HP19 8HL

Phone +49 241 1696-0
Web utimaco.com
E-Mail info@utimaco.com

Office United Kingdom
Utimaco TS UK Limited
9th Floor
107 Cheapside, London
EC2V 6DN
United Kingdom

Web utimaco.com
E-Mail info@utimaco.uk

Office Italy
Utimaco TS S.R.L
Viale Certosa 218
Milano 20156
Italy

Web utimaco.com
E-Mail info@utimaco.it

Office Spain
Utimaco IBERIA S.L.U.
C/Infanta Mercedes 90
Planta 4
28020 Madrid

Phone **+34 91 449 03 30**
Web utimaco.com

Office Israel
Utimaco Technologies Ltd.
32 Maskit St,
POB 2215
Herzeliya Industrial Zone
4612101 Israel

Web utimaco.com
E-Mail info@utimaco.tech

Office APAC
Utimaco IS Pte Ltd.
6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

Phone +65 6993 8918
Web utimaco.com
E-Mail info@utimaco.com