Transition to PQC – A Reality Check

Dr. Volker Krummel

Creating Trust in the Digital Society

utimaco®

Agenda

Reality Check & Real World Experiences

Challenge:
Stateful Hash Based Signatures

References

Post Quantum Reality - Status

1. Quantum Computer poses a threat to current cryptography
2. Post Quantum Cryptography to thwart the **Quantum Threat**
3. Migration to Post Quantum Cryptography is complex

Why should I deal with PQC now?

CNSA 2.0 and NIST Timeline: Start Migration Yesterday

utimaco®

Requirements and Timeline

CNSA 2.0 Timeline

- Exclusive use of CNSA Suite 2.0
- CNSA Suite 2.0 default and preferred
- Option and testing

NIST IR 8547 Transition to Post-Quantum Cryptography Standards

Algorithms Deprecated

Elliptic Curve DH and MQC
(112 bits security strength)

Finite Field DH and MQV
(112 bits security strength)

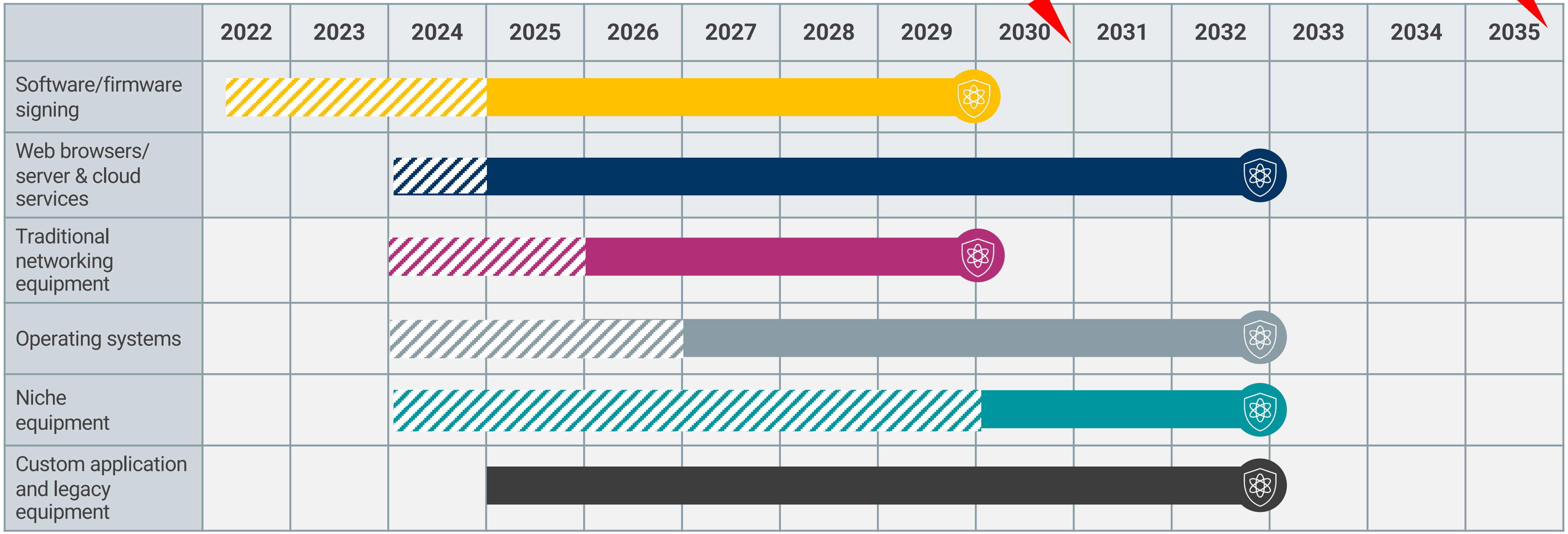
RSA, ECDSA and EdDSA
(112 bits security strength)

Algorithms Disallowed

Elliptic Curve DH and MQC

Finite Field DH and MQV

RSA, ECDSA and EdDSA

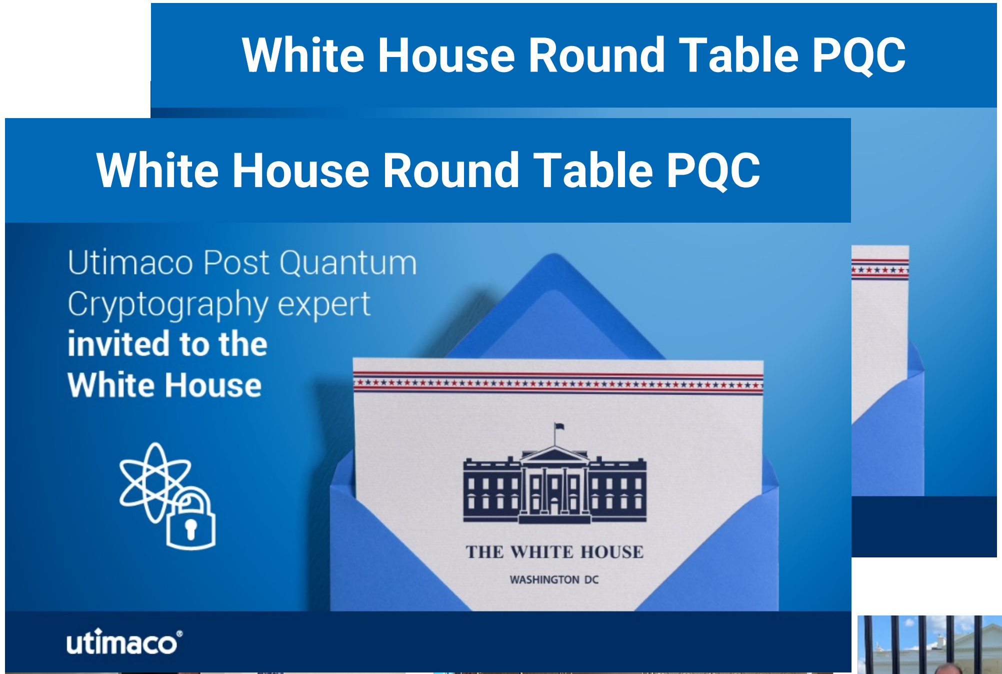


A very strong year …

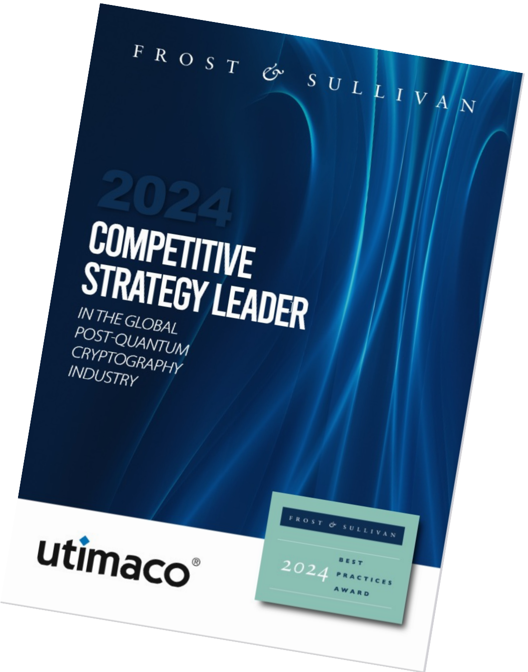
utimaco®

White House - Securing Our Nation With Post Quantum Cryptography

January & August 2024



Analysts



Collaboration

NIST

Bundesamt für Sicherheit in der Informationstechnik

•••

Intellectual Property

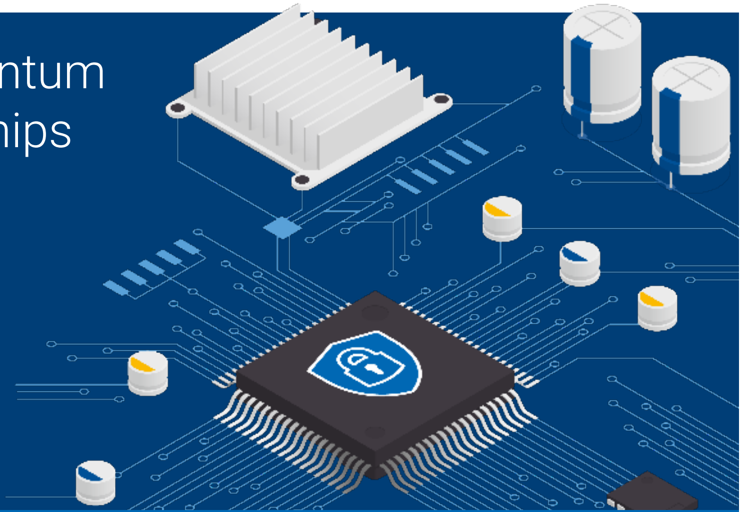
Patent

Case Study PQC for Chip Manufacturer

Applying quantum security for a large chip manufacturer

- **Use Case:** Quantum-secure device attestation
- **Customer:** Global semiconductor designer and manufacturer

Applying Quantum Security to Chips



Cryptographic key injection of Public PQC Key (ML-DSA and LMS) during the production process

Chips are used in a variety of use cases and devices and need to be long-term secure.

Secure, authenticated firmware updates with signed certificates via private PQC key (ML-DSA, LMS)

HSM

Generation of asymmetric key pairs based on ML-DSA, LMS with Utimaco HSM and PQC firmware extension

Enables hybrid signatures

Stateful Hash-Based Signature Schemes

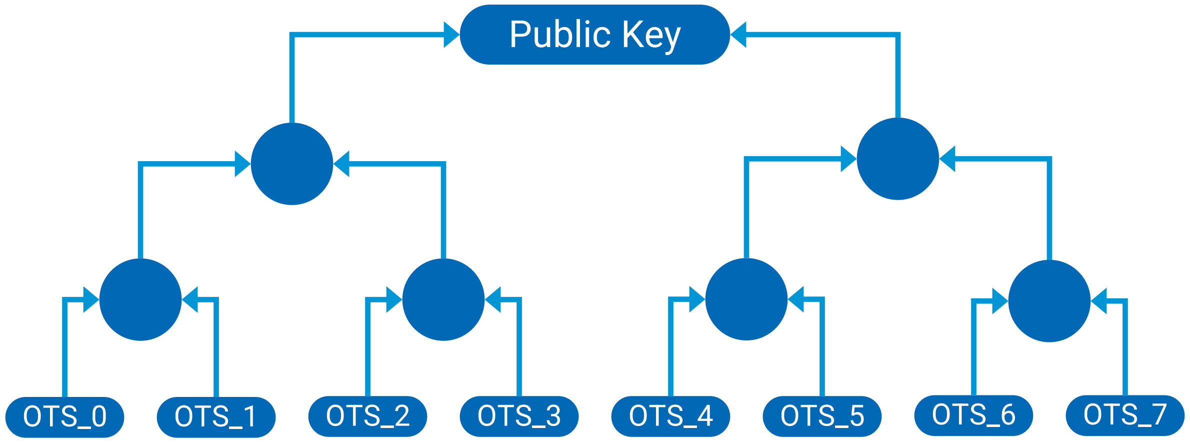
Creating Trust in
the Digital Society

utimaco®

Stateful Hash-based signature schemes

Advantages of stateful hash-based signature schemes

- Mature and proven algorithms
- High level of security
- Relatively small public keys make them simple, fast, and efficient
- Signing and verification require minimal computation effort
- Can be used as standalone algorithm (no need for a hybrid implementation)



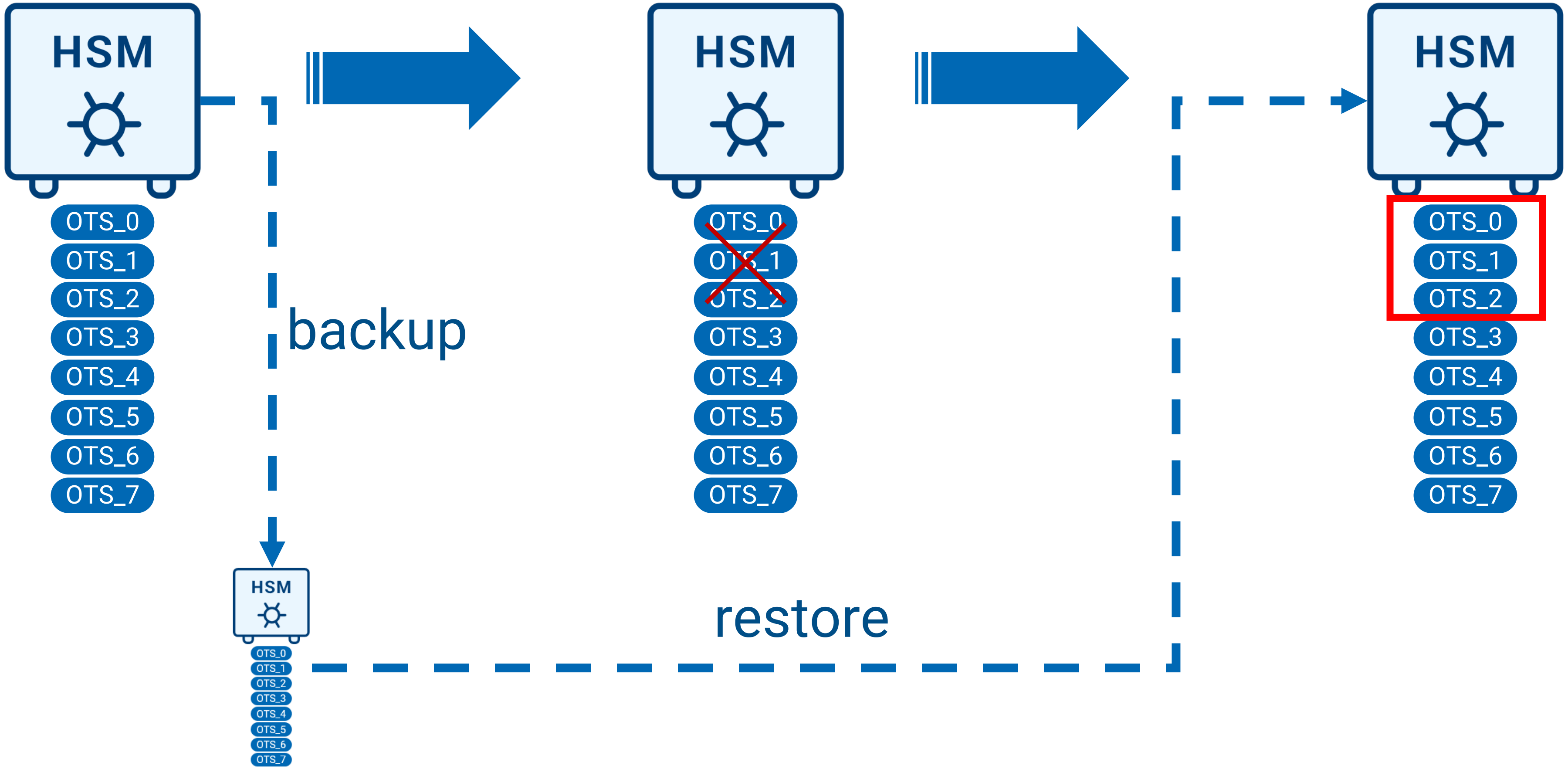
Challenges:

1) Limited number of keys
2) Handling the state (tracking OTS)

State Handling – Pitfall Backup & Restore

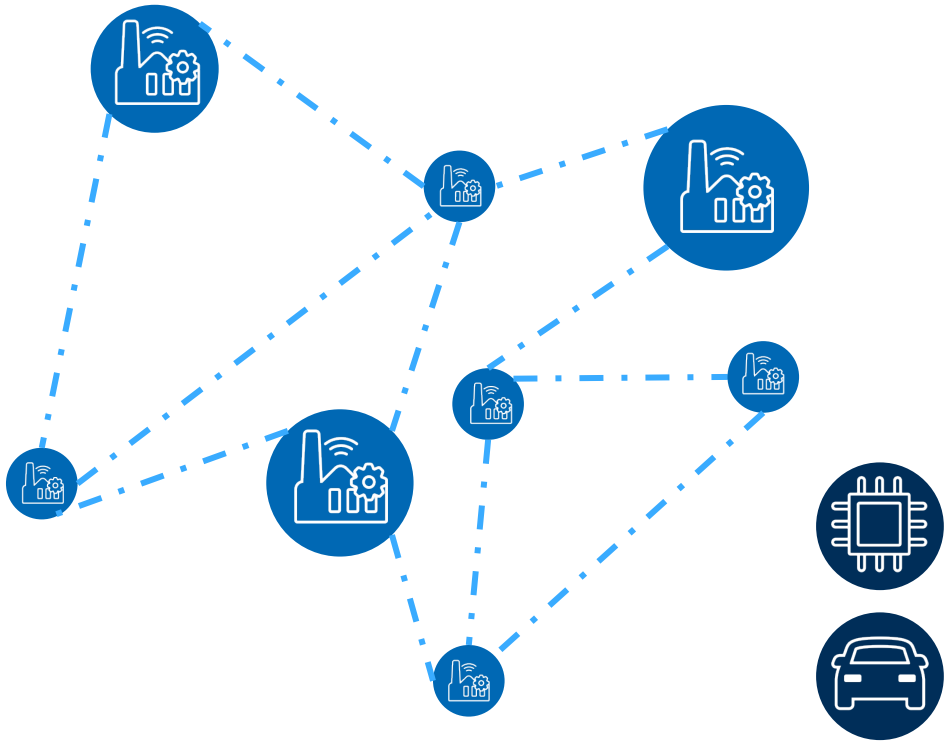
Backup & Restore

- Classical Backup & Restore procedures restore an old state -> violate the security requirement!



Multiple Sites – a **real-life challenge** in customer projects

Stateful Hash-Based Algorithms are great – but distributed environments cause a challenge



Challenge:

Development from centralized to decentralized use case

Decentralized use cases

- Multi site implementation
- State handling is complicated
- Example: Global Automotive supplier

3 Core aspects of the **Utimaco OTS Preserving Framework**

utimaco®

Trust relationship between HSMs

OTS preserving communication between HSMs

Local state management

- HSMs are still passive components
- Application is actively driving the logic (not the security!)

Design Principles for an OTS preserving framework

utimaco®

Security is Paramount: No OTS Key re-use

Design Properties of a Secure State Handling Architecture

Security View

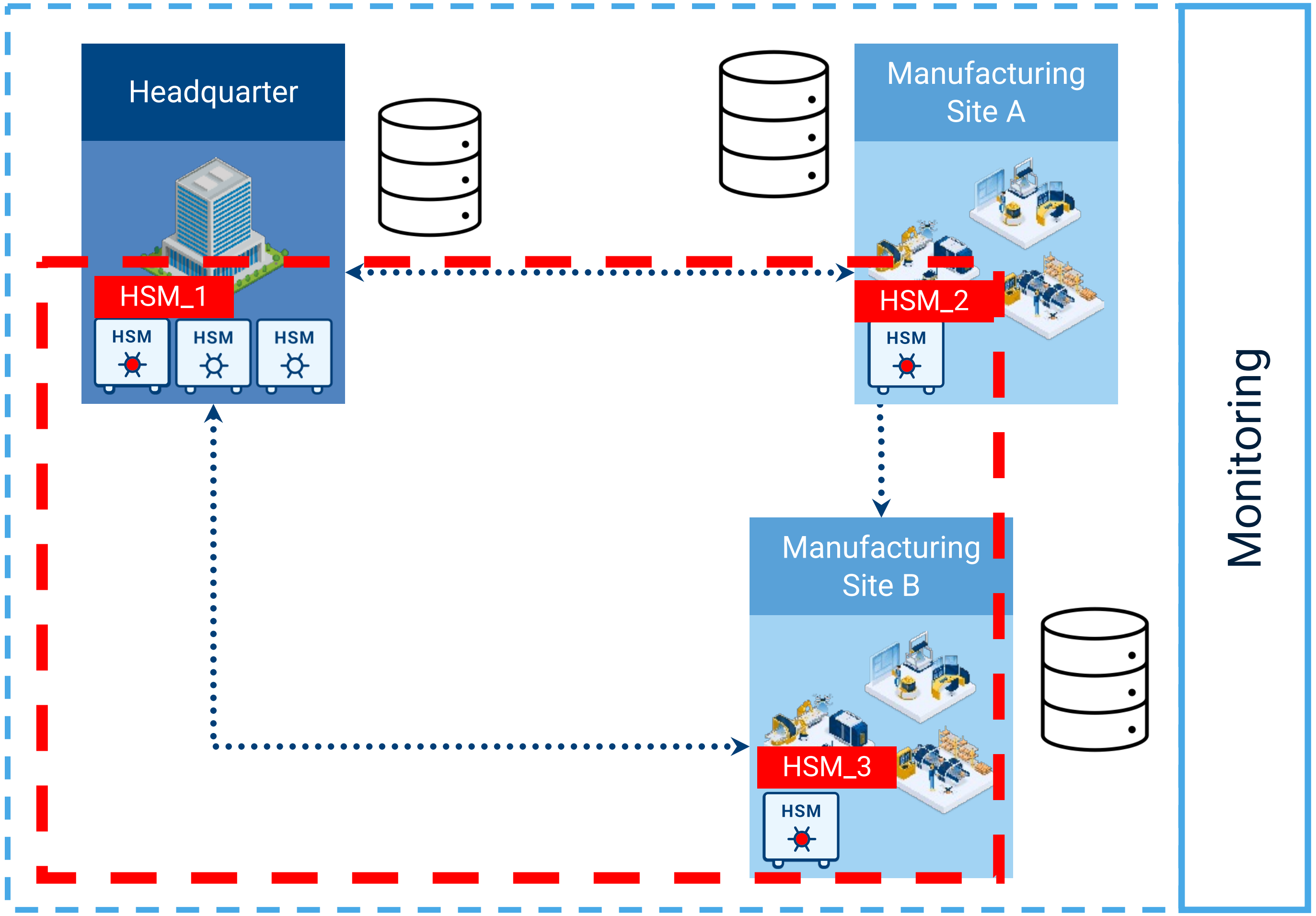
- **Comprehensive security design** - All security should be managed inside of an HSM.
- **Separate key information and state information** - knowing a key vs. using a key
- **Authentic and confidential end-to-end transfer of key and state information** - Do not use algorithms with less maturity.
- **Establish 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

State handling in operation – *Security is Paramount*

utimaco®



1. **Setup phase** (set up trust relationship)
2. Generate key in HQ
3. Distribute subsets to destinations
4. Operate …
    1. If risk of key exhaustion at one site - Securely transfer keys from other site(s)
    2. If site will be shut down - Securely transfer remaining keys to other site(s)
    3. Attacks blocked, e.g., Replay key transfer
    4. Risk of faulty app exhausting all keys - only import small portions of the key; keep rest offline
    5. If HSM is destroyed -> loss is limited to a well-defined subset of the key
5. Add / remove HSM from Trust relationship

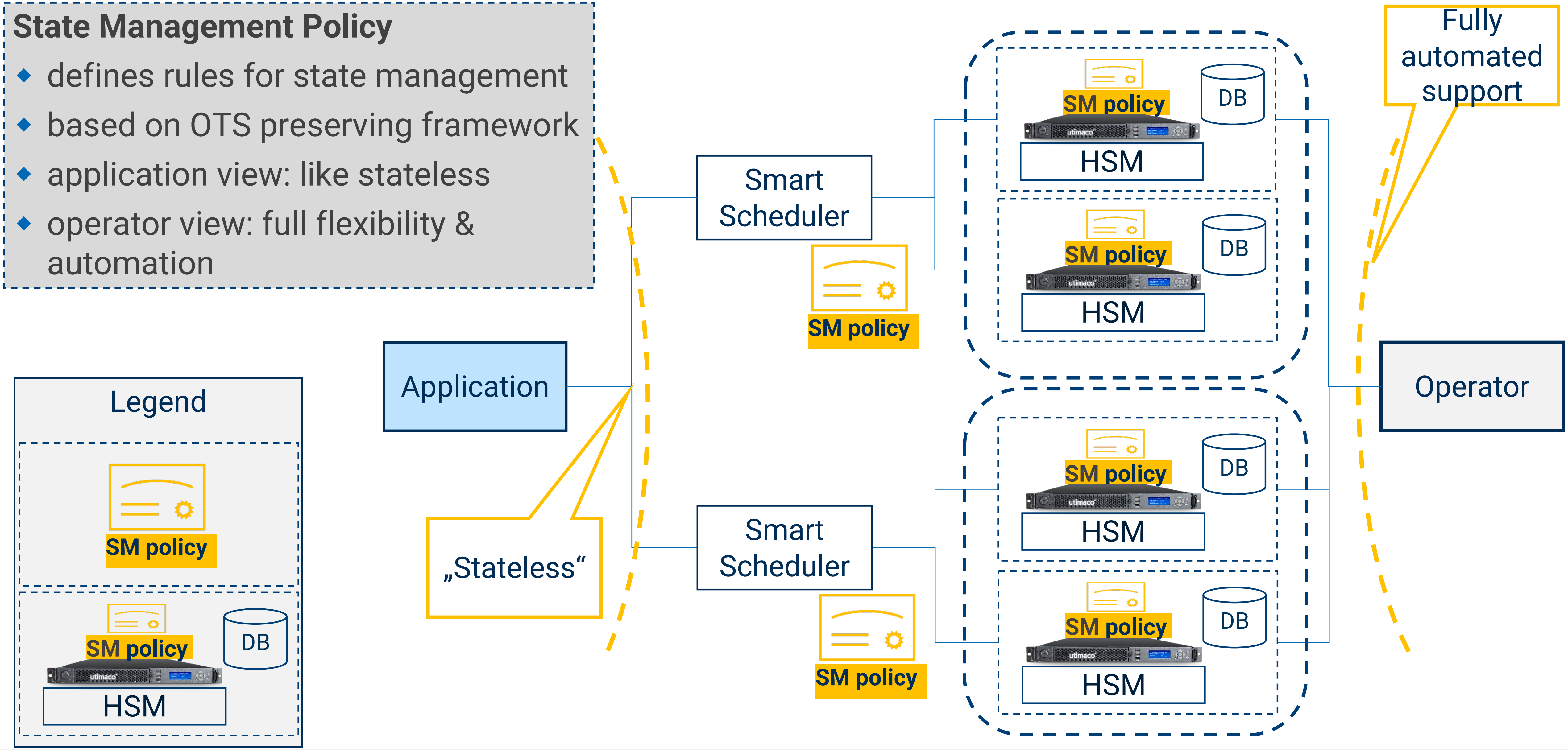
Trust boundary   Logical connection (network, portable storage, …)   External key storage (optional)

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



Summary

- Adress PQC now!
- Challenges can be solved – security and operational aspects
- OTS preserving Framework & State Management Policy => practical stateful hashbased signatures

Selected References

- NIST SP 800-208
- NIST IR 8547
- PQC State and Mitigation
- PQC Integration Study
- PQC FAQs

- PQC Migration Handbook
- FIPS 203

- Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography
- Quantum Computer Development
- BSI TR-02102-1 (in German)
- Quantum Computing Information Page
- FIPS 204
- PQC Information
- CNSA 2.0
- CNSA 2.0 FAQ
- PQC Strategies
- Migration to PQC
- FIPS 205

UTIMACO GmbH
Germanusstraße 4
52080 Aachen
Germany

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

Contact the Experts

Copyright © 2023 – UTIMACO GmbH
UTIMACO® is a trademark of UTIMACO GmbH. All other named trademarks are trademarks of the particular copyright holder.
All rights reserved. Specifications are subject to change without notice.

Thank you
for your attention!

UTIMACO Inc.
900 East Hamilton Avenue
Campbell, CA-95008
United States of America

Phone +1 (844) UTI-MACO
Web hsm.utimaco.com
E-Mail hsm@utimaco.com

Copyright © 2022 – UTIMACO GmbH
UTIMACO® is a trademark of UTIMACO GmbH. All other named trademarks are trademarks of the particular copyright holder.
All rights reserved. Specifications are subject to change without notice.