

Post-Quantum

Cryptography Conference

## Securing Data in the Quantum Era: From the Root of Trust to Protecting Ecosystems

With advancements in Quantum Computing, the security of our data relies heavily on robust cryptographic solutions. Hardware Security Modules (HSMs) with integrated Post-Quantum Cryptographic (PQC) algorithms become center stage for securing data in the Quantum Computing Era. Besides providing PQC algorithms, HSMs also secure and automate key distribution for “complex to manage” stateful hash-based signature algorithms and provide hardware acceleration to meet modern applications’ cryptographic needs. Taking those advancements as starting point, the talk will shift gear and explore how security systems, comprising of software and hardware, use Post Quantum primitives to secure their operation. Important systems include Key Management, PKI, and File & Folder Encryption. The role of each system in the security framework will be discussed, focusing on specific PQC requirements. The talk continues to move to the solution level, and will provide insights and lessons learned for the needs and challenges of securing an inter-banking system, a project currently at the research stage. By the end of the session, attendees will have a good overview on the capabilities of cryptographic components, how those capabilities can be used by security solutions and what is needed next, to secure whole “Ecosystems” against Quantum Computer attacks on today’s cryptography.



**Nils Gerhardt**  
Chief Technology Officer at Utimaco



KEYFACTOR



January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity (“business league”) under Utah law (10462204-0140) | [pkic.org](https://pkic.org)



**PKI**  
Consortium

# Securing Data in the Quantum Era

## From the Root of Trust to Protecting Ecosystems

Nils Gerhardt, CTO

Jan 16<sup>th</sup>, 2025

Creating Trust in  
the Digital Society

utimaco<sup>®</sup>

Level up your crypto to be prepared for the Post Quantum Age

## The building blocks – HSMs role in PQC



Features:  
„All“ PQC algorithms



ASIC & FPGA  
Performance:  
HW Acceleration

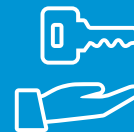


Real world:  
SHBS algorithms in  
decentral environments

## Security systems use PQC and HSMs to protect their operation



Public Key  
Infrastructure (PKI)



Key Management



File & Folder  
Encryption

## Ecosystems use security systems for PQC



**Example:**  
**Payments Ecosystem**

Crypto Discovery & Control



# The building blocks – HSMs role in PQC

## CNSA 2.0

### Software and firmware signing

- ◆ LMS
- ◆ XMSS

### Public key algorithms

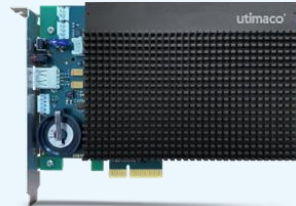
- ◆ Key-establishment:  
ML-KEM (CRYSTALS-Kyber)
- ◆ Digital signatures:  
ML-DSA (CRYSTALS-Dilithium)

### Symmetric key algorithms

- ◆ AES
- ◆ SHA

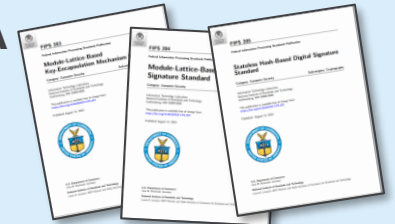
**Mandatory migration starting 2025!**

## Hardware Security Modules



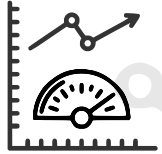
## Global PQC Standards (NIST)

- ◆ **NIST SP800-208**
- ◆ **FIPS 203: ML-KEM**  
based on CRYSTALS-Kyber
- ◆ **FIPS 204: ML-DSA**  
based on CRYSTALS-Dilithium
- ◆ **FIPS 205: SLH-DSA**  
based on SPHINCS+



## Upcoming PQC Algorithms

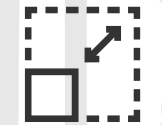
- ◆ FrodoKEM
- ◆ Falcon
- ◆ What's next?



FPGA hardware acceleration delivers a **significant performance improvement** for Kyber and Dilithium



PQC IP cores exhibit **comparable** FPGA resource **utilization** to RSA/EC IP cores.

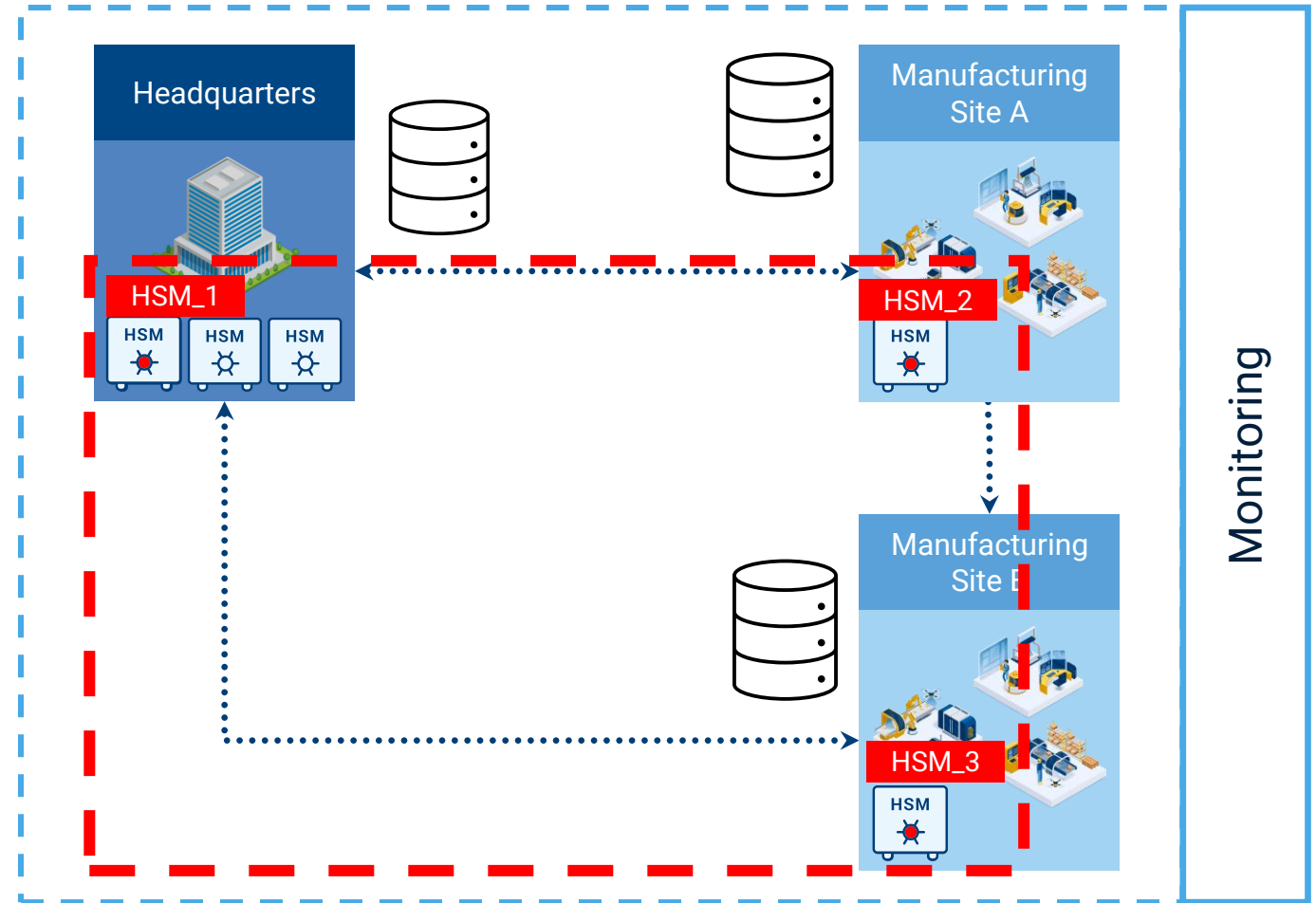
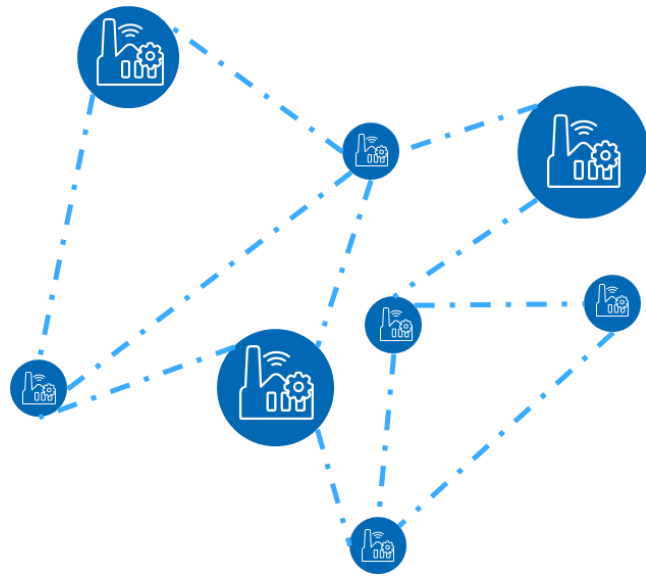


PQC IP core(s) with **scalable** resource utilization based on **available** FPGA **resources**.



**Further Side-Channel Resistance** with fine-grained control over **hardware** design, clock randomization, and **physical isolation**

# HSM are ready for migration – Stateful Hash Based Signature algorithms can be used securely in distributed environments



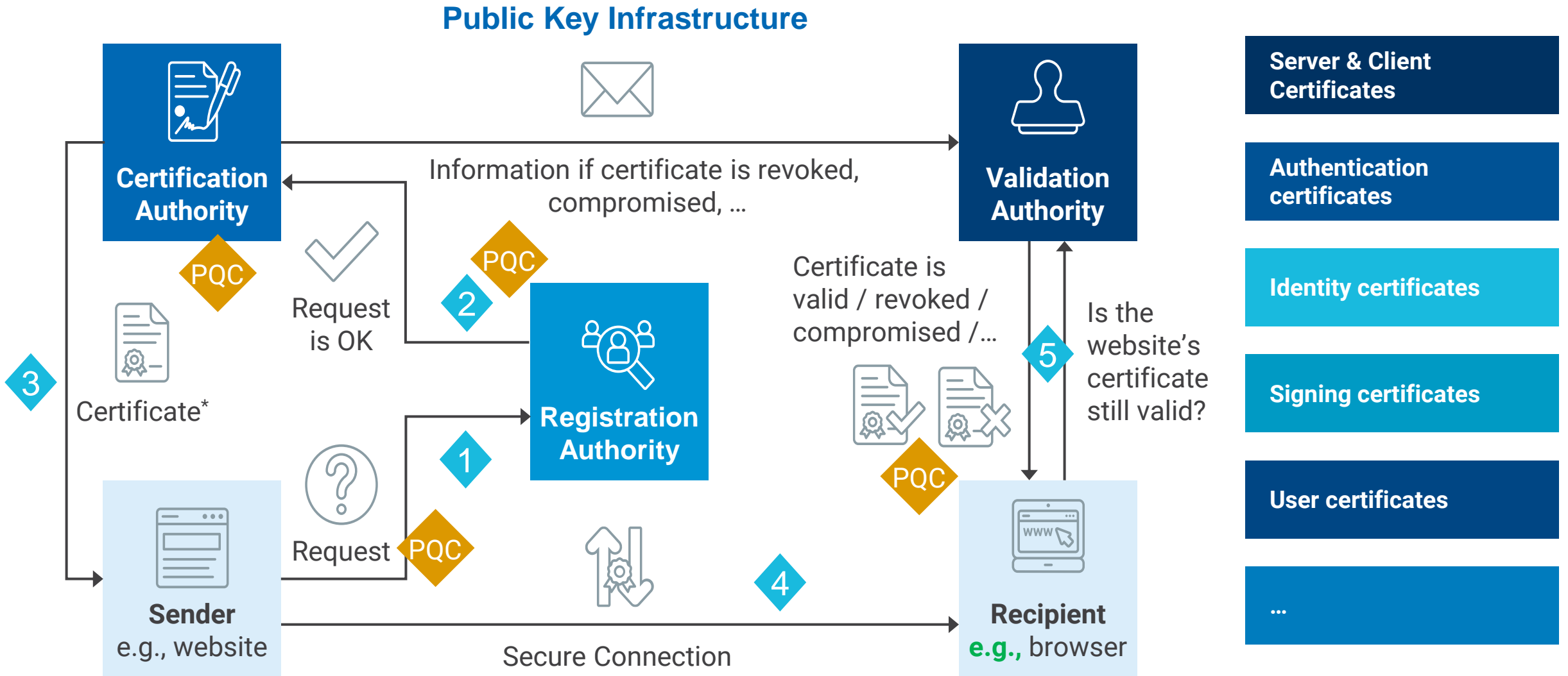
**Challenge:** Development from centralized to decentralized use case

**Solution:** HSM Trust Relationships enable secure key distribution & replenishment



**Security systems use PQC  
and HSMs to protect their operation**





\* The step of registering and requesting a certificate usually happens once each 1-2 years if **it is** a certificate used for HTTPS.

## PQC considerations

### Certificate support

- ◆ PKI systems must adopt PQC certificates from the root downward
- ◆ Hybrid Certificates are required for an interim period (migration)

### Migration

- ◆ Issuance of new PQC certificates
- ◆ Migration of traditional certificates to PQC
- ◆ Make PKI system PQC secure

## Hybrid Certificates

**Challenge:** Migrating existing PKI and CA Systems into a Post Quantum World

**Solution:** *X.509 Hybrid Certificates* help ease the transition to new *quantum-safe systems*

X.509 Hybrid Certificates defined as Internet Draft:

- ◆ Composite Public/ Private Keys for Internet PKI
- ◆ Phased implementation and gradual adoption
- ◆ PKI Vendors provide early access to composite Certificates to start the adoption process

**Secure Root:** Utilization of HSMs with traditional and PQC algorithms

## General

Follow standards, compliance, and readiness of PKI vendors.



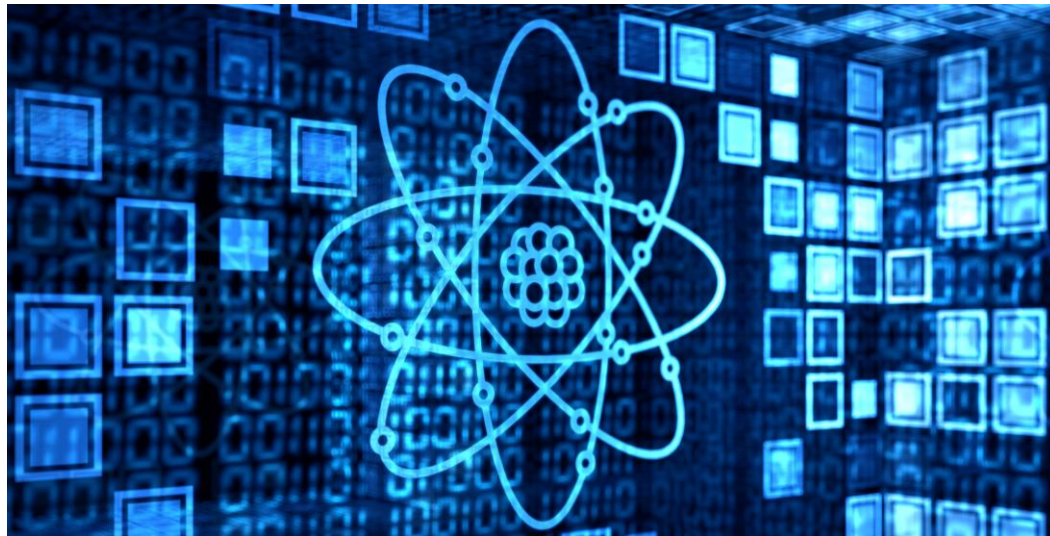
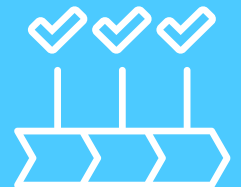
## Start with The Root of Trust

A PQC ready HSM is often used before the PKI is “readied” for PQC.



## Migration

- ◆ Migration to pure PQC certificates will take time
- ◆ Adoption of hybrid certificates can start now
- ◆ Gradually replace keys w. quantum-resistant ones
- ◆ Ensure PKI systems handle larger keys/ signatures
- ◆ Future “pure” PQC certificates likely follow current X.509 Standard, but
  - ◆ OIDs still need standardization



# PQC in Key Management

## Key Management at the Epicenter of Cryptographic Operations

- ◆ Key Management role is to provide a centralized system to
- ◆ Securely generate, store, distribute, use, and manage (quantum-resistant) cryptographic keys
- ◆ Act as the control center for managing the lifecycle of PQC keys across an organization
- ◆ Support efficient adoption/ migration to new quantum-safe standards



## Key Injection



### Use Cases

- ◆ Machine Identity
- ◆ Integrity
- ◆ Confidentiality

## Enterprise Key Management



### Use Cases

- ◆ Data-at-Rest (DAR)
- ◆ Lifecycle management
- ◆ Policy control



## PQC Key Injection

The scale of (PQC) private key replacements will grow exponentially due to

1. the volume of connected digital endpoints
2. PQC key replacements

Today's embedded devices may require replacement, due to lack of PQC support

1. key sizes
2. storage requirements
3. performance for calculation



## PQC Enterprise Key Management

Cryptographic keys are required to encrypt physical storage, servers, VMs, databases, customer data, etc.

Consequently, private key replacements will grow exponentially across tomorrow's enterprise

Unified management platforms are needed that can:

- ◆ Discover all keys – incl. unknown
- ◆ Manage all keys from a single pane of glass
- ◆ Control policy enforcement across the company
- ◆ Automate the key lifecycles

Support organizations crypto agility for PQC migration

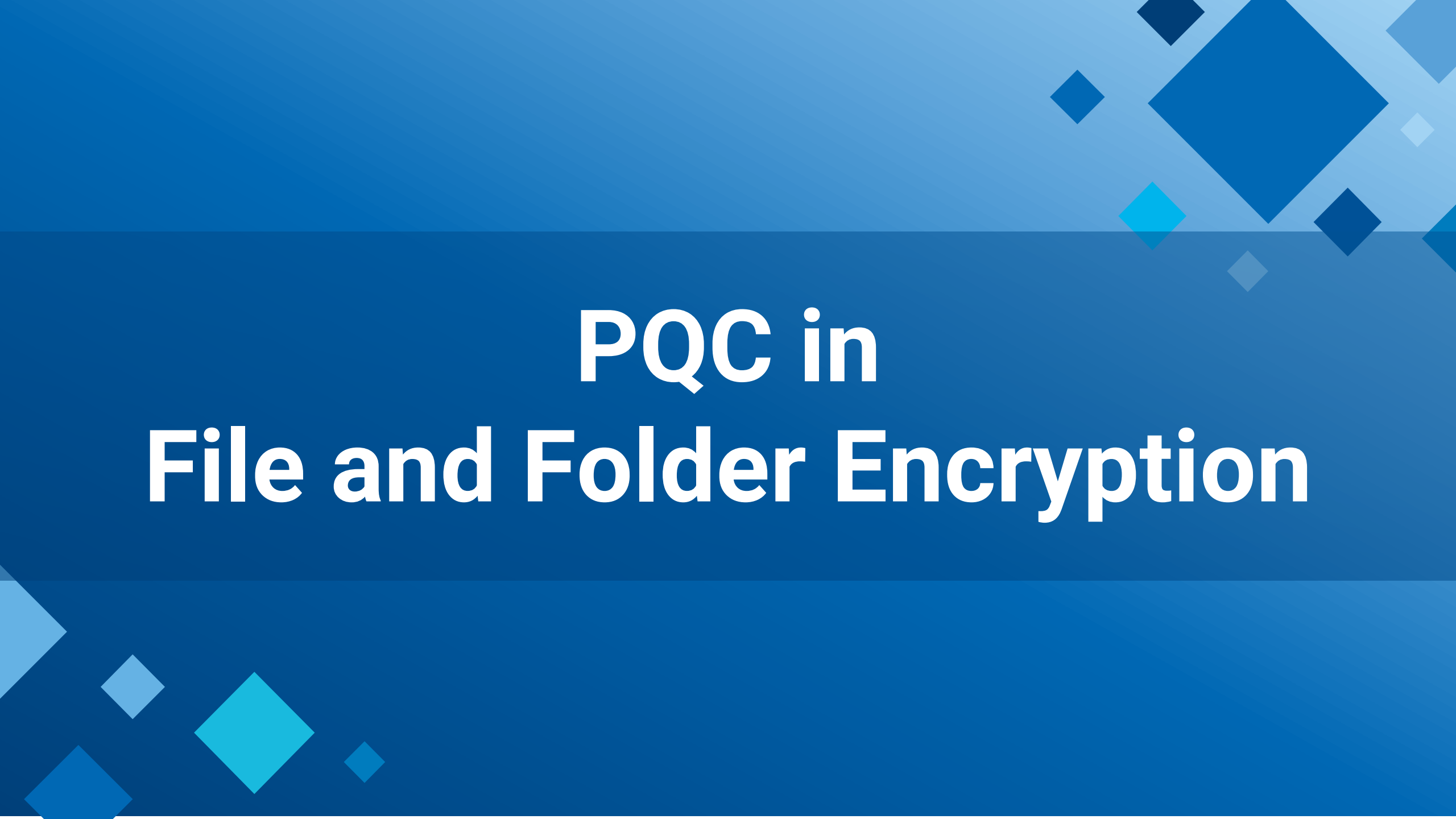
### Secure Root:

Utilization of HSMs w. traditional & PQC algorithms to support security, performance and crypto agility



- ◆ **Key management** is at the epicenter of cryptographic operations & PQC migration
  - **Key injection**
  - **Enterprise lifecycle management**
- ◆ The scale of key replacements will grow exponentially with the volume of connected IoT & enterprise endpoints
- ◆ All private keys will need to be replaced by the time a QRQC is practically available
- ◆ Customers require solutions to implement PQC into cryptosystems, while maximizing agility, visibility, automation, and control





# PQC in File and Folder Encryption





**Utimaco**

LAN Crypt File and Folder Encryption



Transparent Encryption



Data Protection at Rest and in Motion



Compliance Fulfillment – Worldwide



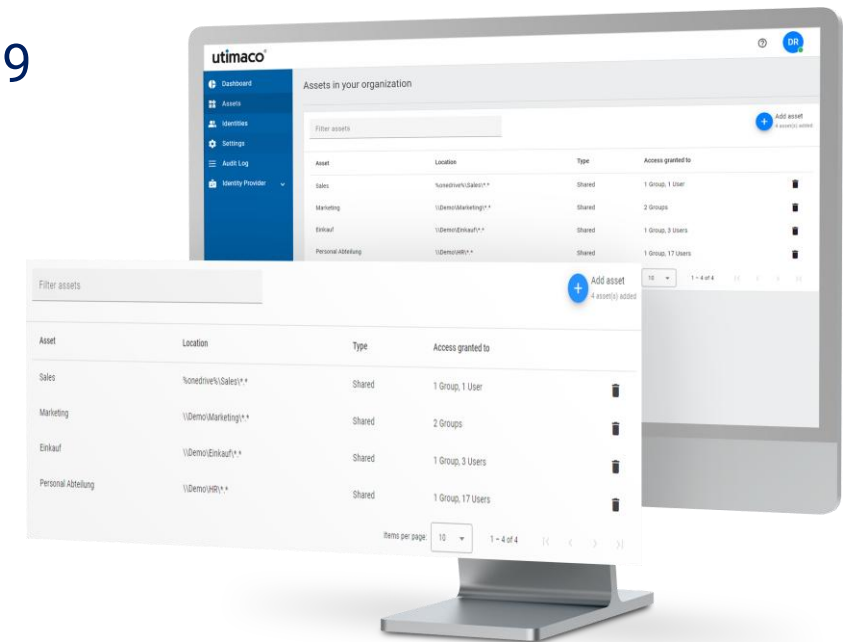
Role-based Access Management

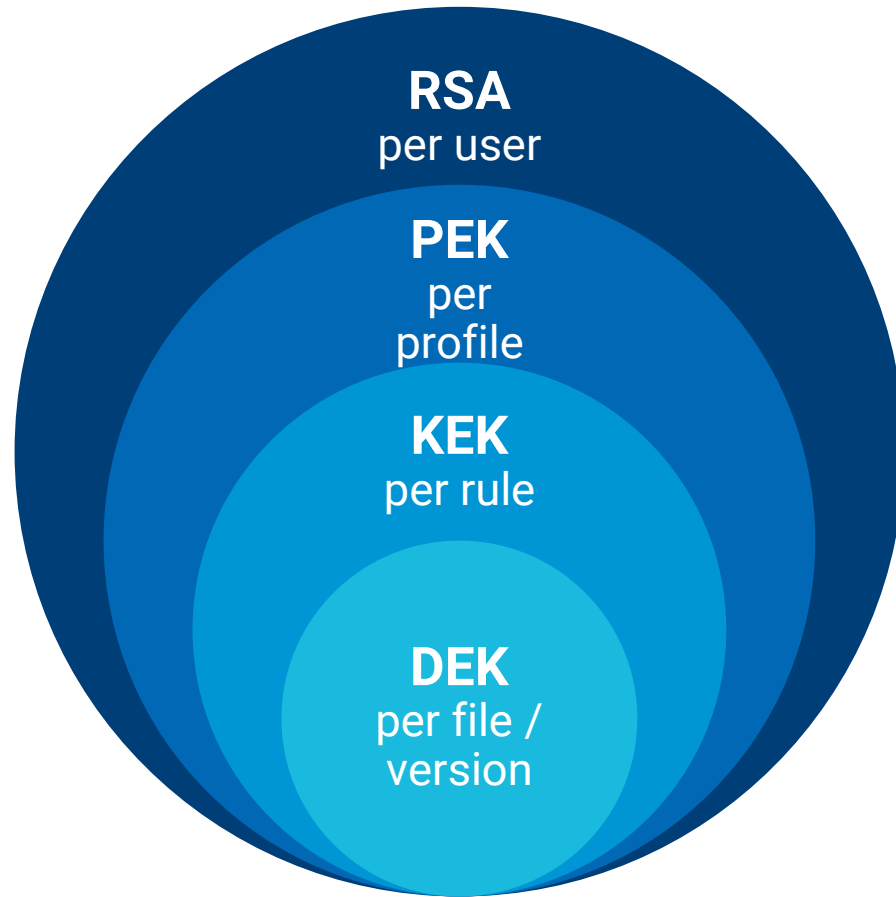


Secure Sharing

## Technology & Standards

- RSA
- X.509

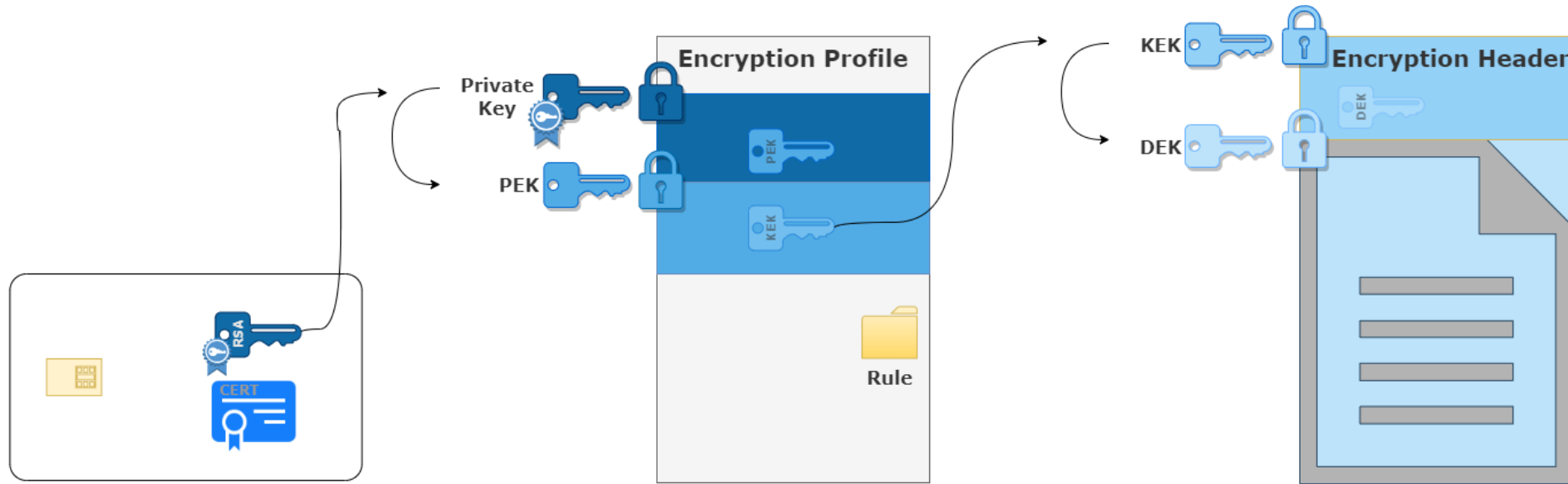




- RSA, asymmetric, RSA 1-4 Kb
- PEK, symmetric, AES 256
- KEK, symmetric, AES 256
- DEK, symmetric, AES 256

## Key Architecture

- ◆ Each file is encrypted with an individual symmetric key, a **Data Encryption Key (DEK)**
  - ◆ DEK is encrypted with a **Key Encryption Key (KEK)**
  - ◆ KEKs are merged with the rules in the **profile**
  - ◆ Profiles for each user are encrypted with an individual symmetric **Profile Encryption Key (PEK)**.
  - ◆ The PEK is encrypted with the user's **public key**.
- ◆ DEKs & PEKs are generated individually each time.
- ◆ KEKs and PEKs are generated by the administrator
  - ◆ Stored in DB (secured by security officer's key pair)



## TRANSPORT

### Attack Scenarios

- ◆ Harvest now, decrypt later
- ◆ Grover's/Shor weakening crypto
- ◆ Internal attacker
- ◆ Backup data (long-term)

## PROFILE

### Mitigations

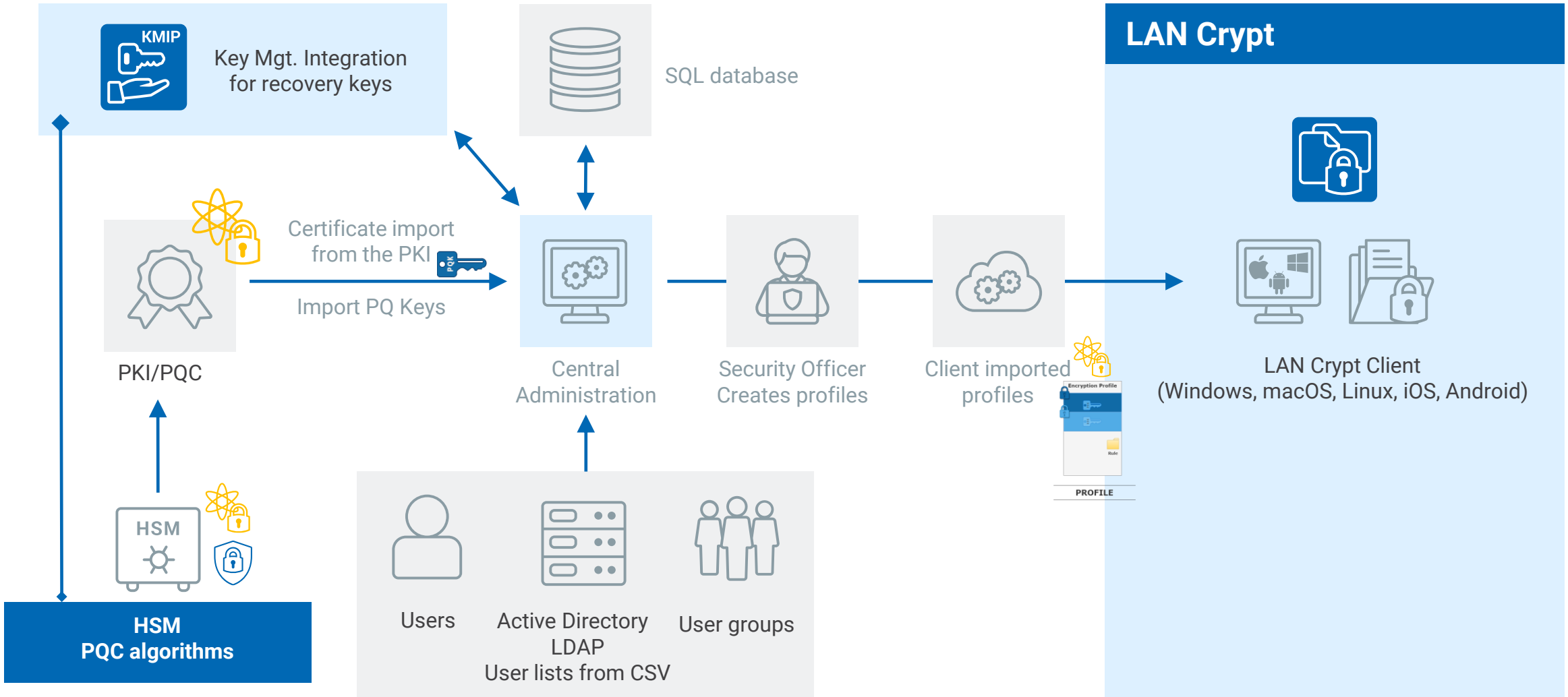
- ◆ Recording
- ◆ Hybrid encryption
- ◆ PQ Transport lock
  - ◆ Profile/ Tunnel encryption

## DATA

### Migration

- ◆ PEK encrypted with users PQ key
- ◆ Replace RSA-based certificates
- ◆ Chose PQC resistant keys
- ◆ Update systems to handle larger key sizes and signatures

## Architecture





# **Ecosystems start using PQC – Example Payments**

## Project „EASEPROFIT“ - PQC Transition of Banking Process

### Project Topic

- ◆ Analysis and Transition of
  - ◆ Electronic Banking Internet Communication Standard (EBICS)
  - ◆ Banking specific processes
- ◆ Holistic Team approach
  - ◆ Research Institutes
  - ◆ Tech-Partners (Financial IT-Provider)
- ◆ Technical Project Goals
  - ◆ Quantum resistant confidential & authentic communication
  - ◆ Distributed signatures
  - ◆ Migration Plan



Bundesministerium  
für Bildung  
und Forschung

<https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/easeprofit>

### Project Team



BUNDESDRUCKEREI

RUHR  
UNIVERSITÄT  
BOCHUM

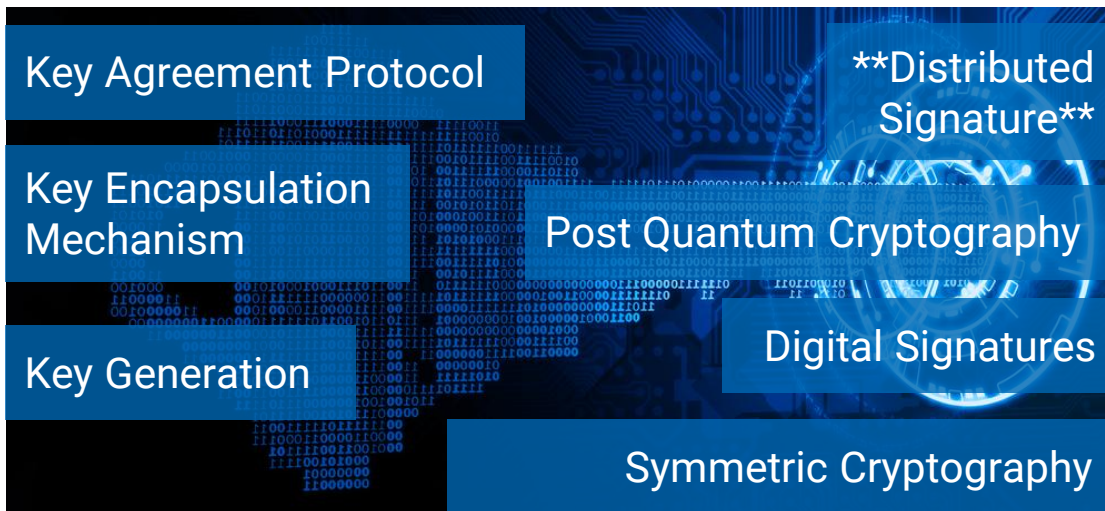
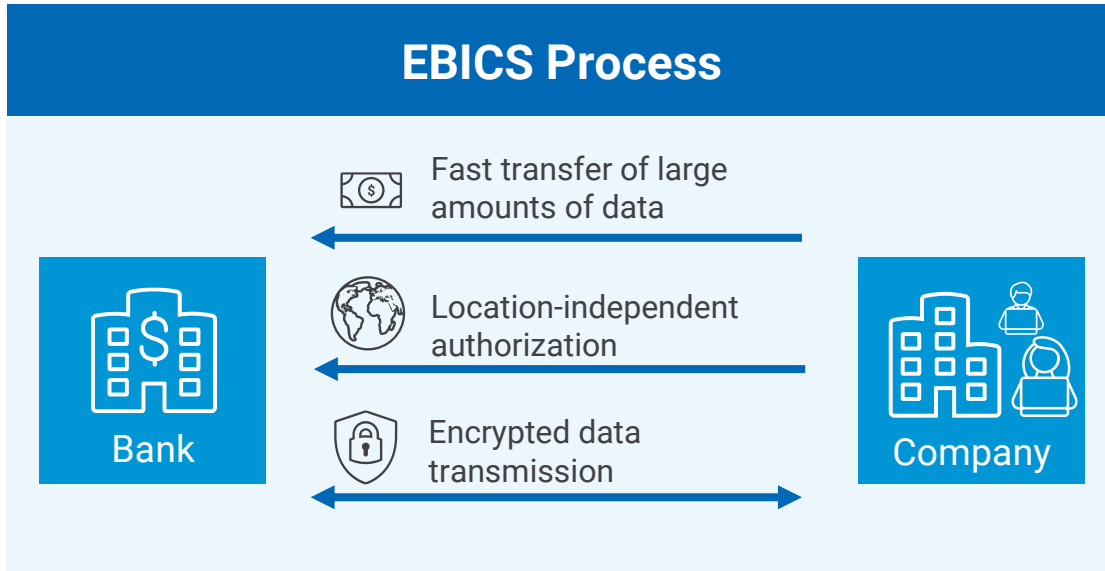
RUB

TUVIT

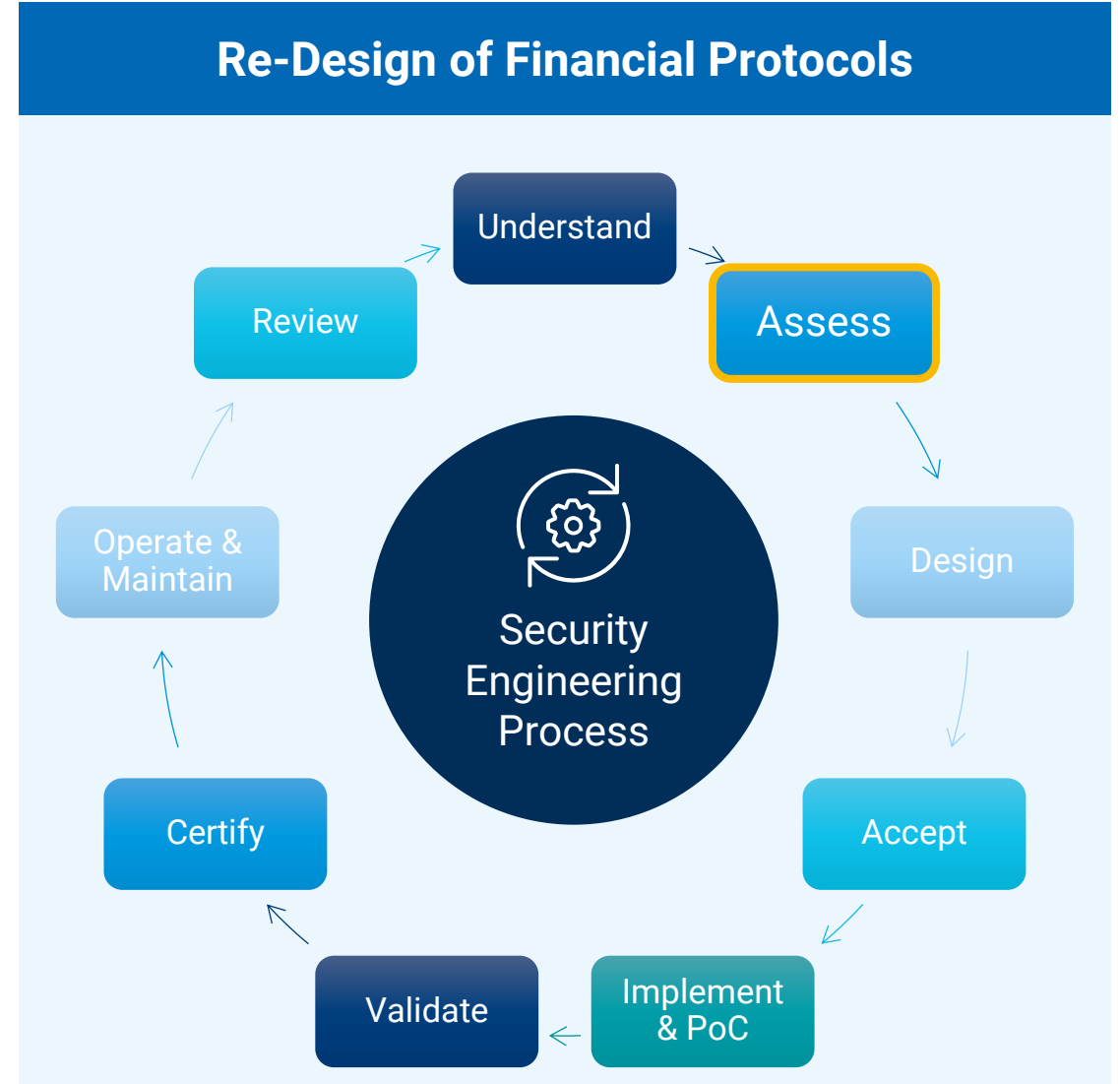
TUVNORDGROUP

**Project Volume: 3.9m EUR**

**Project Start: 08/2024**



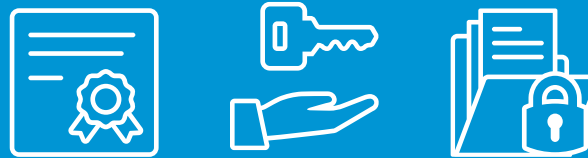
References: <https://www.ebics.de>



## The building blocks – HSMs role in PQC



## Security systems use PQC and HSMs to protect their operation



## Ecosystems use security systems for PQC



### Commercial use well under way

HSMs are key to ensure a safe migration to PQC

### Commercial solutions in prep

Key security systems are in the process of adding PQC support

### PQC adoption at research stage

Ecosystems still require fair amount of research for migration



# Q&A

