Post-Quantum

Cryptography Conference

PQC in Action: From Global Standards to Secure Deployments

Nils Gerhardt
Chief Technology Officer at Utimaco

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

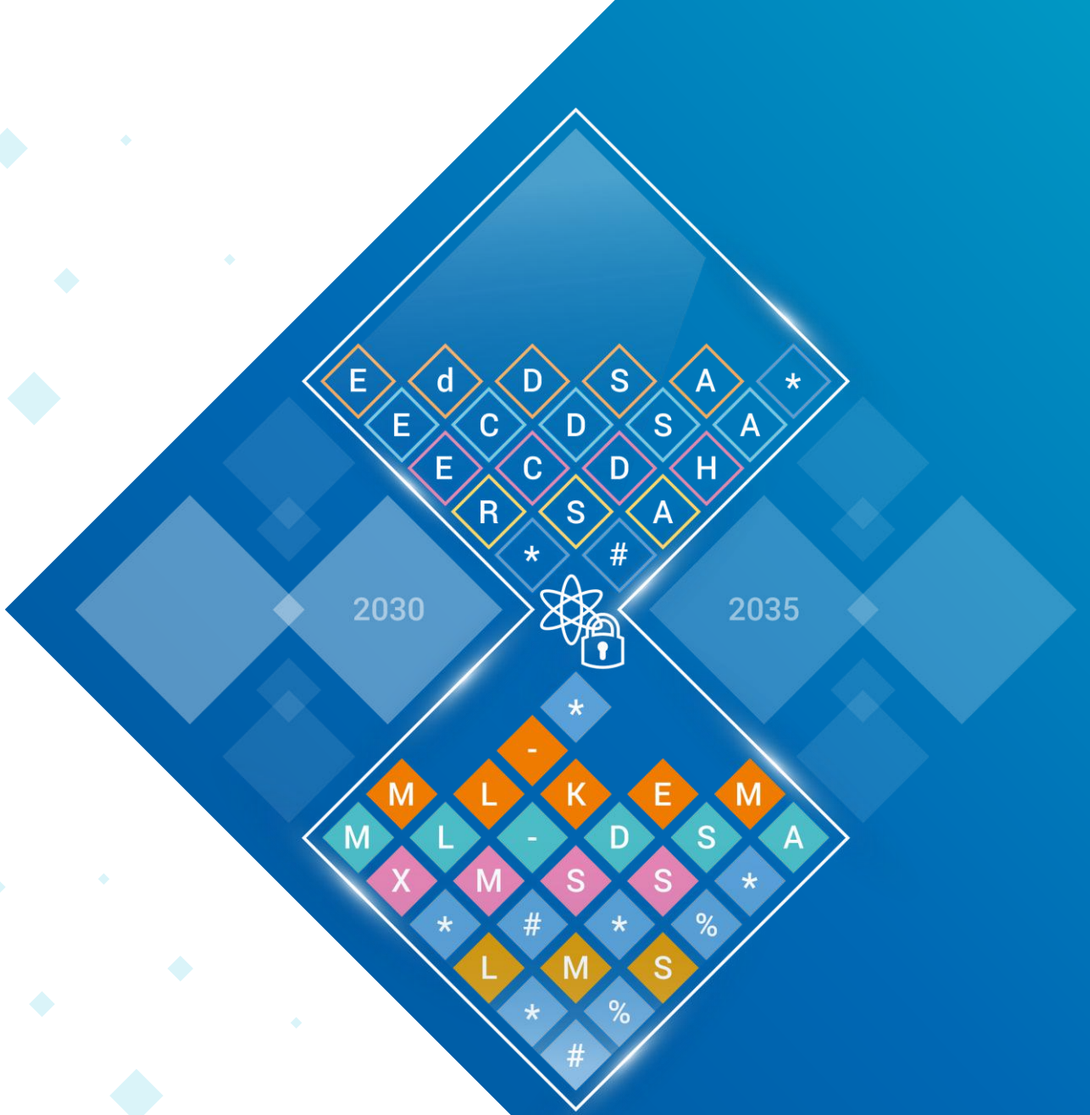
PKI Consortium

utimaco®

The Better Choice for Trust in the Digital Society

PQC in Action:

From Global Standards to Secure Deployments



Nils Gerhardt

CTO Utimaco

Kuala Lumpur, October 29th, 2025

Creating Trust in the Digital Society

utimaco®

Utimaco’s engagement in PQC

Shaping Tomorrow’s Cryptographic World

PQC Consortium: Work Streams Interoperability, Discovery	X9 Post Quantum Cryptography Committee	ETSI Quantum-Safe Cryptography (QSC) Working Group
PQC Consortium: PQC Workstream	White House Roundtable, January + August 2024	And further

ICMC, April 2025

FROST & SULLIVAN
2024 BEST PRACTICES AWARD
GLOBAL POST-QUANTUM CRYPTOGRAPHY COMPETITIVE STRATEGY LEADERSHIP AWARD

Frost & Sullivan 2024 PQC Award

PQC Roundtable at the White House, August 2024

Patented solution for state handling

Post-Quantum Cryptography Conference

The Power of Standardization

NIST Update (1/2)

Standards and activities for PQC migration

NIST Standards

- **2020:** XMMS / LMS
- **2024:** FIPS 203 - ML-KEM, FIPS 204 - ML-DSA/, FIPS 205 - SLH-DSA
- **2025:** HQC selected to be standard in 2027
- Falcon (FN-DSA)

NIST Ongoing Activities

- **Digital Signatures:** CROSS, LESS, SQIsign, HAWK, Mirath, MQOM, Perk, RYDE, SDitH, MAYO, QR-UOV, SNOVA, UOV, FAEST — Selection of x/14 algorithms → Standardization
- **Encryption:** BIKE, Classic McEliece — Selection of x/2 algorithms → Standardization

NIST timelines

- Draft NIST IR 8547 issued late 2024 (migration to PQC)
- SP800-227 released (use of KEMs, incl. hybrid)
- Deprecates RSA, ECC with 112-bit security by 2030
- Disallows any use of RSA and ECC in 2035

NIST Update (2/2)

Crypto agility and testing

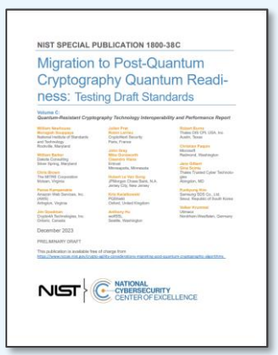
Crypto Agility

- **Start of Working Group** — 2023
- **White paper for comment: NIST CSWP 39 ipd Considerations for Achieving Crypto Agility** — 2025
- **NIST CSWP 39 2pd** — 2025
- **Policy based crypto?** — 2026…
- **Workshop/Conference** — 2025

Inter-operability testing

- **Listing of interoperability results** — 2023
- **Initiation of interoperability testing with round 3** — 2023
- **CAVP/ CSRC** — 2024
- **FIPS submission possible** — 2024
- **CAVP offers two Automated Cryptographic Validation Test Systems (ACVTS)** — 2025…
- **Update with first market feedback** — 2025…

Standardized Interoperability Tests


NIST SPECIAL PUBLICATION 1800-38C

Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards

December 2023

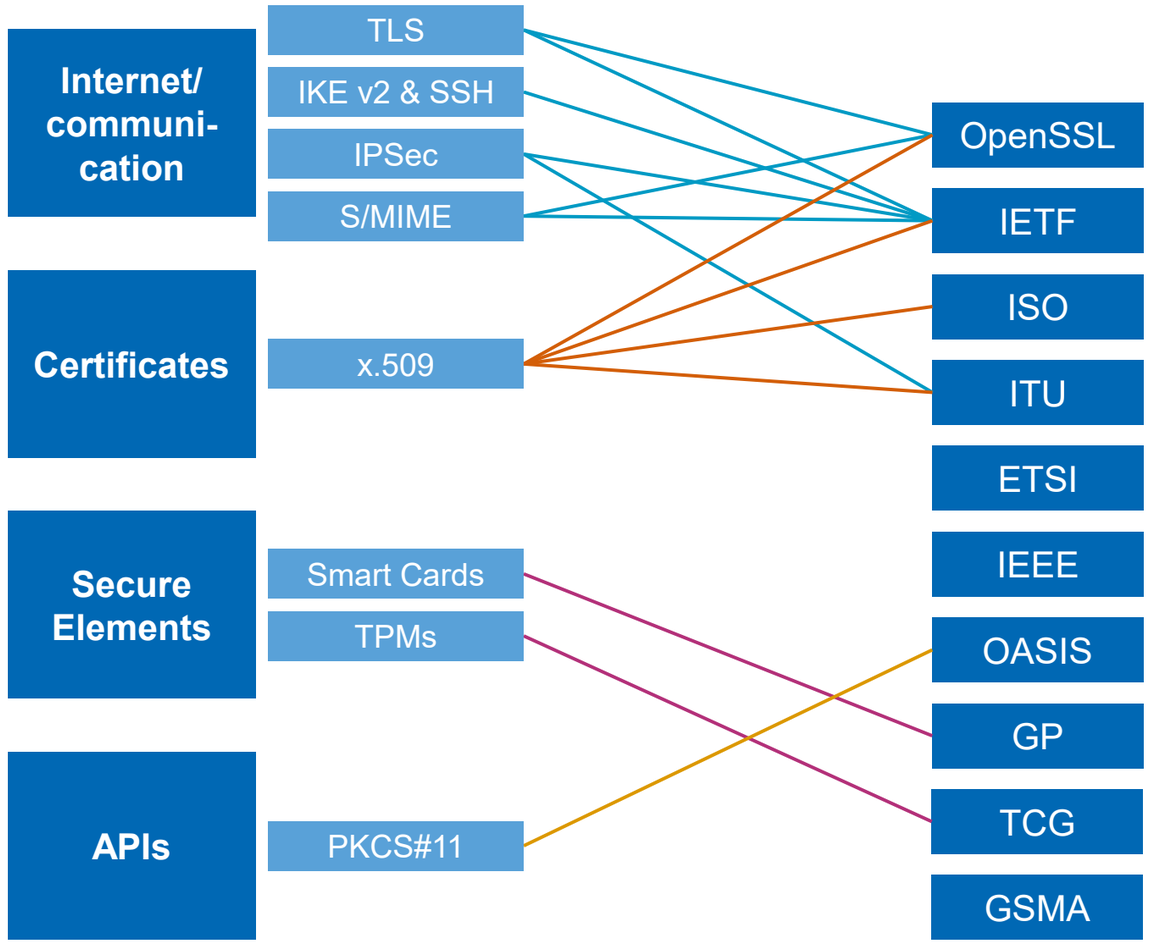
PRELIMINARY DRAFT

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-38C

Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards

Standardization in relevant organizations



Driving Institutions

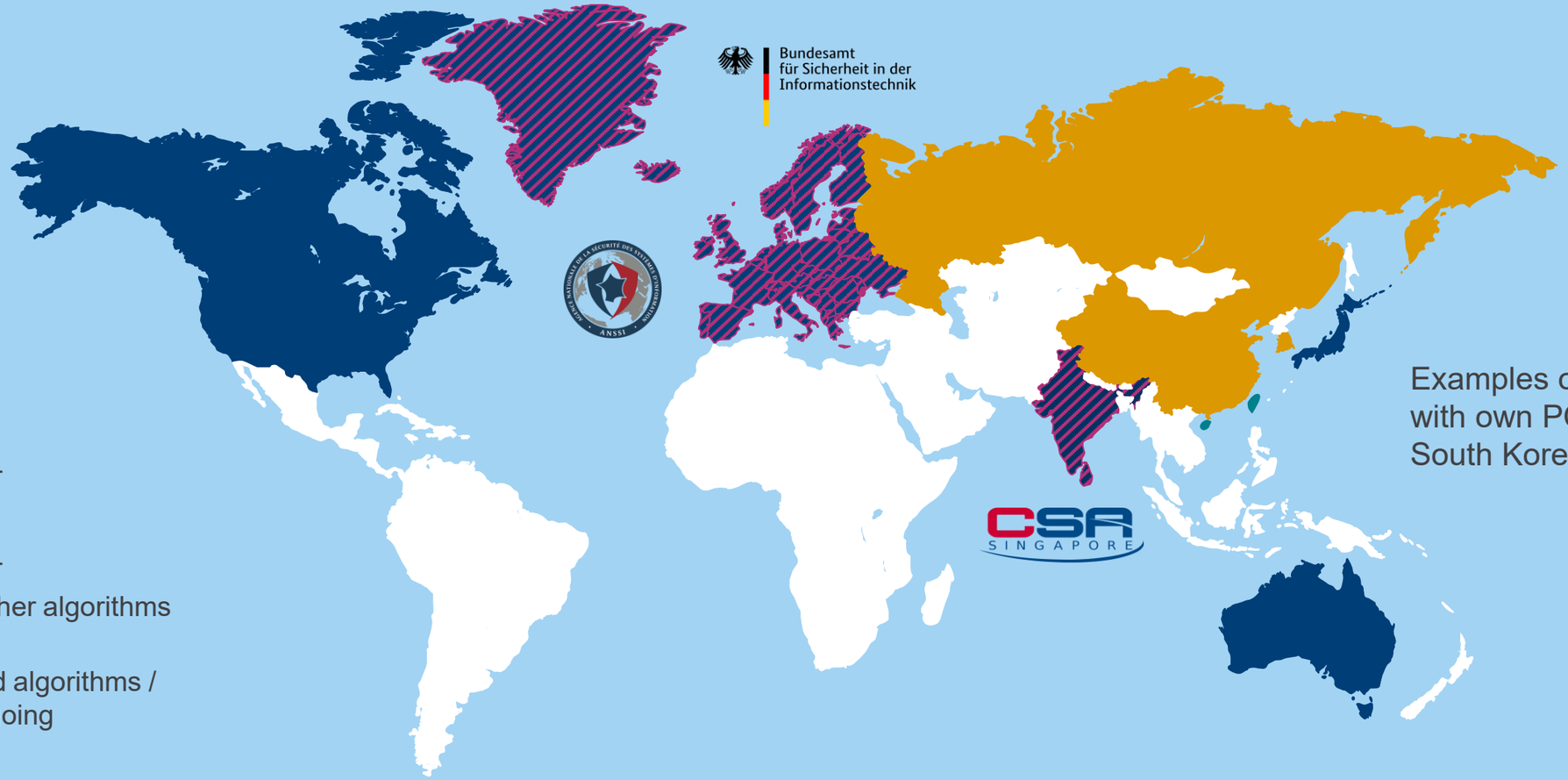
X9 **PKI-Consortium** **NIST**

- OpenSSL 3.5: support for ML-KEM, ML-DSA, SLH-DSA
- NIST refines standards: ML-DSA tech details & State handling
- First Quantum Secure Smart Cards with CC and BSI approved
- **IETF/ISO:**
  - Strong alignment with NIST recommendations
  - Selective adoption e.g. LMS/XMSS in IETF/ISO 14888-4
  - Working groups ongoing for protocols incl. IPSec, IKEv2, TLS 1.3, X.509 in IETF ongoing
  - ISO expected to adopt FrodoKEM as none NIST algorithm
  - IEEE 802.11 PQC standardization ongoing
- **ETSI:** Launch of Q-Safe Hybrid Key Exchange (TS 104 015)
- **Compatibility:**
  - Hybrid is key for protocols, Composite certs for digital sig.

Adoption:
PQC, Hybrid and traditional crypto phase-out

Global view on PQC recommendations: **Strong orientation towards NIST**

utimaco®



NIST

Follows NIST

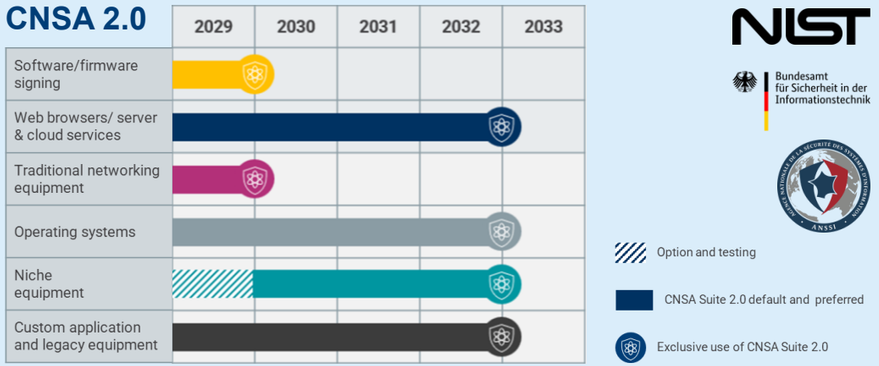
Follows NIST
+ selected other algorithms

Own selected algorithms /
selection ongoing

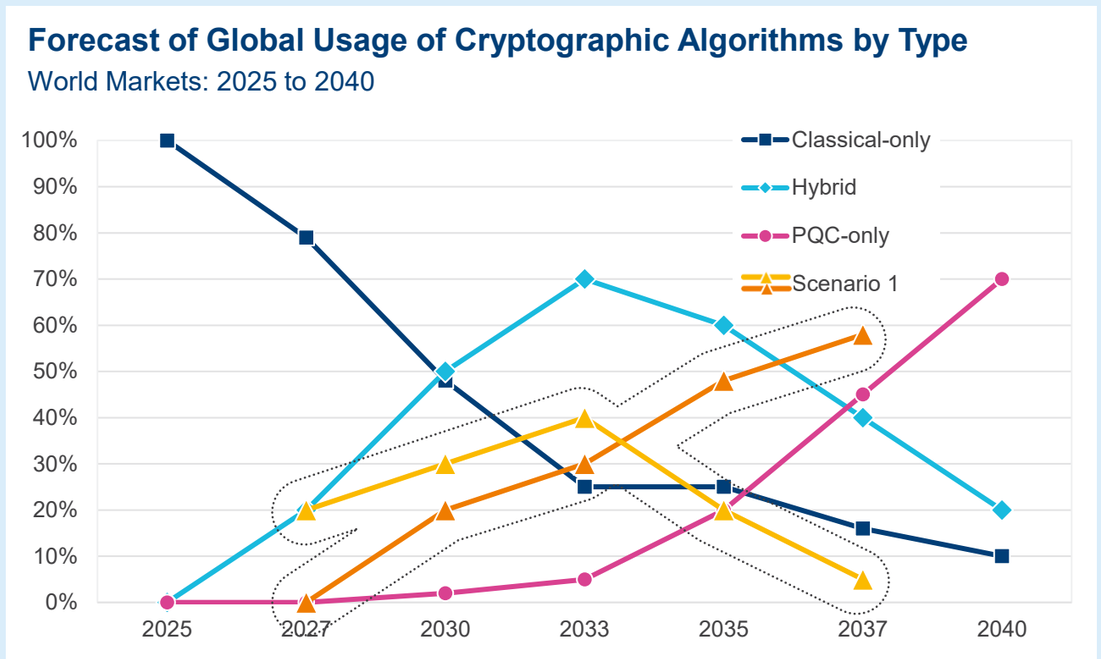
Examples of countries
with own PQC competition:
South Korea, China

Drivers for PQC and Hybrid adoption

A migration prediction



- Hybrid adoption on the rise for compatibility will peak when PQC algorithms are largely standardized and available
- Hybrid for public facing protocols (TLS, VPN), PKI
- PQC only for selected/ green-field use-cases
- Likely pre-dominant use of PQC algorithms by 2040, with few „legacy“ algorithms remaining



Scenario 1/2: Possible Alternative Scenarios

PQC may increase much faster due to regulations
Hybrid methods would show less penetration,

Source: ABI Research

Technologies & Support for PQC are progressing

Update: Applications, PQC libraries & CBOM

- **Botan** is an open-source implementation initiated by BSI under simplified BSD-License
- Release 3.4.0 with support for: ML-KEM, Frodo KEM, ML-DSA, SPHINCS+ and XMSS – Classic McEliece and LMS to follow

- **FIPS-certified open-source cryptographic APIs** for Java and C#
- **Oct/ Nov 2024:** Support of ML-KEM, ML-DAS, SLH-DSA

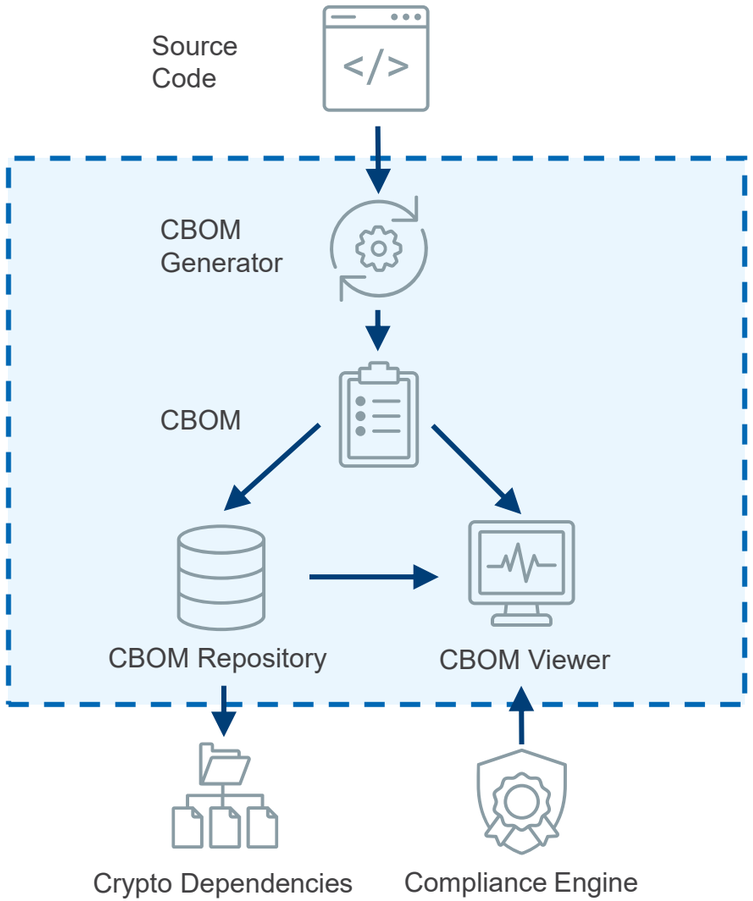
- **OQS is part of the Linux Foundation**'s Post-Quantum Cryptography Alliance
- OQS consists of **two main lines of work**:
  1. an open-source C library for PQC (liboqs), and
  2. prototype integrations into protocols and applications, including a fork of the OpenSSL library.

AWS-LC

- general purpose cryptographic library maintained by AWS
- ARM and x86 optimized algorithms
- AWS-LC FIPS 3.0 in FIPS 140-3 CMVP review: includes ML-KEM

wolfSSL

- SLH-DSA, LMS, XMSS, ML-KEM and ML-DSA (CNSA 2.0 compliant)
- ARM and x86 optimized algorithms



Update on applications, PQC libraries and CBOM (2/2)

utimaco®

Cloud/ SSL/TLS, Web Browser	Cloudflare, Meta, Google, wolfSSL, OpenSSL Library, aws, kubernetes
Email/ Messaging	iMessaging iOS and iPad OS 17.4 and macOS 14.4 Signal Protocol PQXDH ("Post-Quantum Extended Diffie-Hellman")
Operating Systems	Microsoft PQC support in SymCrypt and CNG (preview) for Windows and Linux
VPN	genua. genuscreen 8.4 CC EAL 4+ Microsoft Post-quantum Cryptography VPN (Open VPN Fork) paloalto NETWORKS NetSec Platform CISCO

PQC “ingredience” readiness

- Critical components need to be available for the PQC migration including

Open-Source Libraries for algorithms

IP-Cores for FPGA implementations

Secure Tokens (e.g. Smart Cards) for authentication and security

Means to manage (stateful) algorithms securely

Hardware acceleration

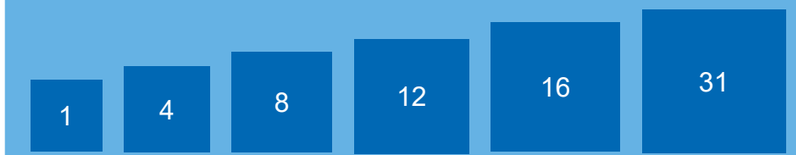
Customer Projects are progressing and diversifying

HSMs: Root of Trust in a Quantum World

utimaco®

Multi tenancy to enable cloud

- Available in different models varying in the number of virtual HSMs



PQC available via Standard interfaces – No Vendor Lock-In

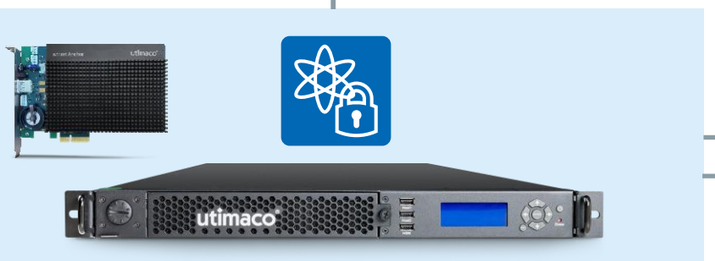
- Integration for instance via PKCS#11

High performance ready for future applications

- Implemented next-generation FPGA or ASIC allows hardware acceleration for future, more demanding use cases

Simulator – Test before you deploy

- Easy installation
- Shorter project evaluation
- Fully functional
- Test before buying
- Ideal for integration testing



Future-proof hardware, crypto-agility supported

- Flexible HW form factors: Appliance, PCIe, portable
- Regular firmware updates including new versions of algorithms

Entropy

- True randomness for a maximum in key security

Universal PQC algorithm support

- Lattice-based: ML-KEM, ML-DSA, SLH-DSA
- Hash-based: LMS, HSS, XMSS, XMSS-MT,
- Frodo-KEM
- Stateless experience of SHBS algorithms
- etc.

PQC in Practice – Customer Segments

- Customer projects extend over various industries with multiple use cases

Satellite communication

- Worldwide Broadband services
- Telemetrics control
- XMSS incl. state handling (sign)
- ML-KEM (key enc.)

Chip Manufacturing

- Key injection for long-term secure firmware updates
- Combination of ML-DSA (sign) and ML-KEM (enc.)

IT Infrastructure

- Use of LMS for (long-term) firmware protection
- Use of Utimaco application to make SHBS algorithms appear stateless

OEMs/ PKIs

- Provision of PQC algorithms as part of own product offering
- Integration of HSMs for PQC into PKI infrastructure

Learnings from customer projects

- PQC is coming and projects are progressing fast

Performance

- PQC in SW was sufficient
- Key generation is less critical
- Signing will require higher performance incl. acceleration
- Highly use case dependent

Interfaces

- Customers that started early, still on PKCS11 alike interfaces
- New standard expected: PKCS11 v3.2
- Other interfaces will follow (e.g. REST)

Regions

- US migration moves first
- EU started a bit later than US
- Asia is expected to start soon

Interop Testing

- CAVP becomes must item
- First “different” interpretations between standards arise
- Vendor Interop testing to continue
- Key import/ export

Application support

- PQC support in HSM was first
- Other applications require PQC support now incl. file and folder encryption, key management and PKI systems

Technology

- Most greenfield projects start as PURE PQC implementations
- Need for Hybrid given due to legacy and for risk mitigation

2025 Utimaco PQC Readiness Survey

Recommendations backed by survey peer results

63%

Public Key Infrastructure (PKI) most urgent **priority**

Over **50%** **In Progress** or plan to start **within 1-3 years**

Nearly **2/3** will follow a **hybrid approach**

Prioritize Use Cases

Get Your Timeline in Place

Consider Alternative Approaches

Inventory Legacy Systems

Collaborate Internally & Externally

Download the 2025 Utimaco PQC Readiness Report Today!

56%

obstacles from legacy systems as a key concern or challenge

Almost **50%**

of **CISOs** or **CTOs** are **leading** the efforts.

Time for Your Questions

utimaco®

Q&A

Any further feedback: hsm@utimaco.com

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