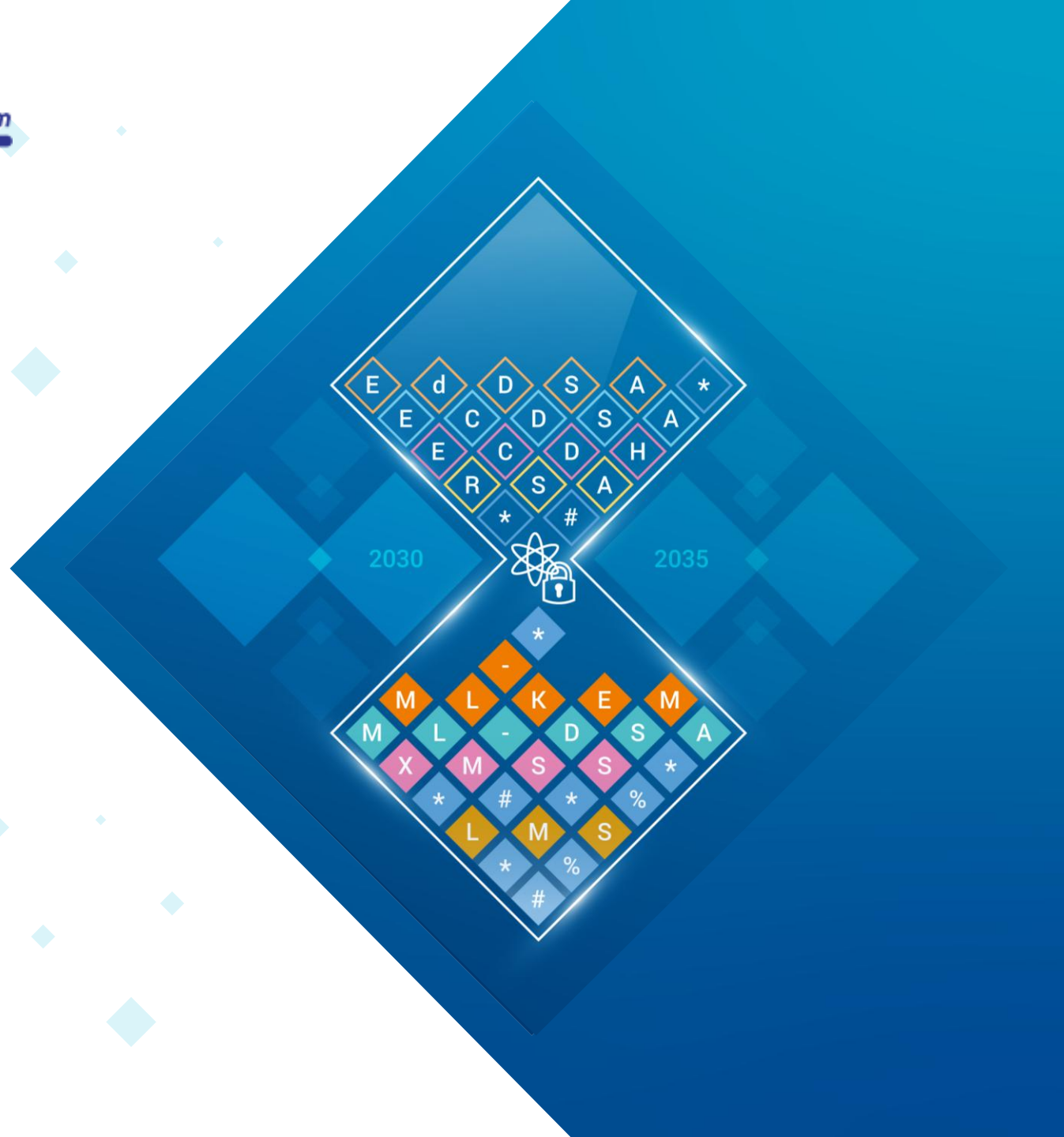
utimaco®

The Better Choice for Trust in the Digital Society

Asia PKI Consortium

HSM and KMS Infrastructure for PQC Migration



Name : Teo Poh Soon, APAC

What is Q-Day? :

It’s not a hard date for organization to protect their Digital Asset with Quantum Resistance Algorithm, It’s a process for Organization to be protected.

The timeline is shifting

- The shrinking of Engineering Gap –Goggle and Microsoft have committed to the entire core infrastructure to migrate to PQC by 2029. The shift is triggered by rapid leaps in Superconducting quantum architectures and Peer-review research indicating a 20 times reduction of physical resource to break Classic Algorithm.
- Transition from “Policy” to Hard Deadlines - Following the NIST’s Finalization of FIPS 203, 204, and 205, CISA and White House enacted a strict Federal buying Guidance that only use PQC ready security device. White House released OMB M-26-15 to enable agencies to assign PQC migration leads and deliver final and comprehensive migration plans. The Impending Procurement freeze, under CNSA 2.0, January 2027 all security acquisitions, operating Systems and deployment must be PQC algorithm by default.
- Shift in Technical Readiness (The Hybrid Protocol Standard) – The internet Engineering Task Force standardized Hybrid PQC Key exchange in TLS 1.3. It provide the compliant bridge for Tech stacks to begin dual-layer encryption without complete replacement of PKI.



NSA : Starting in 2027, all new commercial NSS must support quantum-resistant algorithms. Legacy systems not supporting quantum-resilient algorithms are to be phased out by 2030.

APAC PQC Regulation Timeline

Country	Primary Regulator	Target Sector	Plan Due / Legislative Status	Procurement Mandate	Full Migration Deadline
Singapore	CSA / MAS	CII & Financial	March 31, 2027	Jan 1, 2028 (PQC-ready required)	Dec 31, 2031
Australia	ASD / ACSC	Gov & Critical Infrastructure	End of 2026	Phased by data risk (2028)	End of 2030
Thailand	NCSA	CII, Finance, & Gov Services	In Parliamentary Vetting	Phased via QUANTA platform	2030 (Finance) / 2035 (All CII)
Indonesia	BSSN / Kemenko Polkam	Gov, Military, & Strategic Networks	In Parliamentary Vetting	2027 (Quantum VPN implementations)	2030 (Strategic Networks)
Japan	NCO / CRYPTREC	Government Agencies	Ongoing	2026 (Hybrid standards)	2035
Malaysia	NACSA	Gov & NCII Sectors	Ongoing Audits	Phased	2030 (Gov) / 2035 (NCII)
India	DoT	Telecom & Tech Infrastructure	—	2026 onward	Phased implementation

PQC Standardization :

It has move from algorithm selection to deployment, interoperability, and operational migration.

“Which PQC algorithm is standard?” but

“How do wee deploy PQC across various use case”

APAC PQC Regulation Timeline

Country	Primary Regulator	Target Sector	Plan Due / Legislative Status	Procurement Mandate	Full Migration Deadline
Singapore	CSA / MAS	CII & Financial	March 31, 2027	Jan 1, 2028 (PQC-ready required)	Dec 31, 2031
Australia	ASD / ACSC	Gov & Critical Infrastructure	End of 2026	Phased by data risk (2028)	End of 2030
Thailand	NCSA	CII, Finance, & Gov Services	In Parliamentary Vetting	Phased via QUANTA platform	2030 (Finance) / 2035 (All CII)
Indonesia	BSSN / Kemenko Polkam	Gov, Military, & Strategic Networks	In Parliamentary Vetting	2027 (Quantum VPN implementations)	2030 (Strategic Networks)
Japan	NCO / CRYPTREC	Government Agencies	Ongoing	2026 (Hybrid standards)	2035
Malaysia	NACSA	Gov & NCII Sectors	Ongoing Audits	Phased	2030 (Gov) / 2035 (NCII)
India	DoT	Telecom & Tech Infrastructure	—	2026 onward	Phased implementation

utimaco.com © 2026 Unrestricted

Cryptographic Algorithms

From Draft to Product

Algorithm Draft

Academic Proposals

Research Projects

NIST Submissions

Early Adopters

Satandardization

NIST

ISO

ITU

ESTI

IETF

Other national Standards

API /Integration

PKCS11

Java JCE

Microsoft CNG

RESTful

KMIP

Proprietary

Performance

Software Optimizations

FPGA support

ASIC support

Often in conflict with side-channel resistance

Certification

Product is certified according to Industry Standard

FIPS 140-3

VSNfD

PCI

CC / eIDAS

NITES

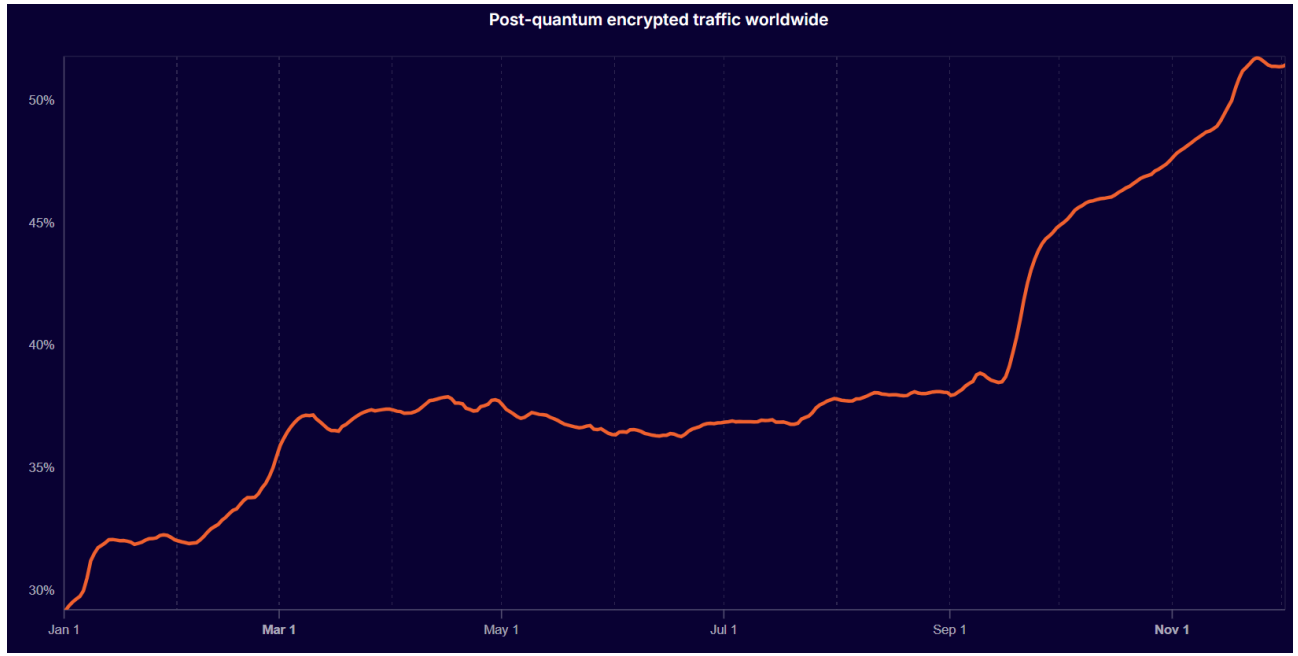
Customization

Special Markets and countries

Use case Specific protocols

PQC Adoption on the Internet

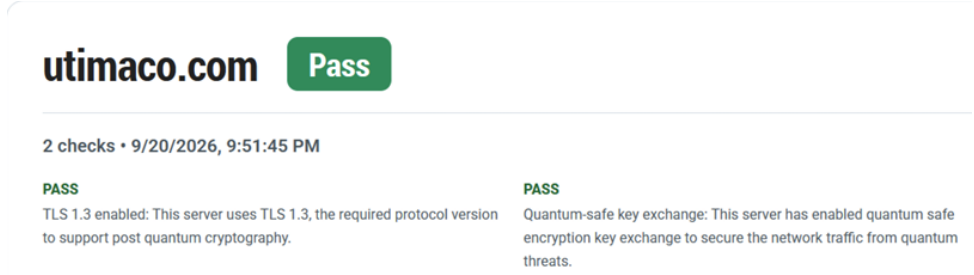
Over 64% of Human-based Internet Connections use PQC encryption (not signatures)



Cloudflare Radar 2025 Year in Review

July 2016	Chrome's first experiment with PQ (CECPQ)
June 2018	Cloudflare / Google experiment (CECPQ2)
October 2022	Cloudflare enables PQ by default server side
November 2023	Chrome ramps up PQ to 10% on Desktop
March 2024	Chrome enables PQ by default on Desktop
August 2024	Go enables PQ by default
November 2024	Chrome enables PQ by default on Android and Firefox on Desktop.
April 2025	OpenSSL enables PQ by default
October 2025	Apple is rolling out PQ by default with the release of iOS / iPadOS / macOS 26.

State of the post-quantum Internet in 2025 | Cloudflare Blog



Adoption in X.509

- Use HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure RFC 9802
- Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-base Digital signature algorithm (ML-DSA) RFC 9881
- Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA).

draft-ietf-lamps-fn-dsa-certificates-00 - Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)

- Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) RFC 9909

Adoption in ESTI Trust Infrastructures





Table 2: Digital Signature Algorithms

Short signature algorithm name	References	R/L
RSA-PKCS#1v1_5	IETF RFC 8017 [3]	L
RSA-PSS	IETF RFC 8017 [3]	R
DSA	FIPS Publication 186-5, ISO/IEC 14888-3 [4]	R
ECDSA	FIPS Publication 186-5 [2]	R
EdDSA	IETF RFC 8032 [23]	R (see note 1)
ML-DSA	NIST FIPS Publication 204 [26]	R
SLH-DSA	NIST FIPS Publication 205 [27]	R
EC-SDSA-opt	ISO/IEC 14888-3 [4]	L
LMS	IETF RFC 8554 [28]	R (conditional, see note 2)
XMSS	IETF RFC 8391 [29]	R (conditional, see note 2)

NOTE 1: EdDSA is not an agreed digital signature scheme under the ECCG Agreed Cryptographic Mechanisms [14]. The "R" status assigned to EdDSA in Table 2 reflects the recommendation of the present document independently of the ECCG ACM.

NOTE 2: LMS and XMSS are stateful hash-based signature schemes. Their use requires that the implementer establishes and maintains secure state management procedures to prevent private key reuse. Failure to manage state correctly may result in complete compromise of the signing key. The use of LMS and XMSS is therefore restricted to deployment environments where state management can be strictly enforced.

- **ML-DSA**
  - ML-DSA-44: acceptable where ML-DSA-65 or ML-DSA-87 is not feasible. ML-DSA-65 or ML-DSA-87 preferred
  - HashML-DSA is excluded
  - For HSM-based or remote signing scenarios External Mu allowed
- **SLH-DSA**
  - pure, non-hybrid deployment model allowed
  - HashSLH-DSA is permitted if pre-hash function provides 192 bits collision resistance.
- **XMSS/LMS**
  - pure, non-hybrid deployment model allowed
  - specifically suitable for use cases such as firmware signing and time-stamping
  - Implementers shall establish, document, and enforce secure state management procedures to prevent private key reuse

Hybrid Signatures in Trust Infrastructures

- **Signer Certificates**: During the transition to Post-Quantum Cryptography, hybrid certificates containing both classical and post-quantum keys (or multiple certificates linked via specific extensions) are **RECOMMENDED** for CA issuing keys to ensure long-term security.
- **OCSP responses**: During the transition to Post-Quantum Cryptography, OCSP responders may sign responses using hybrid schemes (e.g. classical signature + post-quantum signature) to ensure long-term non-repudiation.
- **CA certificates**: During the transition to Post-Quantum Cryptography, hybrid CA certificates (e.g. using X.509 alternative public key extensions or composite keys) are RECOMMENDED for Issuer CA keys to ensure long-term security of the PKI hierarchy.
- **Root CA certificates**: To ensure long-term security during the transition to Post-Quantum Cryptography, issuers should consider using hybrid schemes (e.g. using X.509 alternative public key extensions to carry a PQC key alongside a classical key) for Root CAs.
- **TST issuers**: should support SLH-DSA, XMSS or LMS
- **TST verifiers**: shall support SLH-DSA, XMSS or LMS
- For long-term archiving (> 20 years), the use of Post-Quantum Cryptography is required. XMSS (IETF RFC 8391 [29]) and LMS (IETF RFC 8554 [28]) are stateful hash-based signature schemes specifically recommended for use cases like firmware updates and time-stamping, where the state management can be securely handled by the TSU.
- **TSU certificate**: should support Hybrid (Classical + ML DSA)
- **TSU public key**: should support SLH-DSA, XMSS or LMS (PQC)
- XMSS and LMS are specifically **RECOMMENDED** for Time Stamping Units (TSUs) where state management can be strictly enforced by the cryptographic module, providing high security assurances against quantum computer attacks for long-term validation.

Adoption in PKCS #11



Asia PKI Consortium

utimaco®

October 2020:

Stateful hash-based signature schemes:
LMS, XMSS, HSS, XMSS^{MT}

August 2024:

Final Standards

ML-DSA, ML-KEM,

SLH-DSA

Q4 2026 – Q1 2027 (?):

Composite Signatures and KEMs

SLH-DSA w/ reduced parameter sets

v3.0 (June 2020)	v3.1 (July 2023)	v3.2 (June 2026)	v3.3 (target mid 2027)

• No PQC	• LMS/HSS	• XMSS(-MT)
		• SLH-DSA
		• ML-DSA
		• ML-KEM
		• API Adaptions
		  • for KEM support: C_Encapsulate / C_Decapsulate
		  • For verification where signature is needed at the beginning: C_VerifySignature…
			• ML-DSA external mu
			• T/PQ composite ML-DSA*
			• T/PQ composite ML-KEM*
			• SLH-DSA reduced parameter sets (NIST SP 800-230)**

Vendor defined mechanisms: support proprietary extensions

* Depending in release of RFC‘s by IETF

** Depending on official publication by NIST

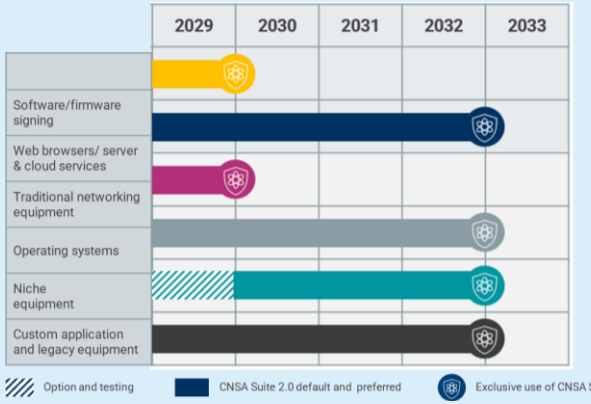
A cryptanalytical-relevant Quantum Computer is expected in 2029.

PQC, Hybrid and traditional crypto phase out

Drivers for PQC and Hybrid adoption

A migration prediction

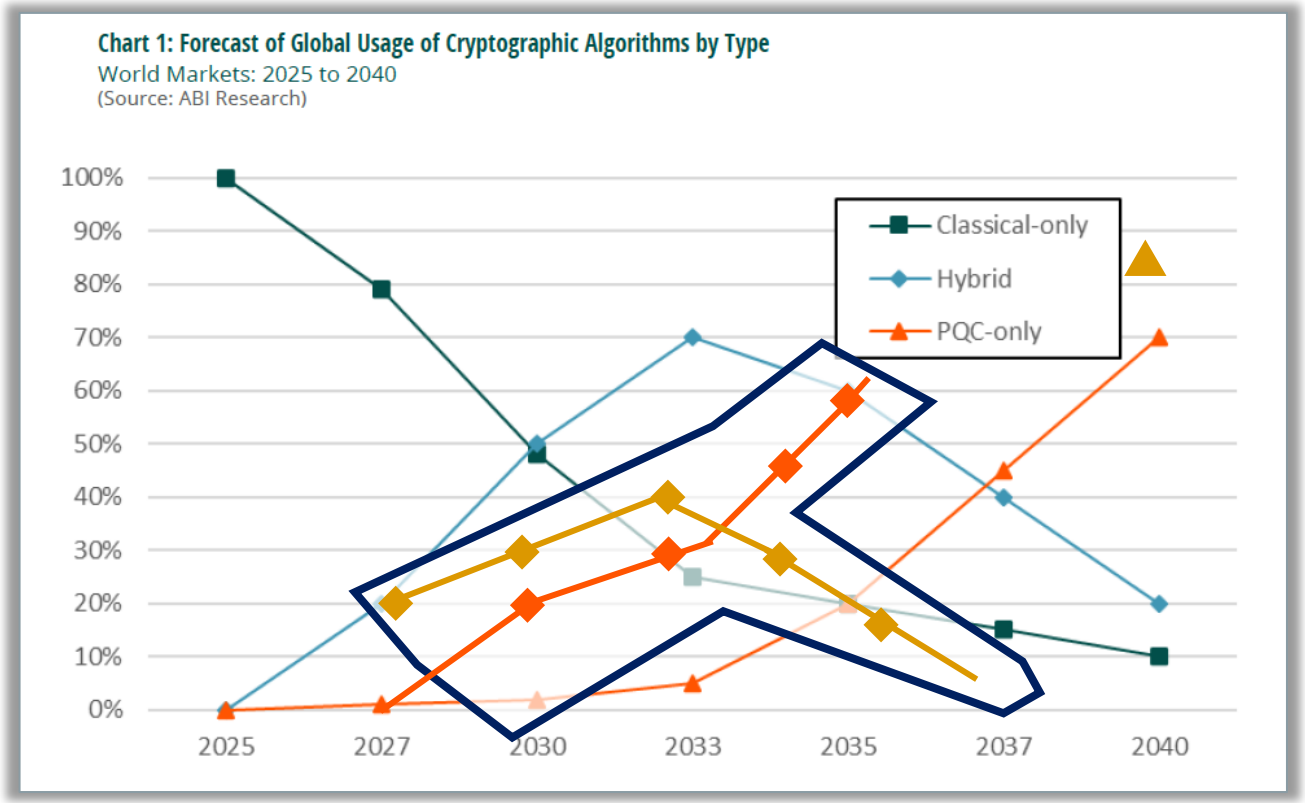
CNSA 2.0



NIST

Bundesamt für Sicherheit in der Informationstechnik

- Hybrid adoption on the rise for compatibility will peak when PQC algorithms are largely standardized and available
- PQC only for selected use-cases
- Strong influence: NIST communicated sunset of RSA/ECC by 2035
- Likely pre-dominant use of PQC algorithms by 2040, with few „legacy“ algorithms remaining

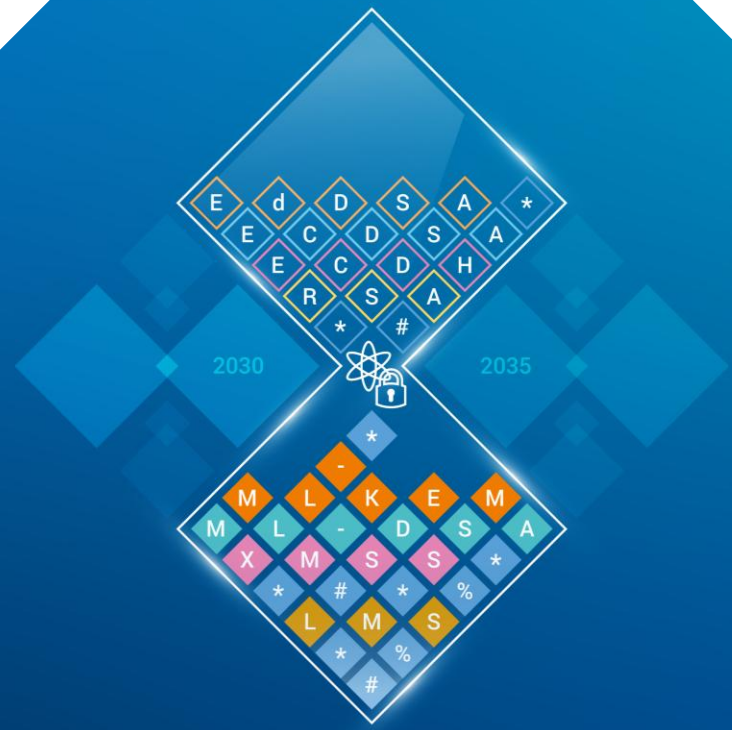


Possible Alternative Scenario

PQC may increase much faster due to regulations

Hybrid methods would show less penetration,

Utimaco 2025
PQC Readiness Report



Unrestricted

2025 Utimaco PQC Readiness

Recommendations backed by survey peer results

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

63% see **Public Key Infrastructure (PKI)** as most urgent **priority**

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

56% **obstacles from legacy systems** as a key concern or challenge

Almost **50%** of **CISOs** or **CTOs** are **leading** the efforts.

Download the 2025 Utimaco PQC Readiness Report Today!

Quantum-resistant strategies

Quantum Key Distribution

- Technique for securely exchanging keys using quantum mechanics
- Built-in eavesdropping detection: By utilizing entangled quantum states
- Believed to be Resistant to attacks by both classical and quantum computers
- Use case limitations and high investment costs

Symmetric cryptography

- Generally considered secure against quantum attacks
- Grover's algorithm can speed up brute-force attacks on symmetric keys
- Impact can be mitigated by larger symmetric key length
- Only suitable for encryption, not for digital signature use cases

Hybrid cryptography

- Combination of classical algorithms and PQC algorithms
- Allow a gradual transition to PQC-only use cases
- Layered security approach (“on the safe side”)
- Might have an impact on performance and memory space

Full PQC adoption

- Cryptographic algorithms that withstand cryptanalytic attacks by quantum computers
- Rely on “hard mathematical problems”
- Use cases: Key agreement and digital signatures
- Standardized algorithms:
  - ML-KEM (FIPS-203)
  - ML-DSA (FIPS-204)
  - SLH-DSA (FIPS-205)

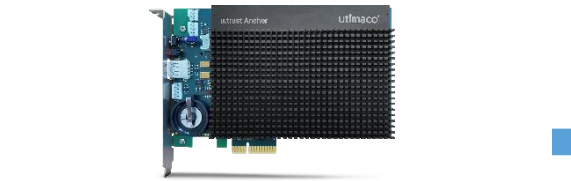
HSM and KMS - Ready for Quantum Future



© 2025
Unrestricted

Utimaco's PQC Solution

Prepared for Quantum-secure Use Cases – Already in Use Today



Crypto agile Hardware Security Module

Post Quantum Cryptography Firmware extension

Hybrid cryptography implementation possible

Convenient firmware extension, no hardware exchange

Simulator Available NOW!

Utimaco PQC Algorithm Suite

Digital Signatures	Key Encapsulation
CRYSTALS-Dilithium	CRYSTALS-KYBER
LMS, HSS	
XMSS, XMSS-MT	
On the roadmap	
SPHINCS+	Frodo-KEM
FALCON	Classic McEliece

Including patent for **state handling** of stateful hash-based signatures

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/selected-algorithms

Unrestricted

Apply high security standards

u.trust General Purpose HSM Se-Series



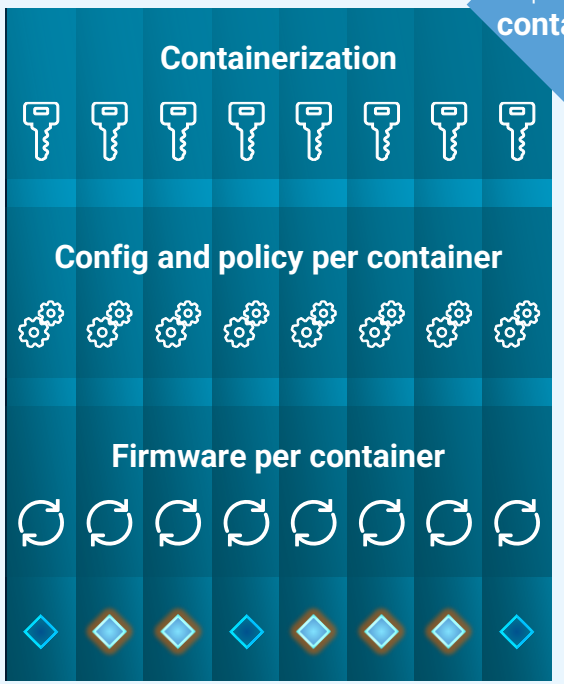


Generate PQC keys in a high-security environment!

- Multi-tenancy with up to 31 containers
- Designed crypto agile
- FIPS 140-3 Level 3 certified
- SDK for custom implementations
- Free, fully functional simulator

- General Purpose HSM (e.g. FIPS / Non-FIPS)
- SDK - customized
- Blockchain
- 5G
- Payment
- PQC

Up to **31** containers



Unrestricted

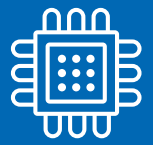
PQC in Practice

Utimaco customer projects



Satellite communication

- Providing fast, affordable broadband to communities around the world
- XMSS incl. state handling (signatures)
- ML-KEM (key encapsulation)



Chip Manufacturing

- Customer: NXP
- Key injection for long-term secure firmware updates
- Combination of ML-DSA (signatures) and ML-KEM (encryption)



Code Signing

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

Test the algorithms

Utimaco
Quantum Protect Simulator

Asia PKI Consortium

utimaco®

Free PQC simulator for testing and evaluation

Includes NIST-standardized PQC algorithms supported by Utimaco Quantum Protect

- ML-KEM
- ML-DSA
- XMSS and XMSS-MT
- LMS and HSS

Easy installation

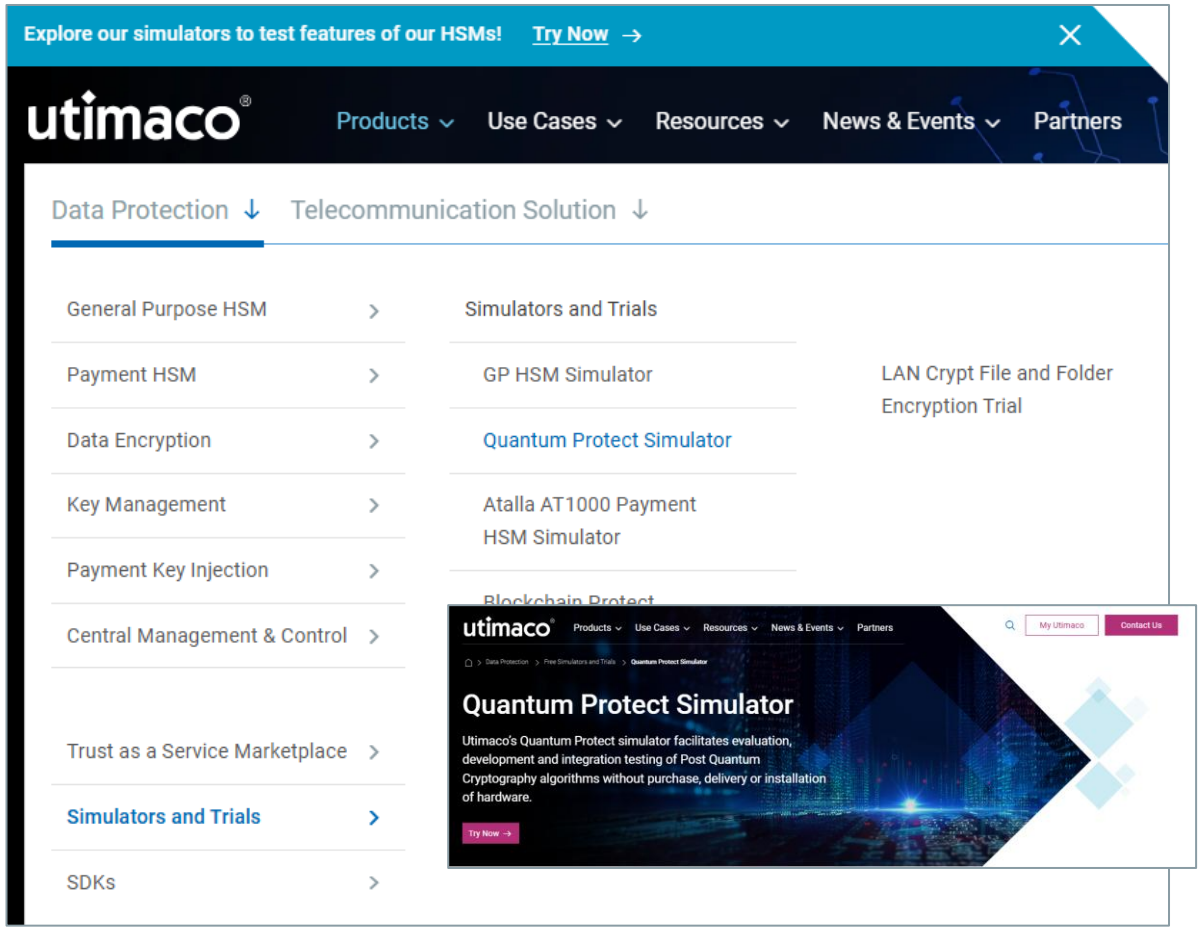
Test before buying

Shorter project evaluation

Ideal for integration testing

Fully functional

Free PQC simulator



Key Management – Enterprise Secure Key Manager

Enterprise Secure Key Manager

- **Centralize Key Management**

  Consolidate both Symmetric and Asymmetric Keys

- **Scalable to thousands of nodes, and millions of keys**

  Unprecedented Capacity for >2 million keys, >25,000 clients, and thousands of ESKM nodes per distributed cluster.

- **Competitive Application Programming Interfaces (APIs)**

  OASIS KMIP (Key Management Interoperability Protocol) ◆ RESTful interface API ◆ KMS ◆ ESTI 014
  ◆ Industries broadest integration portfolio.

- **Highest Level of Security on the Hardware Level**

  Security hardened Linux-based server appliance with encrypted redundant storage
  ◆ FIPS-compliant architecture*, certificate-based authentication, and built-in CA ◆ Embedded Utimaco GP HSM for highest local key protection** ◆ Integration with CC and VS-NfD certified Utimaco GP HSM for key protection compliant to specific compliance requirements***

- **Cloud and on-prem workloads**

  Utimaco's Enterprise Secure Key Manager (ESKM) offers organizations of all sizes a superior solution for key storage and management capabilities, delivering high security and compliance; whether on premises or in the cloud.

- **Simplified Key Lifecycle Management**

  Enables unified enterprise key management with reliable policy controls, centralized administration, and comprehensive audit trails.



* FIPS 140-3 Level 2 appliance (pending), FIPS 140-2 L3 and L4 (embedded HSM)
** For ESKM L3 and ESKM L4 (physical)
*** for vESKM

Unrestricted

Key Management – Enterprise Secure Key Manager

Deployment and Features – Enterprise Secure Key Manager

Deployment Options

Fully functional **60 day trial** of **vESKM***

Network Appliance

- Level 2: FIPS 140-3 Level 2 appliance (pending)
- Level 3: With embedded FIPS 140-2 Level 3 embedded HSM
- Level 4: With embedded FIPS 140-2 Level 4 embedded HSM



Virtual Appliance

- Level 1: Designed to FIPS Level 1 Standards



Features

- Support for OASIS KMIP, RESTful API, KMS, ESTI 014
- Support for various cryptographic algorithms such as AES, 3-Key Triple DES, HMAC, RSA, and ECDSA key types
- Support PQC (In Roadmap)
- Simplified RESTful API interface for key CRUD operations and crypto
- Supports open client libraries such as KMIP, OpenKMIP and PyKMIP
- NIC Teaming Support
- Integrates with all major Cloud Service Providers

*: Registration required

High Availability

A single pane of glass for all cryptographic keys

Unrestricted

Questions & downloads

Contact:

hsm@utimaco.com

2025 Utimaco PQC Readiness Report

Free PQC Simulator