UTIMACO
Quantum Computer Age Security

CHUA Zhong Han Pre-Sales Engineer (ASEAN)

August 5, 2025

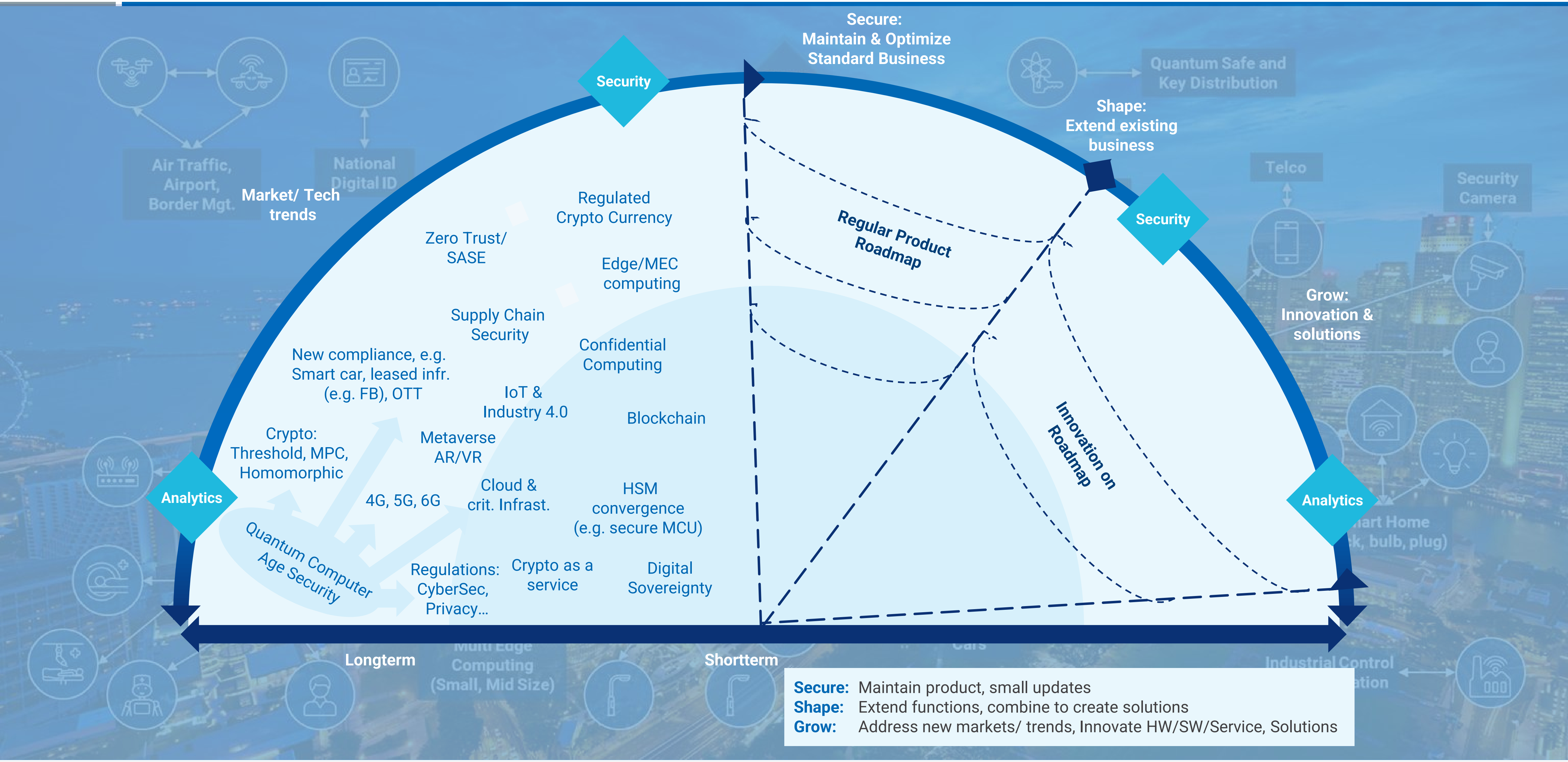
Creating Trust in
the Digital Society

utimaco®

Agenda

1. Tech trends & market size
2. Short intro: Quantum computer
3. Post Quantum Computer Age Security
   - PQC
   - Crypto agility
   - QKD
   - Quantum randomness
4. Addressing the Quantum Threats to the PKI system and application
5. Utimaco strategy and research involvement
6. Industry Organization and Standard
7. CSNA 2.0 and NIST Timeline
8. u.Trust GP HSM, PQC Ready and ESKM, QKD Ready
9. Use case

Tech trends influencing UTIMACO's products & solutions – Quantum Computer Age Security influences most other technology trends



Post quantum computer age security – Estimated market size

	Quantum Computer Age Security
Market size	2030 Q Sec: **$10 bn***
Time relevancy	**2 – 10 years**
Fields to play	PQC · Crypto Agile · Randomness · QKD

* https://thequantuminsider.com/2022/02/02/the-quantum-insider-report-forecasts-quantum-security-market-worth-10-billion-by-2030/

Agenda

Quantum Computers and what they can do (1/2)

Traditional computer with 2 bits – sequential representation of numbers 0 – 3

[0,0] → 0

[0,1] → 1

[1,0] → 2

[1,1] → 3

1 0 2 2 1 3 0 2 0 1 3 0 2 ...

Quantum computer with Qubits – representing the values 1 or 0 and everything in between, simultaneously.

[0,0] → 0

[0,1] → 1

[1,0] → 2

[1,1] → 3

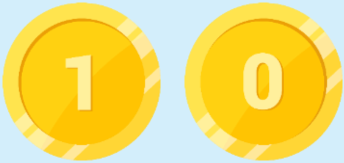
...and more!

01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | 01 23 | ...

Quantum Computers and what they can do (2/2)

Traditional computer –
1 state at a time

Traditional 1 and 0
as determined states



Either 1 or 0

2 Bits: 4	3 Bits: 8
00	000
01	001
10	010
11	011
	100
	101
	110
	111

Quantum Computer –
all states at a time

Various states in parallel

2 qBits: 4	3 qBits: 8
00	000
01	001
10	010
11	011
	100
	101
	110
	111

Qubits interact with each other which improves the processing speed of quantum computers.

Entanglement

Qubits exist in more than one state or location simultaneously.

Superposition

Mega Trend: Quantum Computer

utimaco®

Problem Statement

- Shor’s Algorithm **breaks asymmetric crypto**
  - Breaks **RSA** by quickly factoring large numbers
  - Breaks **Elliptic Curve** Cryptography and **Diffie-Hellman** by solving the discrete log problem
- Grover's Algorithm **weakens symmetric crypto**
  - Square-root speedup on search algorithms
  - **Weakens** symmetric encryption and hashing **by 50%**

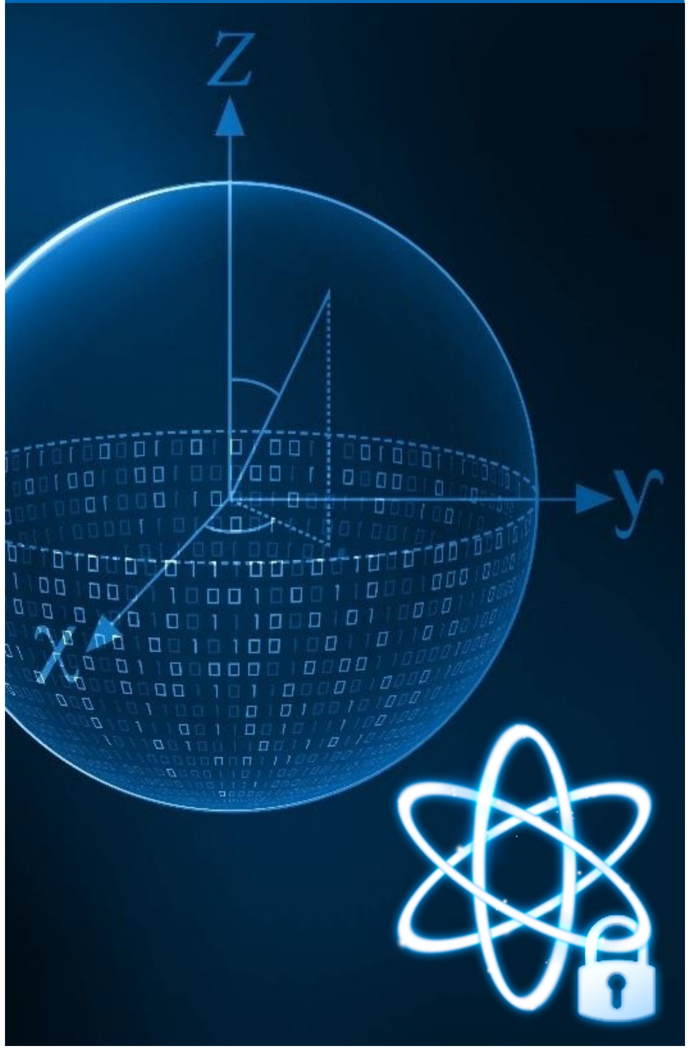
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor’s Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover’s Algorithm
	AES 256	256	128	

Agenda

1. Tech trends & market size
2. Short intro: Quantum computer
3. Post Quantum Computer Age Security
   - PQC
   - Crypto agility
   - QKD
   - Quantum randomness
4. Addressing the Quantum Threats to the PKI system and application
5. Utimaco strategy and research involvement
6. Industry Organization and Standard
7. CSNA 2.0 and NIST Timeline
8. u.Trust GP HSM, PQC Ready and ESKM, QKD Ready
9. Use case

Quantum Computer Age Security – Post Quantum Cryptography

Post Quantum Cryptography



Crypto Use Cases

QC Risk

Solutions

SSL

Email Security

Hardware Encryption

VPN

...

RSA (and ECDSA, DSA…)

4096 bit

AES

-50%

128 ▶ 256 bit

PQC safe algorithms

- Kyber
- Dilithium
- XMSS

Quantum Key Distribution

Crypto agility

Quantum Randomness

Hybrid crypto

Challenges Quantum Computers will bring without PQC

utimaco®

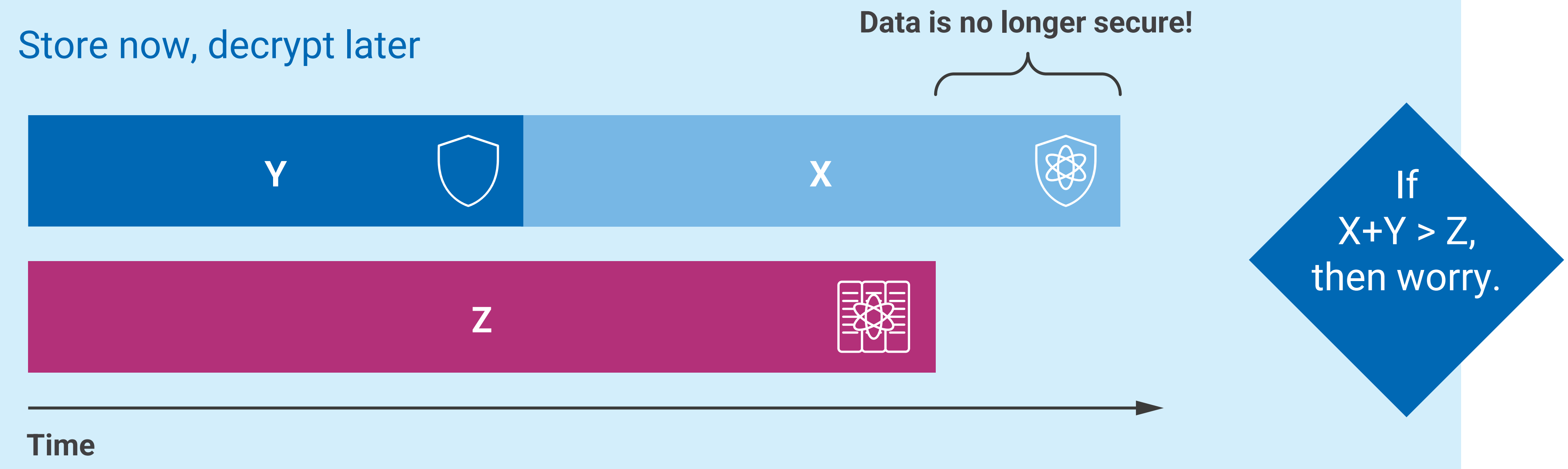
Store now, decrypt later	Digital signatures may be broken
	

How much time is left for getting Quantum Computer Age secure?

utimaco®

Mosca theorem

- **X** = Number of years to protect specific data
- **Y** = number of years needed to convert to Quantum Computer Age security
- **Z** = number of years until Quantum Computer can break today‘s crypto



What algorithms are available to address digital signatures and KEM?

utimaco®

Your choice of algorithms

Key Encapsulation / Encryption

Algorithm	Method	Status	Recommendation
ML-KEM	Lattice-based	NIST Standard published: FIPS-203	ML-KEM-1024 for all classification levels
HQC	Code-based	NIST Selected Algorithm to be Standardized	N/A
Classic McEliece	Code-based	NIST PQC Standardization Round 4	N/A
Bike	Code-based	NIST PQC Standardization Round 4	N/A
Frodo-KEM	Lattice-based	Not standardized Recommended by German Federal Office for Information Security	N/A

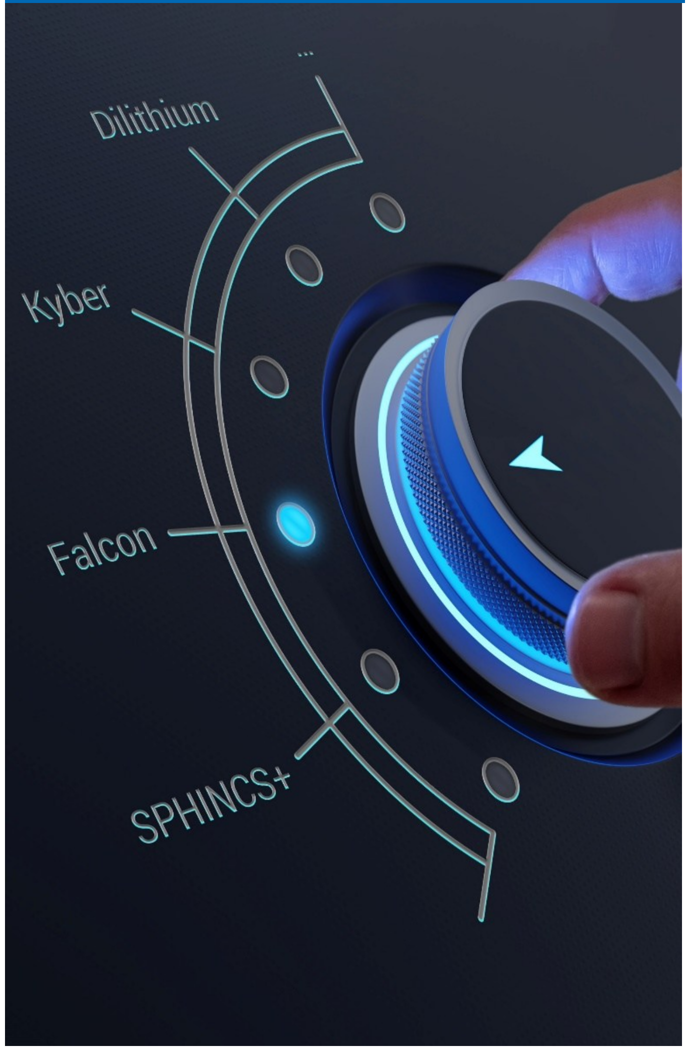
Digital Signatures

Algorithm	Method	Status	Recommendation
ML-DSA	Lattice-based	NIST Standard published: FIPS-204	ML-DSA-87 for all classification levels
SLH-DSA	Hash-based	NIST Standard published: FIPS-205	N/A
FALCON	Lattice-based	NIST Selected Algorithm to be standardized	N/A
LMS / HSS	Stateful Hash-based	Standardized NIST SP 800-208	All parameters approved for all classification levels. LMS SHA256/192 is recommended
XMSS / XMSS-MT	Stateful Hash-based	Standardized NIST SP 800-208	All parameters approved for all classification levels
SHA family	Hash function	Standardized FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels

Take away: There is no magic bullet!
You need to consider which cryptographic use cases you have in your organization and test which PQC algorithm fulfills this use case in your environment. **Most of the algorithms will not be a 1:1 replacement.**

Quantum Computer Age Security – Crypto agility

Crypto agility



Today

Office | ERP | ...

PKCS #11 | CSP | ...

Tomorrow – Crypto agility opportunity

Office | ERP | ...

Crypto API

Crypto Logic

Traditional Crypto

- RSA
- AES
- ECC
- ...

Post Quantum

- Dilithium
- Kyber
- Falcon
- SPHINCS+
- AES
- ...

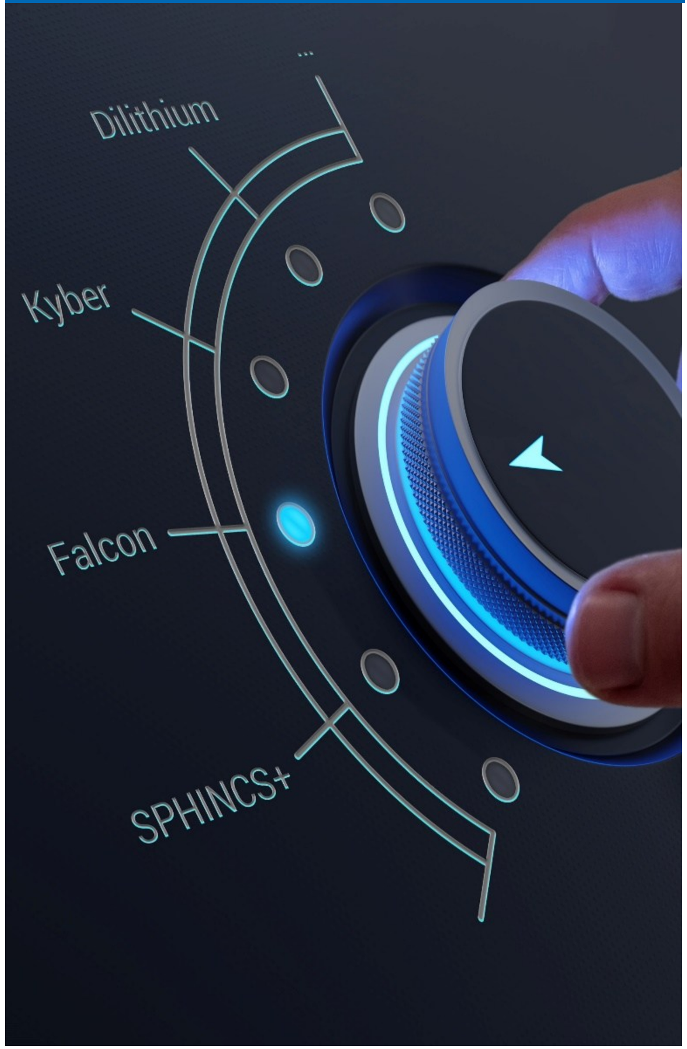
HSM

Crypto Agility:

- Much **more frequent change of crypto algorithms** in future expected
- Intelligent new crypto API allows to **change crypto algorithm without changing applications**

utimaco®

Crypto agility



Different Key Lengths

100100101101001010100100101101001010100100101101001010
100100101101001010100100101101001010
100100101101001010

5 10 15 20 25 30 35 40 45 50 55

Different Algorithms

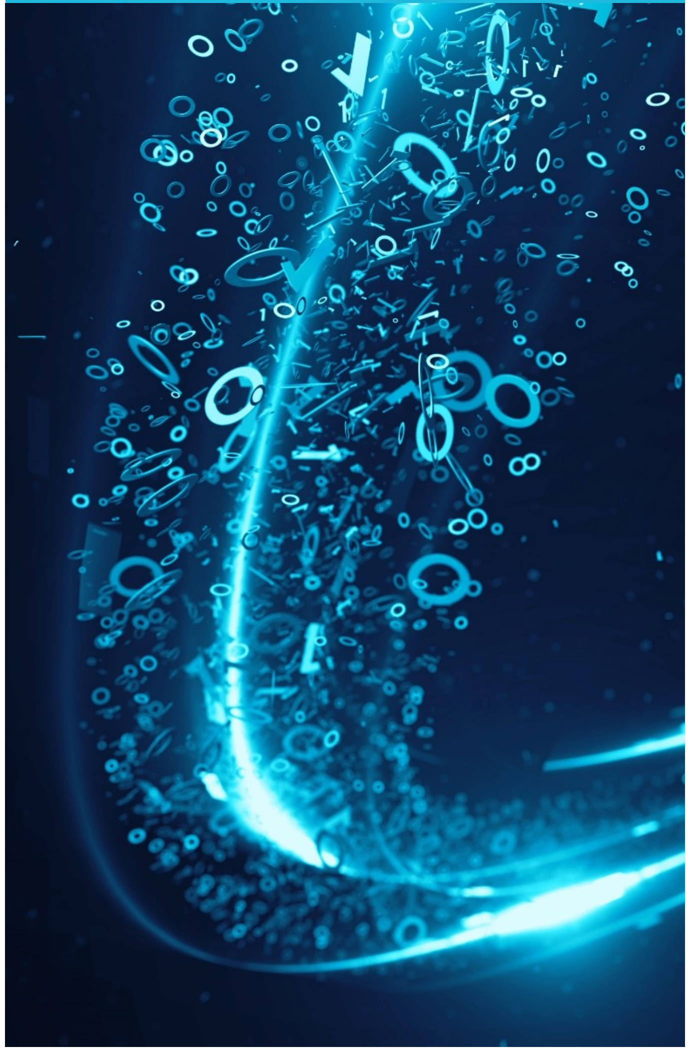
Digital Signature	Dilithium	Falcon	SPHINCS+	...
KEM	Kyber			

Flexible Interface

- Variable parameters
- Different message sizes
- Fields for additional information

Quantum Computer Age Security – Quantum randomness

Quantum randomness



Software Random Number Generator

- Randomness created **by software**
- Often **pseudo random**

Partly HSM implementation opportunity

Hardware Random Number Generator

- Randomness created by atomic/ subatomic **physical phenomenon**
- Can be **true random generators**
- **Examples:** radioactive decay, thermal noise

Quantum Random Number Generator

- Randomness created by measuring **quantum phenomenon**
- Special case of **true random number generators**
- **Examples:** entangled photons

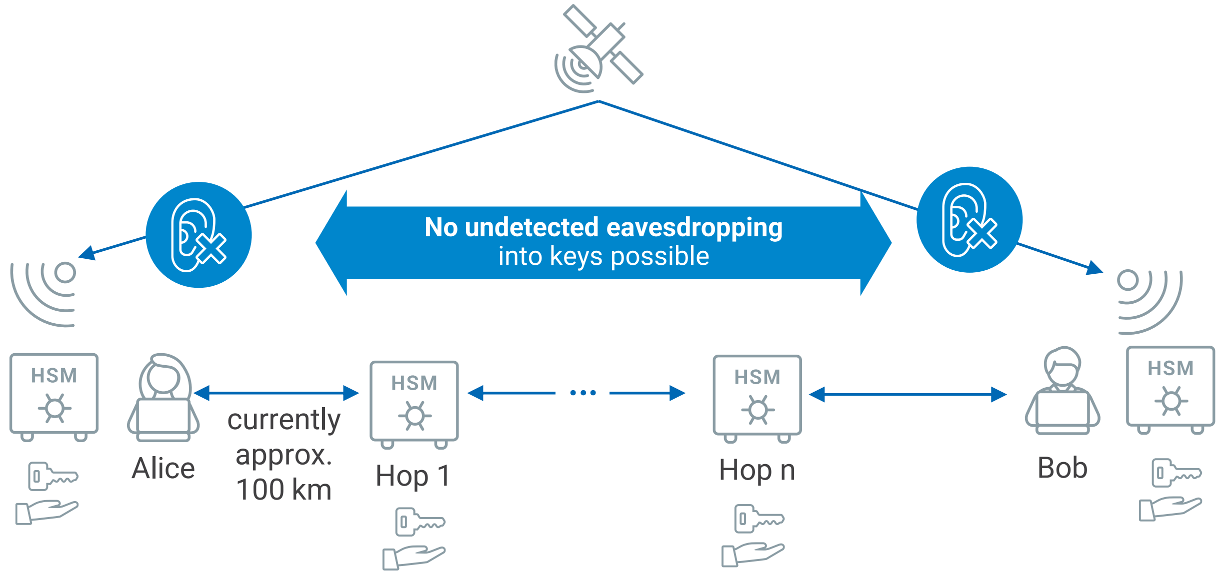
HSM implementation opportunity

HSM

Quantum Computer Age Security – Quantum Key Distribution

Quantum Key Distribution

QKD Use Case



Solutions

Highly Secure Key Generation

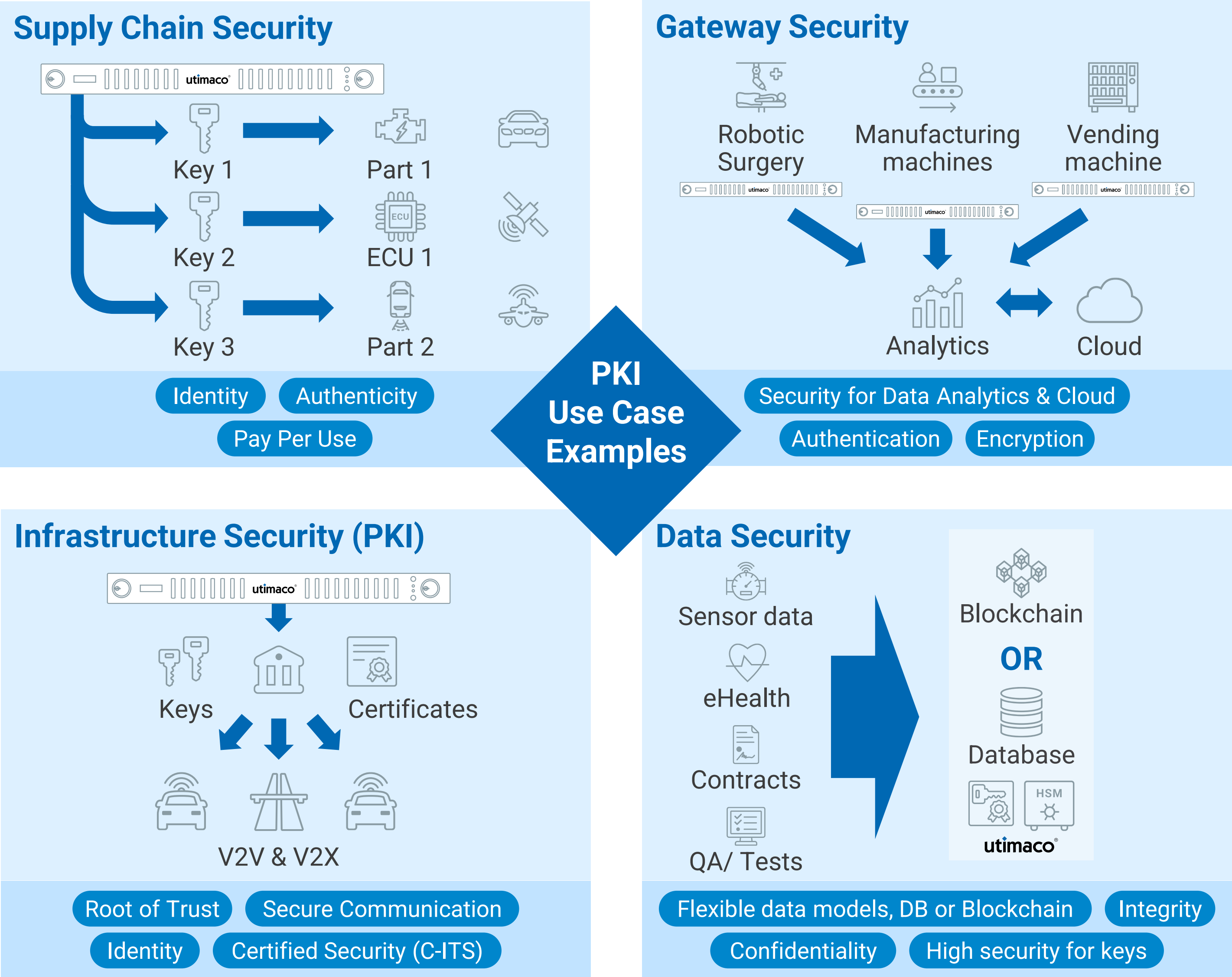
- Randomness by **entangled photons**
- Source must **not be trusted**
- **Eavesdropping** can be **detected**
- Longer **transmission distances when send from satellite**

System set up

- Due to limited transmission distances, **HSMs and Key Management Systems for endpoints** and transmission needed

Agenda

Another example where PQC is critical – PKI/ Certificates



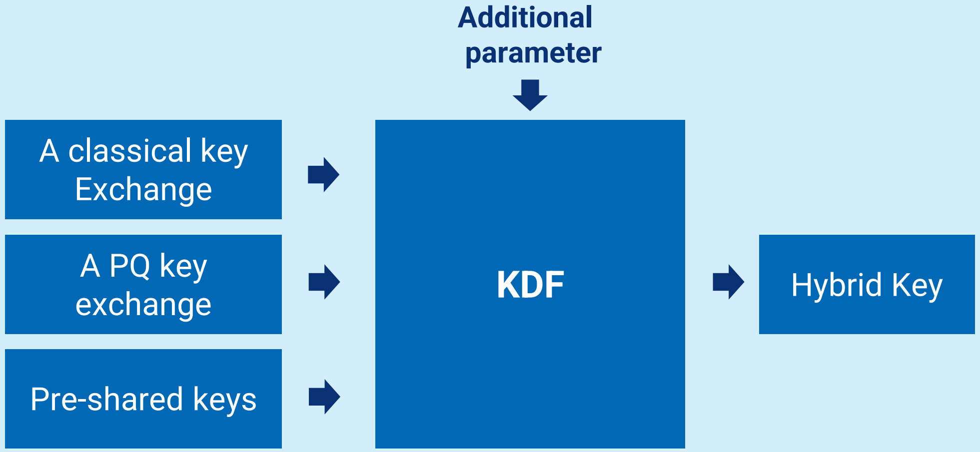
Hybrid Algorithms – Combine PQC and classical crypto algorithms

Definition of hybrid methods

- Hybrid use of cryptography allows to combine classical and PQC algorithms
- Can be used for deriving hybrid keys or digital signatures
- Should either of the two algorithms show weaknesses, there is still the other algorithm to rely upon

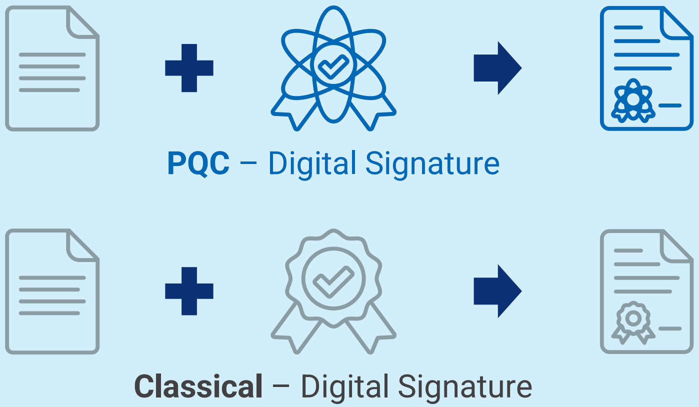
Method 1

- Execution of classical and post quantum key exchange (or use of pre-shared secrets
- Combination of both results in Key Derivation Function (KDF)



Method 2

- For signature schemes, signatures can be concatenated and both signatures need to be valid



Agenda

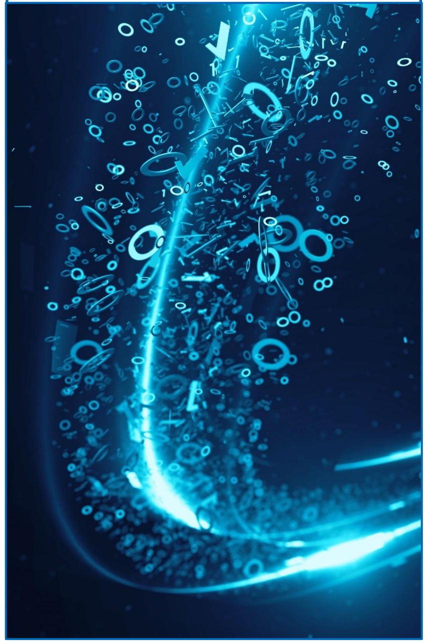
Summary: Utimaco to position in 7 areas to address Quantum Computer Age Security holistically

utimaco®

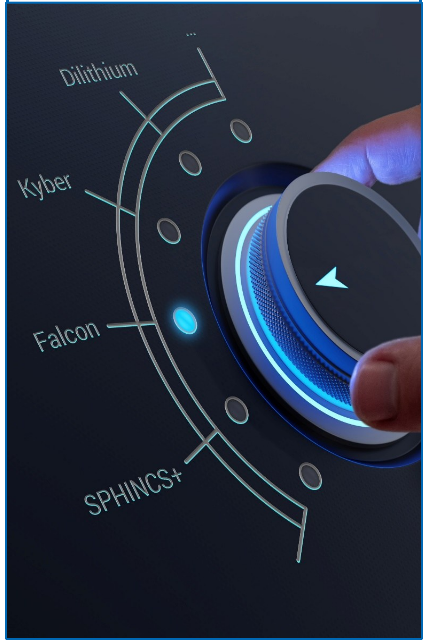
1 Post Quantum Cryptography

2 Quantum Key Distribution

3 Quantum Entropy



4 Crypto Agility



5 Hybrid Use of Algorithms

6 Research Co-operations, Funded projects, Standardization

7 Consultancy/ migration support

Research projects with Utimaco involvement – building out infrastructure, know how and brand

		Project	Utimaco share	Status
QKD	**Q-Fiber & Q-net-Q**	• German wide QKD network via satellite • Prevent side channel attacks	• Secure processing of keys in HSM	• Waiting for approval
	ISQKMS	• Development of Quantum Key Mgt. System	• Secure processing of keys in HSM	• Running
	QCNTF	• QKD network specification for Singapore	• Utimaco specifying key mgt. layer	• Completed
PQC	**QRCrypto**	• PQC systems for different industries (e.g. space,	• HSM/ Key Mgt. support for various use cases	• Application in finalization

Agenda

Industry Organizations and Standardization

Shaping Tomorrow's Cryptographic World

NIST	Accredited Standards Committee X9 Inc. – Financial Industry Standards	ETSI	Bundesamt für Sicherheit in der Informationstechnik
PQC Consortium: Work Streams Interoperability, Discovery	X9 Post Quantum Cryptography Committee	ETSI Quantum-Safe Cryptography (QSC) Working Group	Federal Office for Information Security in Germany
GSMA	PKI Consortium	The White House, Washington	enisa, ITU, bitkom
PQC Working Groups	PQC Consortium: PQC Workstream	White House Roundtable, January 2024	And further

Playing a key role in shaping the future landscape of Post Quantum Cryptography

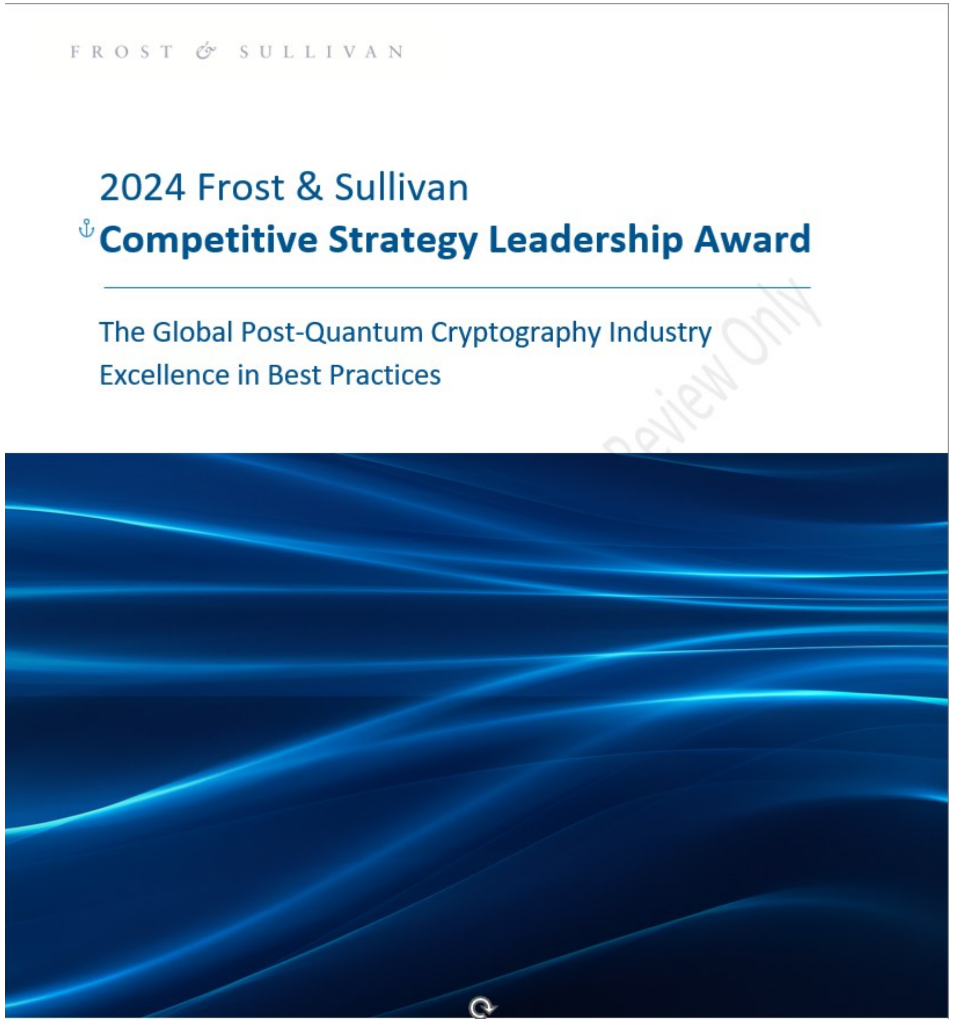
White House Roundtable on PQC, August 2024

ICMC, *September 2023*

Post-Quantum Cryptography Conference, *November 2023*

Utimaco awarded as Best Practice in PQC

utimaco®


FROST & SULLIVAN

2024 Frost & Sullivan
Competitive Strategy Leadership Award

The Global Post-Quantum Cryptography Industry
Excellence in Best Practices

Review Only

FROST & SULLIVAN
BEST PRACTICES
AWARDS

"Utimaco's expertise in deploying HSMs both for general purpose and specialized use cases translates well to the post-quantum era, which requires high levels of customization and adaptability. An integral part of the migration to PQC as a supplier of roots of trust, Utimaco also strategically positions itself as a wide-ranging partner for organizations in this monumental task, providing consultancy services, quantum-readiness assessments, and crypto-agility solutions."

- Özgün Pelite, Sr. Industry Analyst

Agenda

RSA-2048 is only considered secure until 2030.

(guidance in NIST SP 800-78-5)

NIST IR 8547 Transition to PQC Standards

(Published November 2024)

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Regulatory Initiatives Around the World on PQC

utimaco®

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	ACSC-2023 ACSC-2024	Start planning for transition to quantum resistant cryprography.
Canada	NIST	CAN-01 CAN-02	Start planning, wait for standards. CSE is updating detailed PQC guidance.
China	China Specific	CAICT-2023	Start Planning
Czech Republic	NIST (but not restricted to)	NÚKIB-2023	Migrate by 2027 (key establishment, encryption). As soon as possible for firmware & software signing.
European Union	NIST Plan to select PQC EU algorithms	ENISA-2022 EC-2024	Start planning Define a coordinated PQC roadmap for Member States by 2026
France	NIST (but not restricted to)	ANSSI (2022, 2023)	Start planning; Transition from 2024
Germany	NIST (but not restricted to)	BSI-2021 BSI-2023 BSI-2024	Start planning
Italy	NIST	CAN-2024	
Japan	Monitoring NIST	JAPAN-2022	Start planning; initial timeline. CRYPTREC is preparing detailed PQC guidelines.
Netherlands	ML-KEM, Classic McEliece and FrodoKEM recommended in hybrid mode for TLS.	NL-2022 AIVD-2023 NL-2024	Draft action plan with timeframes
New Zealand	NIST	NZISM-2024	Start planning. Transition from 2026-27.
Singapore	Monitoring NIST	SG-2022 MAS-2024	No timeline available. Financial services firms required to prepare plan.
South Korea	KpqC	MSIT (2022) MSIT (2024)	Start competition First round (Nov.'22-Nov.'23). PQC Roadmap published
Spain	NIST and FrodoKEM.	CCN.ES-2022	Four phase approach today to post-2030.
United Kingdom	NIST	NCSC-2024a NCSC-2024b	Start planning; use only standards in production. NCSC is preparing detailed PQC guidance.
United States	NIST	NSM-10 CISA-2021 CNSA20 HR7375 CISA-2023 CISA-2024	Implement 2023-2033

*https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/

The CNSA 2.0 Algorithm Suite

CNSA 2.0 Requirements and Timeline

Software and firmware signing

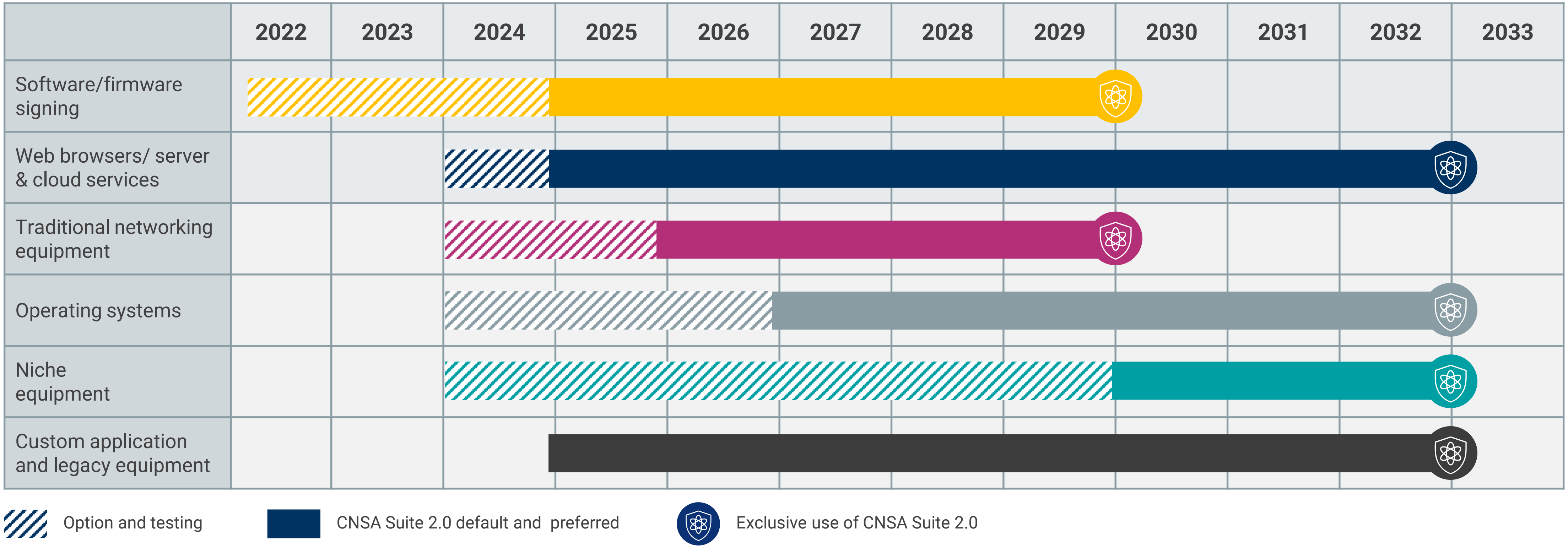
- LMS
- XMSS

General quantum-resistant public key algorithms

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

Symmetric key algorithms

- AES
- SHA



Agenda

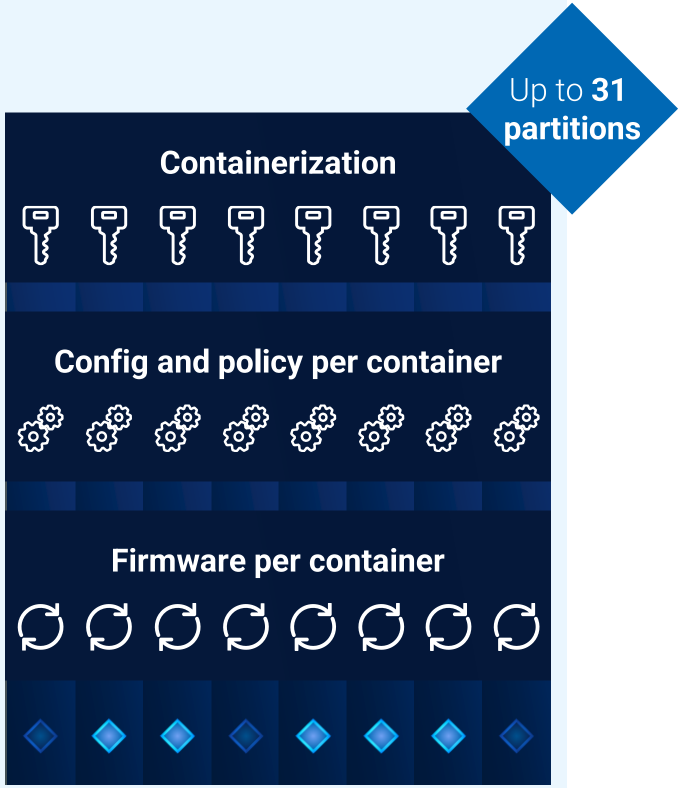
u.trust General Purpose HSM Se-Series

The Cloud-inspired, Next Generation HSM

Superior Performance ◆ Multi-Tenant ◆ PQC-ready ◆ FIPS-certified ◆ SDK ◆ Free Simulator

- Up to 40,000 RSA 2K operation / s
- Multi-tenancy with up to 31 containers
- Designed crypto agile
- FIPS 140-2 Level 3 certified (FIPS 140-3 in progress)
- SDK for custom implementations
- Free, fully functional simulator

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



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 Update coming soon!

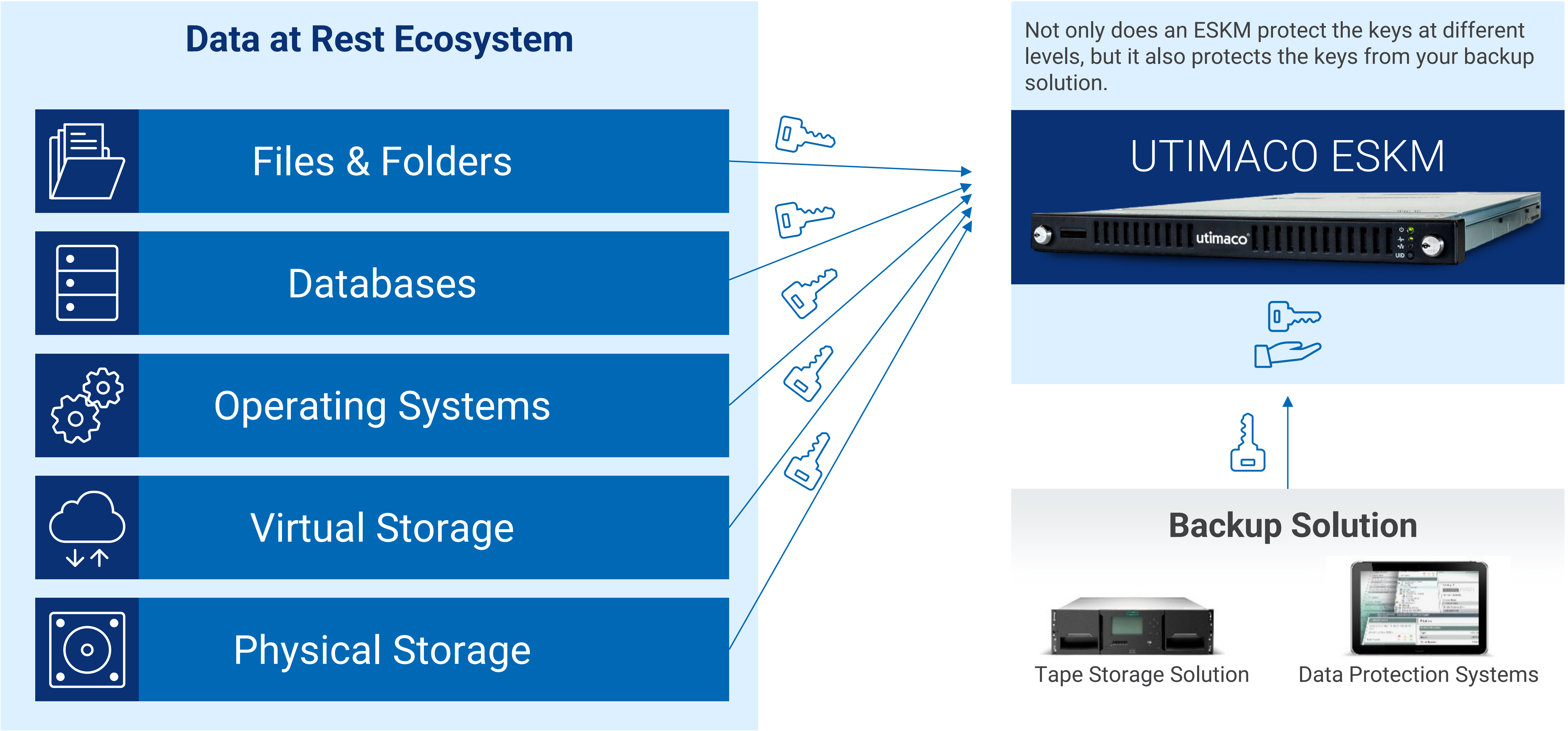
Utimaco PQC Algorithm Suite

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

ESKM Secures the Keys at Different Levels AND Secures the Backup

Securing the Access to Data and Information at Different Levels



UTIMACO ESKM – Product Overview

utimaco®

Key Manager with broad integration portfolio

Secure

- Meet NIST standards, validated to **FIPS 140-2 Level 1-4, Common Criteria**
- Encrypts keys in transit and at-rest
- Certificate-based authentication and built-in CA

Interoperable

- **Support OASIS KMIP** (Key Management Interoperability Protocol)
- Support RESTful interface
- No vendor lock-in
- Custom integrations using SDK

Available

- **Active-Active** cluster with thousands of nodes
- **Automatic key replication**, client failover
- **Highly redundant** hardware

Scalable

- Geographically **separated clusters** across datacenters
- Supports thousands of clients, and **millions of keys**

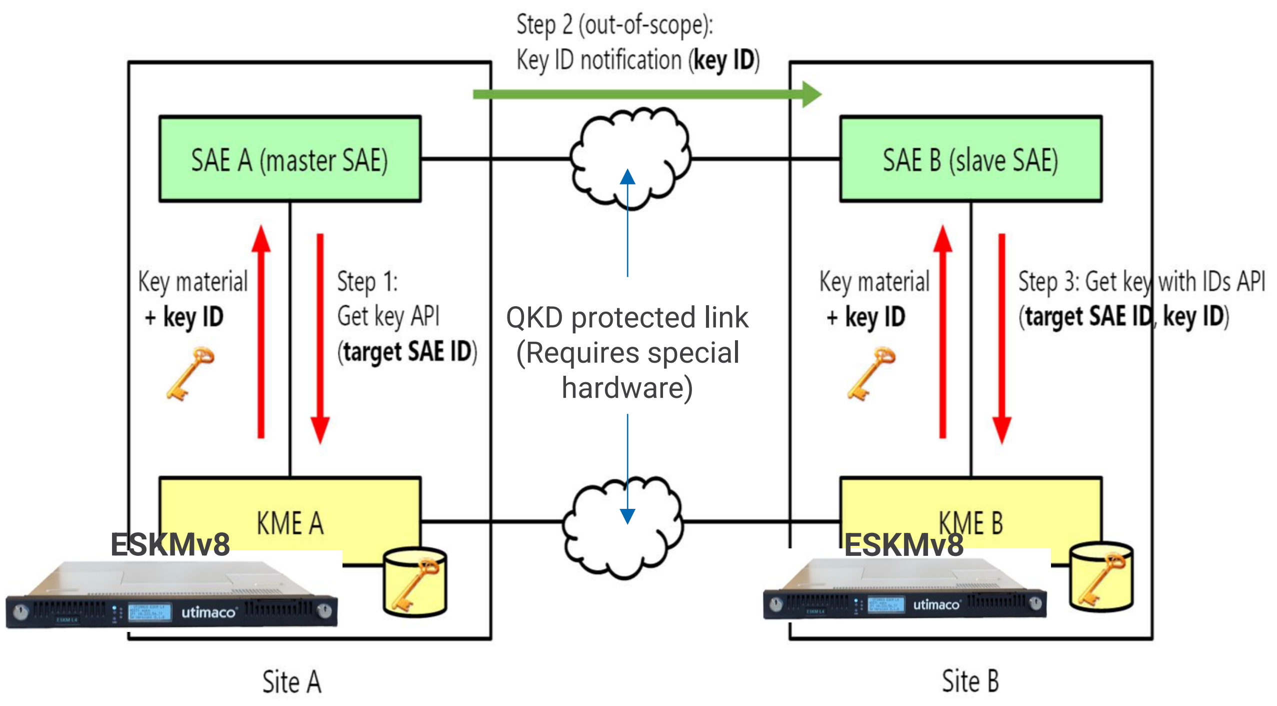
Managable

- Configuration and keys replicated across cluster automatically
- **Hands-off adminis-tration**, automated backups and audit logging

ESKM – QKD Integration

utimaco®

Quantum Key Distribution (QKD)



Advanced REST Settings

Enable ETSI QKD 14:	☑
ETSI QKD 14 Port:	7443
ETSI QKD 14 CA:	Local: ESKMCA

- ETSI GS QKD 014 V1.1.1 (2019-02) titled "**Quantum Key Distribution (QKD) Protocol and data format of REST-based key delivery API**"
  - Three API commands
    - Get Status
    - Get Key
    - Get Key IDs
  - API Data format for those 3 API commands
- These REST APIs enable an SAE to request & get keys from a KME within THE SAME Trusted Node (TN)

Agenda

utimaco®

Securing Satellite Communication with XMSS and Kyber

Use Case: Digital Signatures to Secure Satellite Communication

Quantum-proof digital signatures and encryption for long-term secure satellite communication

Project: Securing **Satellite Communication**

➡ Providing fast, affordable broadband to unserved and underserved communities around the world

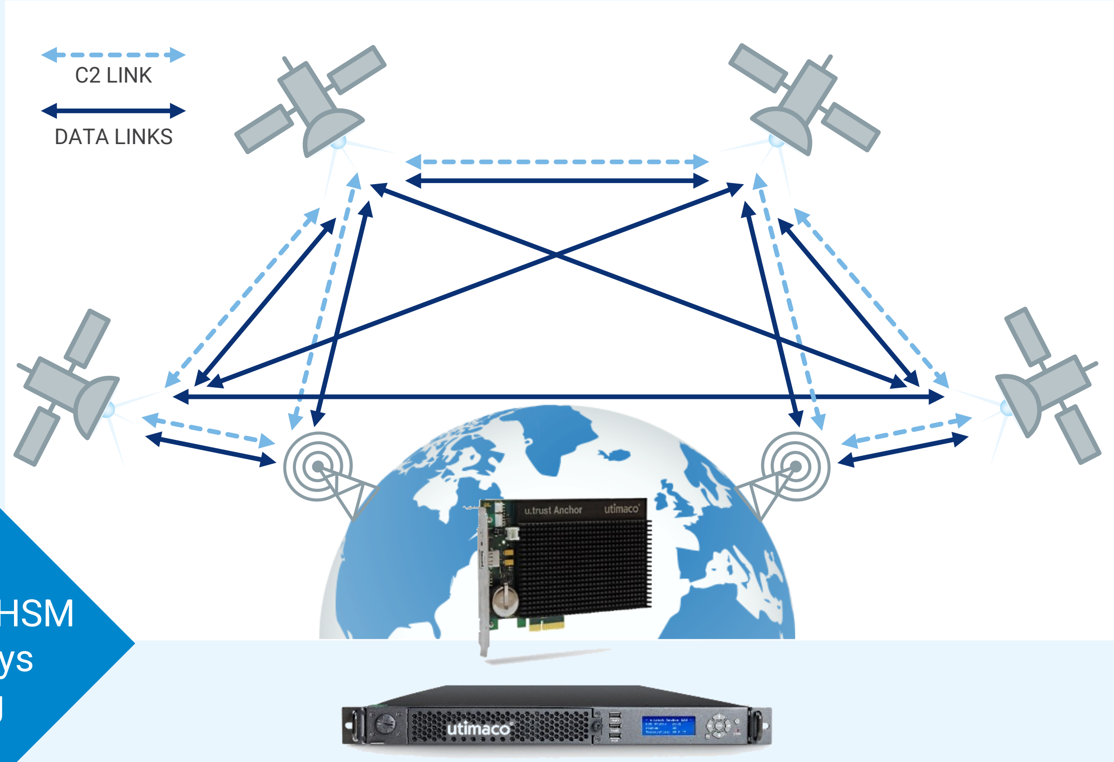
CCSDS Space Data Link Security Protocol
requires cryptographic algorithms for

- Authentication
- Encryption
- Authenticated encryption

Algorithms and methods used

- XMSS incl. state handling (signatures)
- CRYSTALS-Kyber (key encapsulation mechanism)

Keys are generated in the HSM with private keys never leaving the HSM



Solution:
u.trust General Purpose HSM Se-Series upgraded with Quantum Protect + SDK

Secure Updates for Embedded Devices

Use Case: Key Injection for Long-term Secure Firmware Updates

Securing firmware updates for Chips using PQC

Algorithms

- CRYSTALS-Dilithium (signatures)
- CRYSTALS-Kyber (encryption)

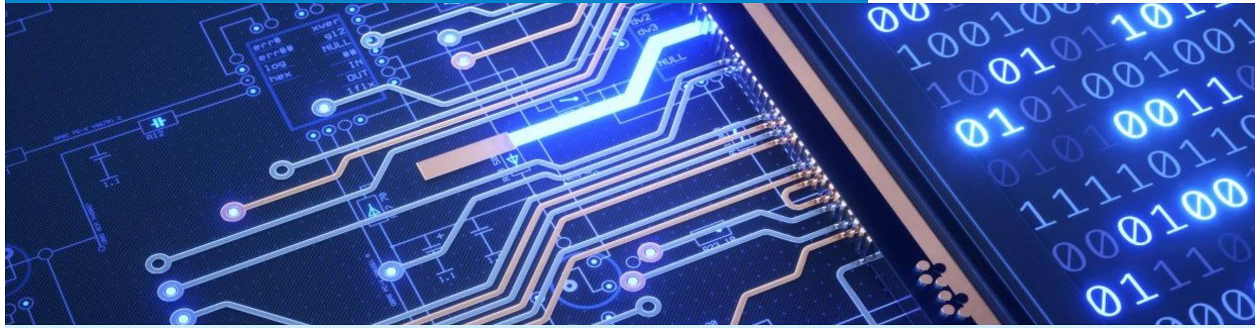
Methods used

- Generation of CRYSTALS-Dilithium key pair in the HSM
- Cryptographic key injection (Public Dilithium key) during chip manufacturing
- Signature verification in the field
- Confidentiality achieved by encrypting with CRYSTALS-Kyber

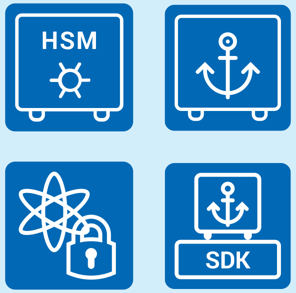
Challenges solved

- Memory space on the chips
- Protection against side channel attacks

Customer:
NXP Semiconductor industry
World leader in secure connectivity solutions for embedded applications



Solution: Utimaco u.trust General Purpose HSM Se-Series upgraded with **PQC algorithms** + **SDK** for custom firmware



Thank you

for your attention!

UTIMACO GmbH

Germanusstraße 4
52080 Aachen
Germany

Phone +49 241 1696-0
Web https://hsm.utimaco.com
E-Mail hsm@utimaco.com

UTIMACO Inc.

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

Phone +1 (844) UTI-MACO
Web https://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.