Post-Quantum

Cryptography Conference

2025 is Here - How to get your PQC Readiness Plan Underway

2024 saw NIST's milestone release of the first certified PQC algorithms. As 2025 begins, it is more urgent than ever to "get your house in order" with Quantum Readiness. We will discuss these current & future risks and outline how to effectively counter against evolving threats with strategic and tactical steps within a PQC readiness plan. This session will also identify some of the industry challenges affecting today's PKI, IoT, TLS & Code Signing. To conclude, strategies will be presented citing real-world examples including PQC code signing that specifically describe ecosystem collaboration and testing within critical enterprise applications and infrastructure.

Blair Canavan
Director, Alliances - PQC Portfolio at Thales

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

THALES

Building a future we can all trust

2025 is Here!

How to get your PQC Readiness Plan Underway

January 15, 2025
Austin, TX

Blair Canavan
Director, Alliances, PQC Portfolio

https://cpl.thalesgroup.com/

PKI Consortium

THALES

Building a future we can all trust

PQC-Worthy Jokes:

A man calls quantum IT support and complains that his quantum computer isn't working.

A Qubit walks into two bars at the same time.........

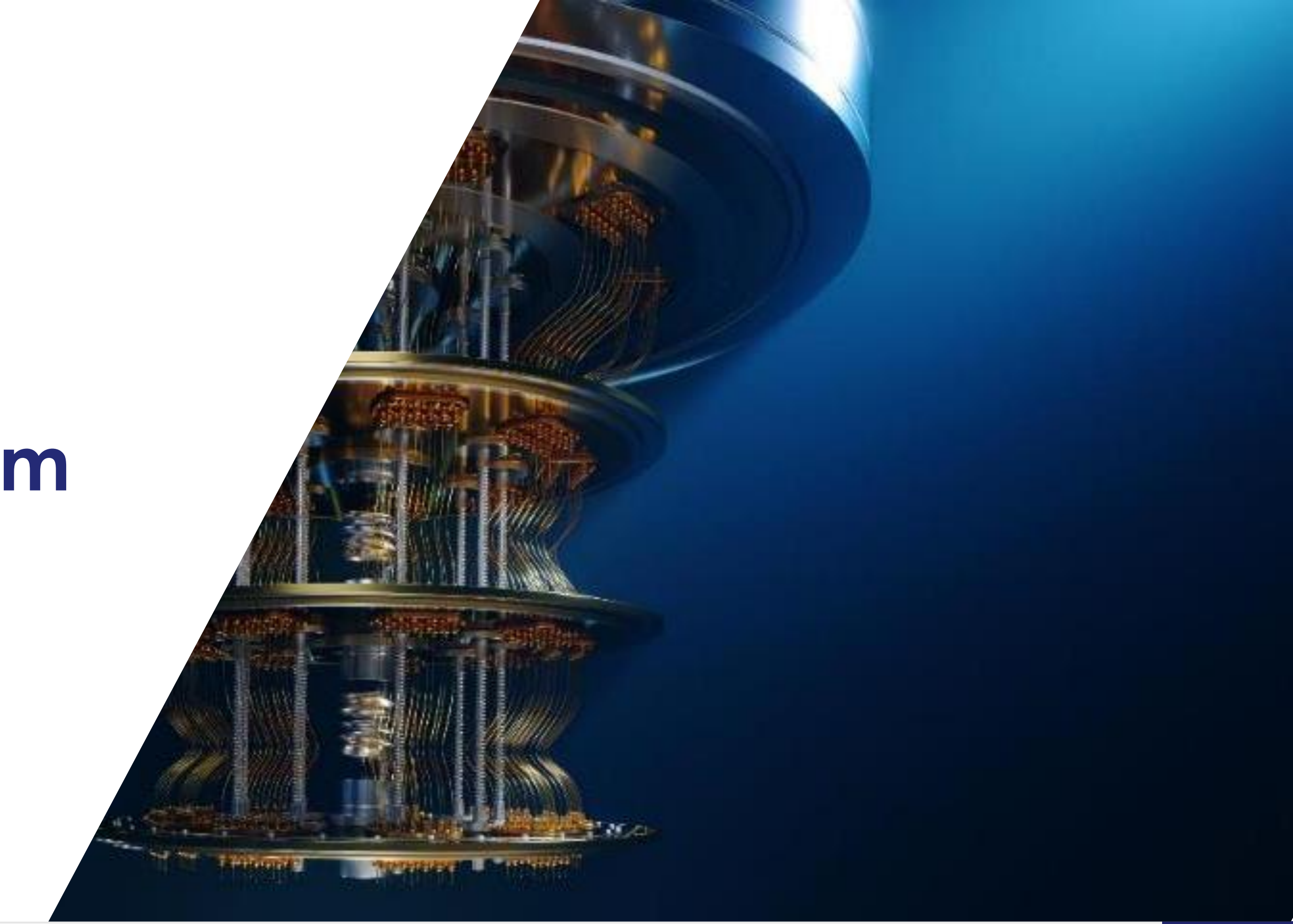
Quantum IT support:

"Have you tried turning it off and on at the same time?"

TODAY'S AGENDA

1. The problem
2. Areas of risk
3. Industry challenges
4. The Path to Success
5. Key Take-aways

The Problem



SIMPLY SAID

Without quantum-resistant encryption, **everything** that has been transmitted, or will ever be transmitted over a network, **will be vulnerable** to eavesdropping and public disclosure.

—ETSI White Paper No. 8 Quantum Safe Cryptography and Security

Beyond algorithms, threat impacts

OVERALL ECOSYSTEM

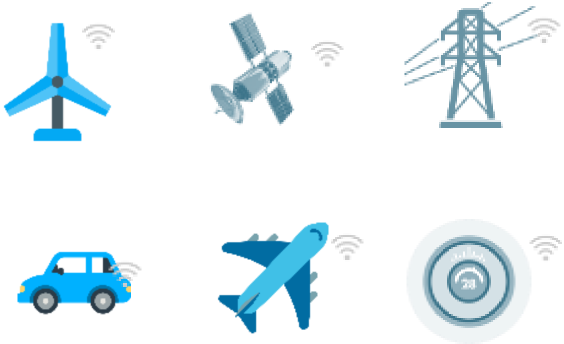
- **Communication protocols**
  (TLS, IPSec, SSH, …)
- **Certificates** (X.509)
  (Identities, Code Signing, Doc Signing)
- **Key management protocols**
  (KMIP, IKE)

Areas of Risk

Area of high risk: Authenticated Software

What’s at risk?

Durable connected devices (IoT) with **long in-field lives**



What’s the attack?

Forged software updates by quantum-enabled adversaries

Areas of high risk

FORGED SIGNATURES

Impersonate entities

Load malicious SW/FW on long life devices

Create fraudulent financial transactions

Redirect funds

MAN IN THE MIDDLE ATTACKS

Access secure systems

Compromise military command and control

Disrupt critical infrastructure

Interfere with elections

HARVEST NOW, DECRYPT LATER

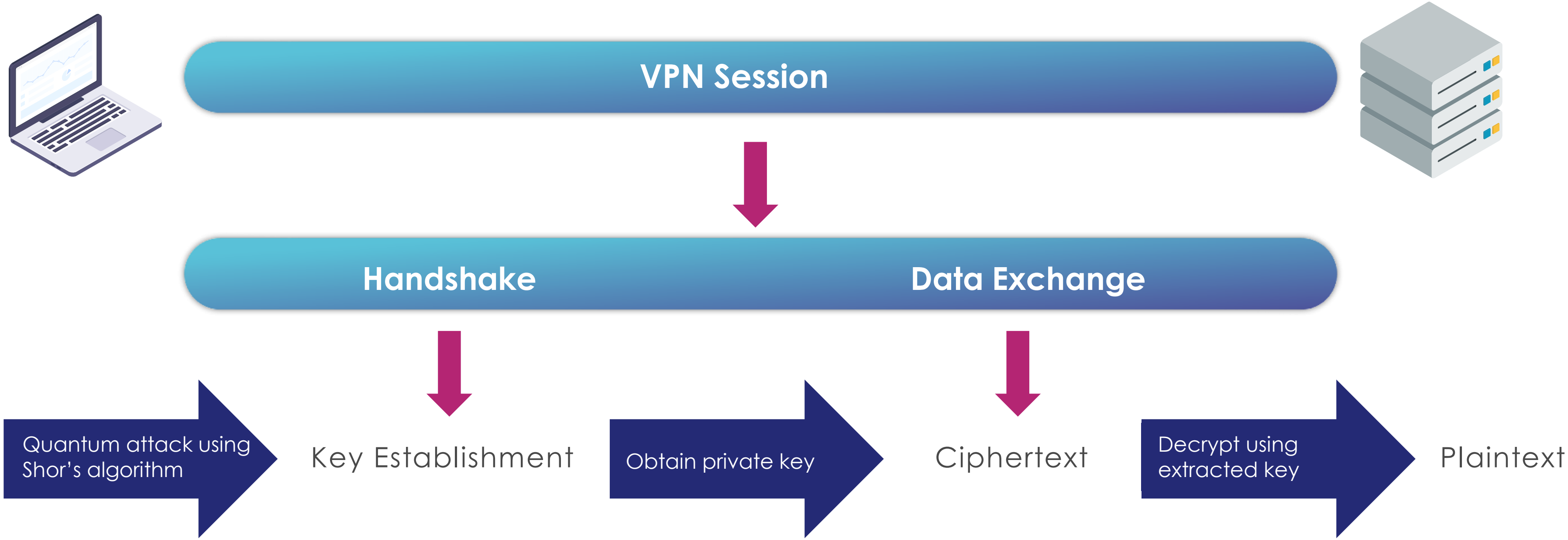
Intercept classified comms

Expose government secrets

Perform corporate espionage

Access personal information

Area of high risk: Confidential Communications



VPN Session

Handshake

Data Exchange

Quantum attack using Shor's algorithm

Key Establishment

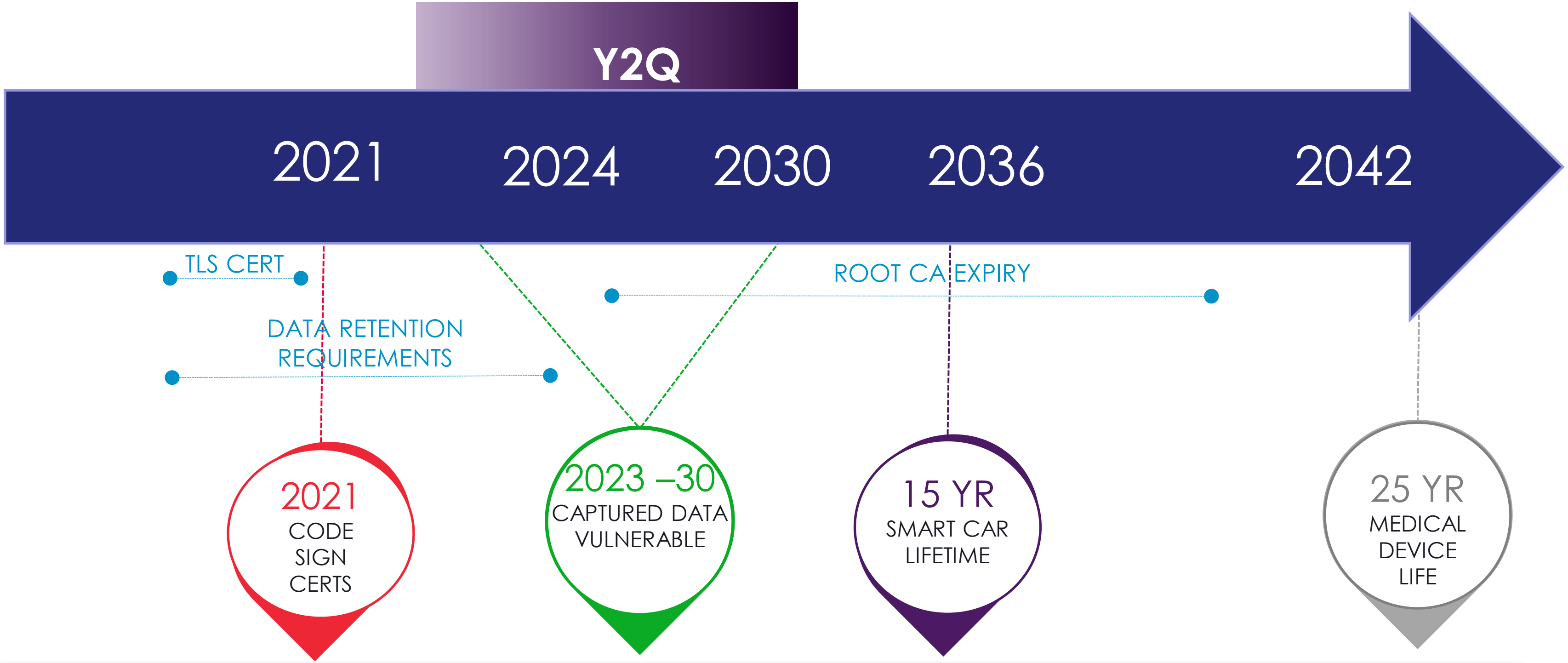
Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext

Areas of high risk: Keys or Data with a long life



Hackers are already using a Harvest Now, Decrypt Later strategy in preparation for quantum attacks.

Across the globe, regulatory bodies recommend to prepare for PQC now

ANSSI recommends introducing **post-quantum defense-in-depth as soon as possible** for security products aimed at offering a long-lasting protection of information (until after 2030) or that will potentially be used after 2030 without updates.

CISA, NSA, and NIST **urge organizations to begin preparing now** by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors.

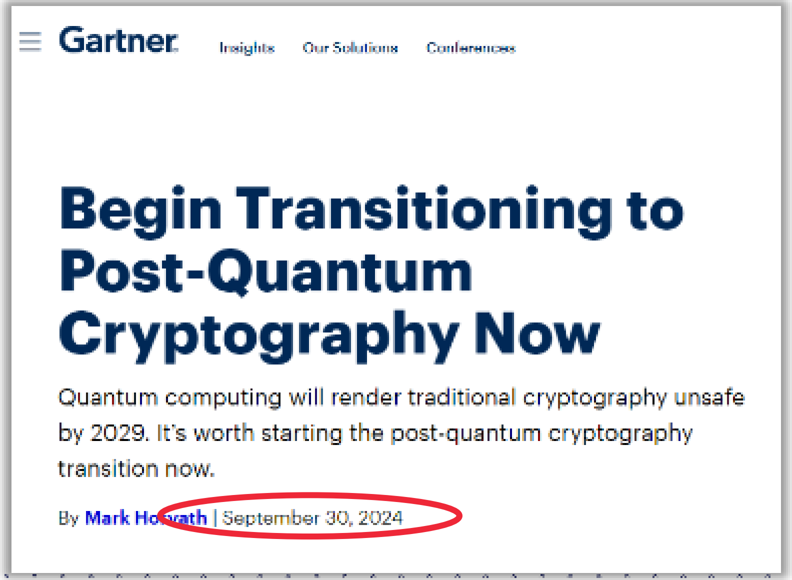
For MAS, the goal is developing strategies and building capabilities to address cybersecurity **risks associated with quantum as soon as possible.**

From the BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer paramount. First post-quantum algorithms have been selected by NIST for standardisation **and post-quantum cryptography will be used by default.**

Industry Challenges

Countdown is on!

> Gartner brings forward Q-DAY



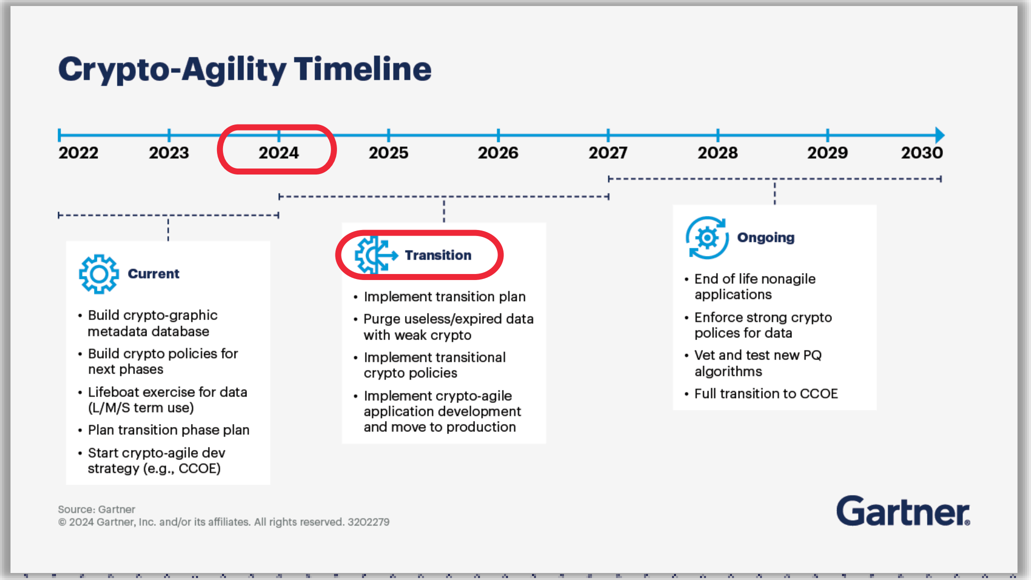
Gartner Insights Our Solutions Conferences

Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By Mark Horvath | September 30, 2024

> Start transition to PQC now



Crypto-Agility Timeline

2022 2023 2024 2025 2026 2027 2028 2029 2030

Current

- Build crypto-graphic metadata database
- Build crypto policies for next phases
- Lifeboat exercise for data (L/M/S term use)
- Plan transition phase plan
- Start crypto-agile dev strategy (e.g., CCOE)

Transition

- Implement transition plan
- Purge useless/expired data with weak crypto
- Implement transitional crypto policies
- Implement crypto-agile application development and move to production

Ongoing

- End of life nonagile applications
- Enforce strong crypto polices for data
- Vet and test new PQ algorithms
- Full transition to CCOE

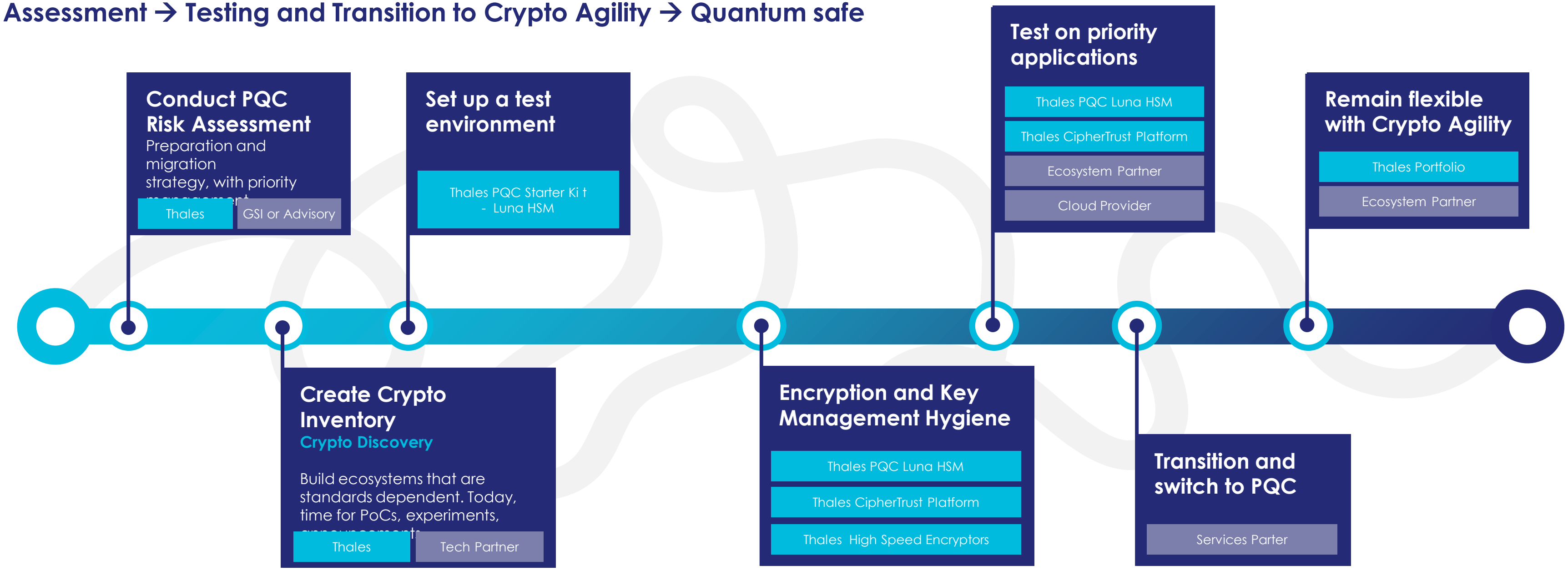
Source: Gartner
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. 3202279

Gartner

THALES
Building a future we can all trust

PQC: Simplifying a complex journey

Assessment → Testing and Transition to Crypto Agility → Quantum safe



Conduct PQC Risk Assessment

Preparation and migration strategy, with priority management

Thales | GSI or Advisory

Create Crypto Inventory

Crypto Discovery

Build ecosystems that are standards dependent. Today, time for PoCs, experiments, announcements

Thales | Tech Partner

Set up a test environment

Thales PQC Starter Ki t - Luna HSM

Encryption and Key Management Hygiene

- Thales PQC Luna HSM
- Thales CipherTrust Platform
- Thales High Speed Encryptors

Test on priority applications

- Thales PQC Luna HSM
- Thales CipherTrust Platform
- Ecosystem Partner
- Cloud Provider

Transition and switch to PQC

Services Parter

Remain flexible with Crypto Agility

- Thales Portfolio
- Ecosystem Partner

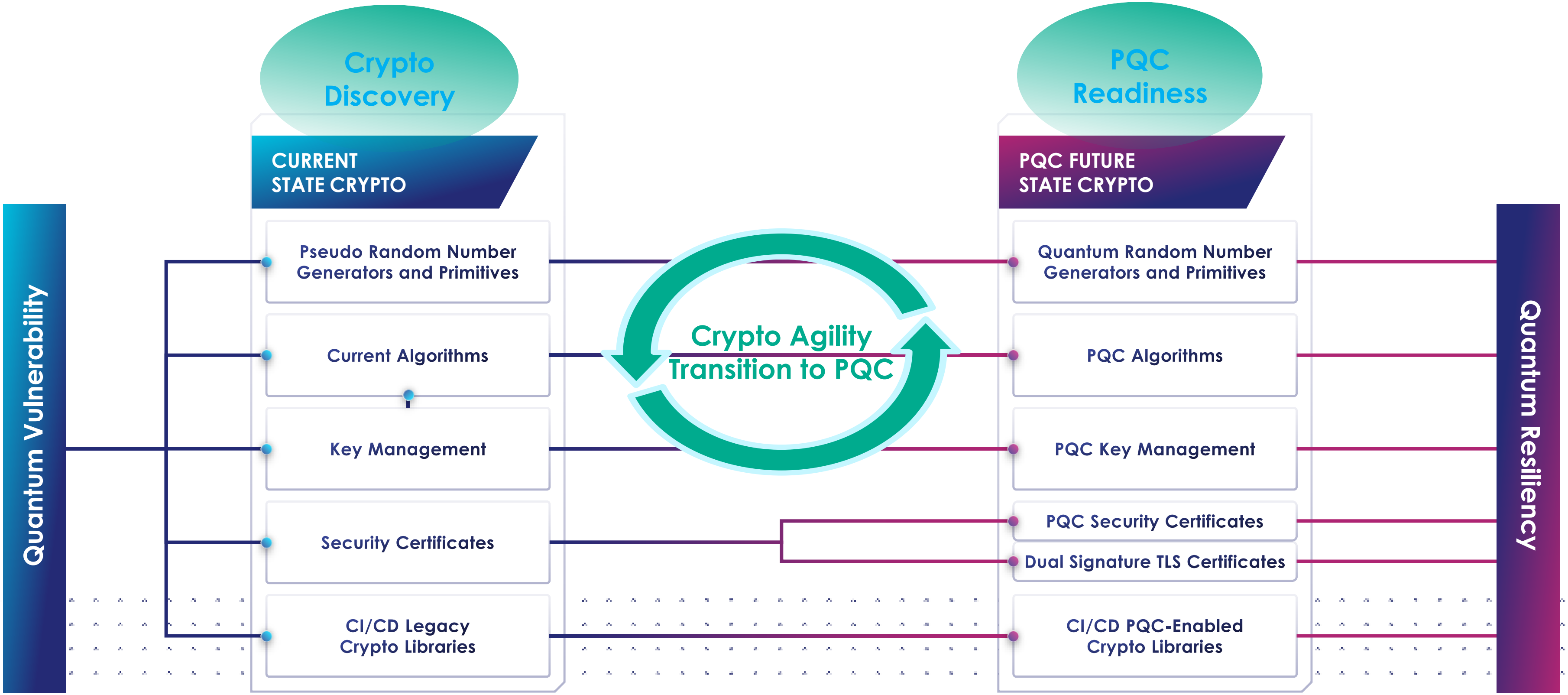
Go Hybrid
Classic & Quantum crypto
Support classic and Qsafe Algorithm modes

Build ecosystem
Changing algorithms, protocols, key can be costly, complex,
time-consuming & needs multiple players

Evolve with the standards
NIST-certified Random Number Generators
As Standards are approved, implement and re-certify

Thales has solutions and partnerships in place today to support your quantum safe journey

PQC Challenges in Real Time



Crypto Discovery

CURRENT STATE CRYPTO

Pseudo Random Number Generators and Primitives

Current Algorithms

Key Management

Security Certificates

CI/CD Legacy Crypto Libraries

Quantum Vulnerability

Crypto Agility Transition to PQC

PQC Readiness

PQC FUTURE STATE CRYPTO

Quantum Random Number Generators and Primitives

PQC Algorithms

PQC Key Management

PQC Security Certificates

Dual Signature TLS Certificates

CI/CD PQC-Enabled Crypto Libraries

Quantum Resiliency

Challenge #1: Crypto discovery

> Crypto objects

- Discover and register all crypto objects (keys, certs etc)
- Thales: CipherTrust DDC
- Partner: InfoSecGlobal, IBM, etc

> Cloud keys

- Discover and register keys (with attributes and origin) used in multi-clouds
- Thales: CipherTrust CCKM

> Crypto Library

- Discover the crypto library used by applications and APIs
- Thales: Imperva App/API Sec

Challenge #2: Transition to PQC, Crypto Agility

Standards Bodies

NIST

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

IETF

PKI Consortium

ETSI World Class Standards

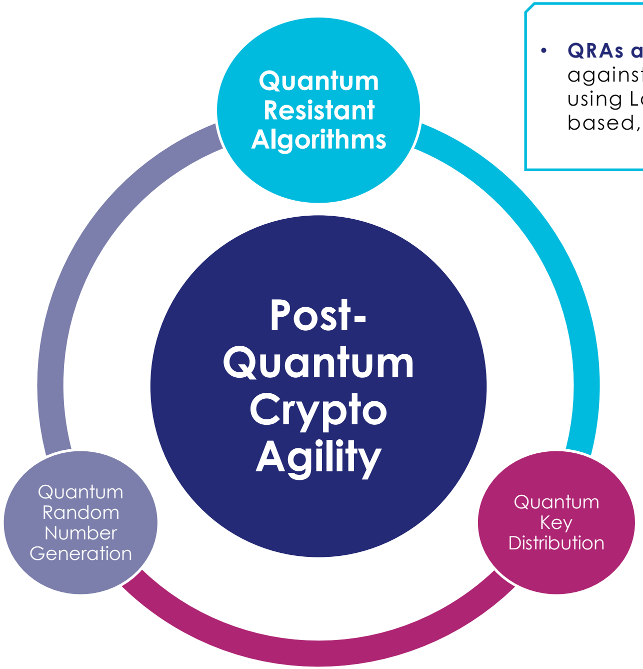
ANSI

Accredited Standards Committee X9 Financial Industry Standards

CA|B CA/BROWSER FORUM

CSA cloud security alliance

FS-ISAC


Quantum Resistant Algorithms
Post-Quantum Crypto Agility
Quantum Random Number Generation
Quantum Key Distribution

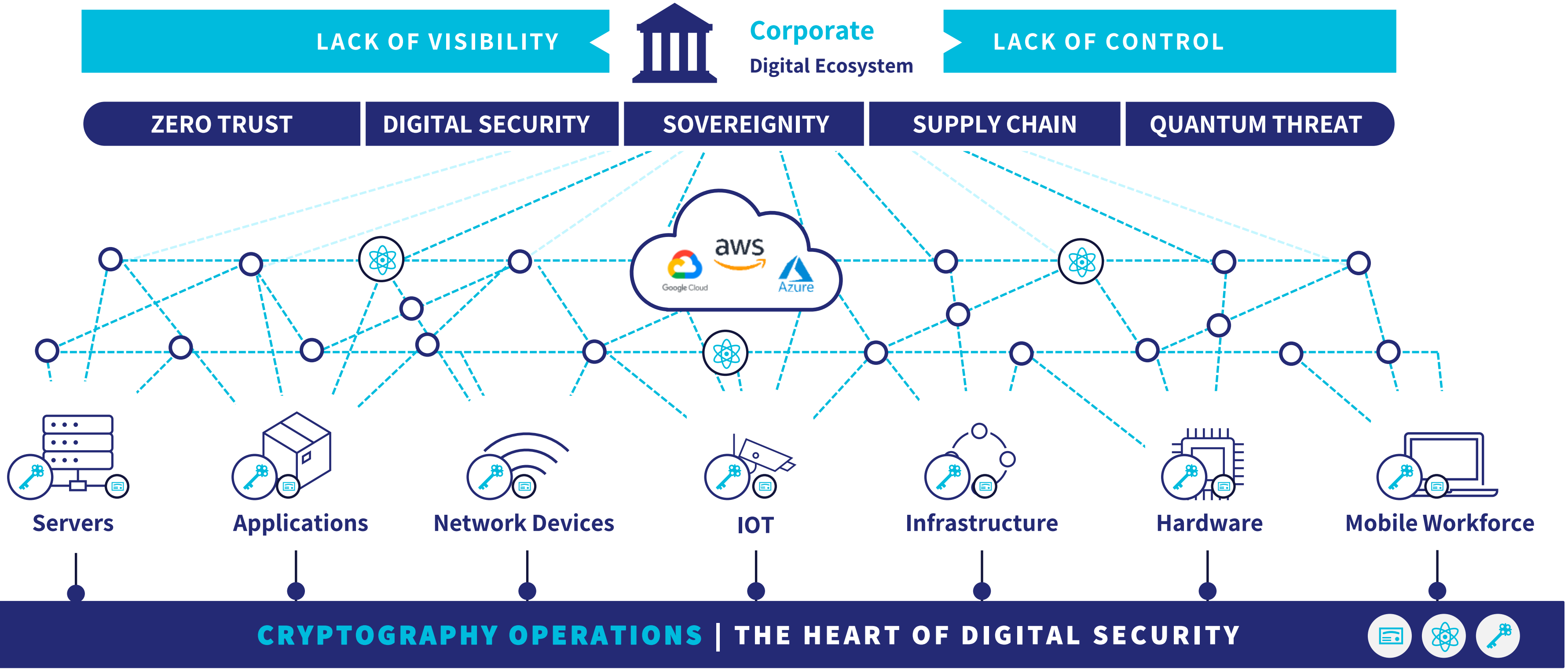
- **QRAs are fundamental** to protecting against quantum attacks whether using Lattice based, Multivariate, Hash based, or Code-based cryptography

QKD distributes encryption keys between shared parties based on the principles of **quantum physics** and the properties of **quantum mechanics**

QRNG is a high bit rate random number source harnessing the **inherent randomness** in quantum mechanics to create encryption keys

The Path to Success

Problem | Cryptography is everywhere



LACK OF VISIBILITY

Corporate
Digital Ecosystem

LACK OF CONTROL

ZERO TRUST | DIGITAL SECURITY | SOVEREIGNITY | SUPPLY CHAIN | QUANTUM THREAT

Servers

Applications

Network Devices

IOT

Infrastructure

Hardware

Mobile Workforce

CRYPTOGRAPHY OPERATIONS | THE HEART OF DIGITAL SECURITY

Certificates & Identities

Keys & Secrets

Ciphers & Algorithms

Libraries & Protocols

THALES
Building a future we can all trust

Use Cases | Discover

1

Cryptographic
Vulnerabilities

Identify and remediate critical cryptographic vulnerabilities hidden in the digital landscape.

2

Cryptographic
Keys in the Wild

Hunt cryptographic keys and secrets across infrastructure to ensure compliance and security.

3

Cryptographic
PQC Migration

Prepare transition to Quantum Safety by monitoring deployment of Post-Quantum Cryptography.

4

Cryptographic
Compliance

Identify breaches of cryptographic compliance based on standards and corporate policies.

5

Cryptographic
Cloud Migration

Understand current uses of cryptography to prepare for transition from on-prem to cloud.

Cryptography Inventory

Inventory | Knowledge is Power

SSH Inventory

- Private SSH Keys
- Public SSH Keys

Keys Inventory

- Private Keys
- Public Keys

Keystores Inventory

- Private Key Stores
- Secrets Managers

Locations

- File System
- Running Process
- Certificate Store
- Network Interface
- Repository

Certificates Inventory

- Root CA
- Intermediate CA
- SSL / TLS
- Personal Certificate
- S/MIME Encryption
- Digital Signing
- Time Stamping

Crypto Libs Inventory

- Classical Libraries
- PQC Ready Libraries

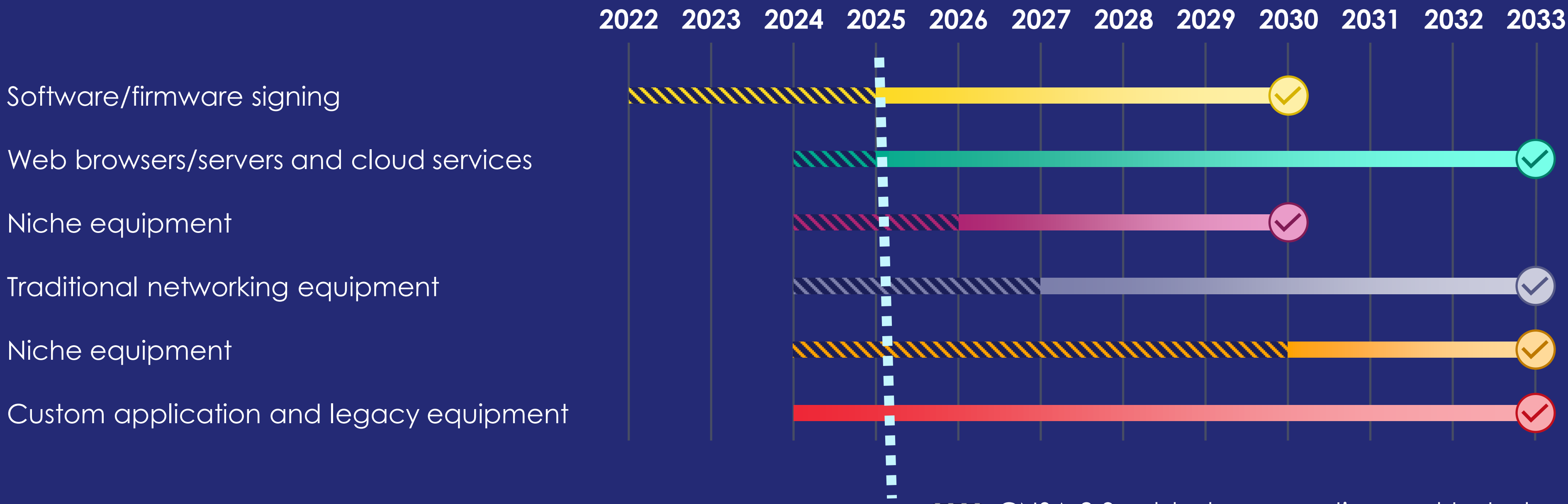
Algorithms Inventory

- Classical Algorithms
- Post-Quantum Algorithms

Ciphers & Protocols Inventory

- TLS/Crypto Protocols
- Cipher Suites

Understanding implementation timelines by industry type



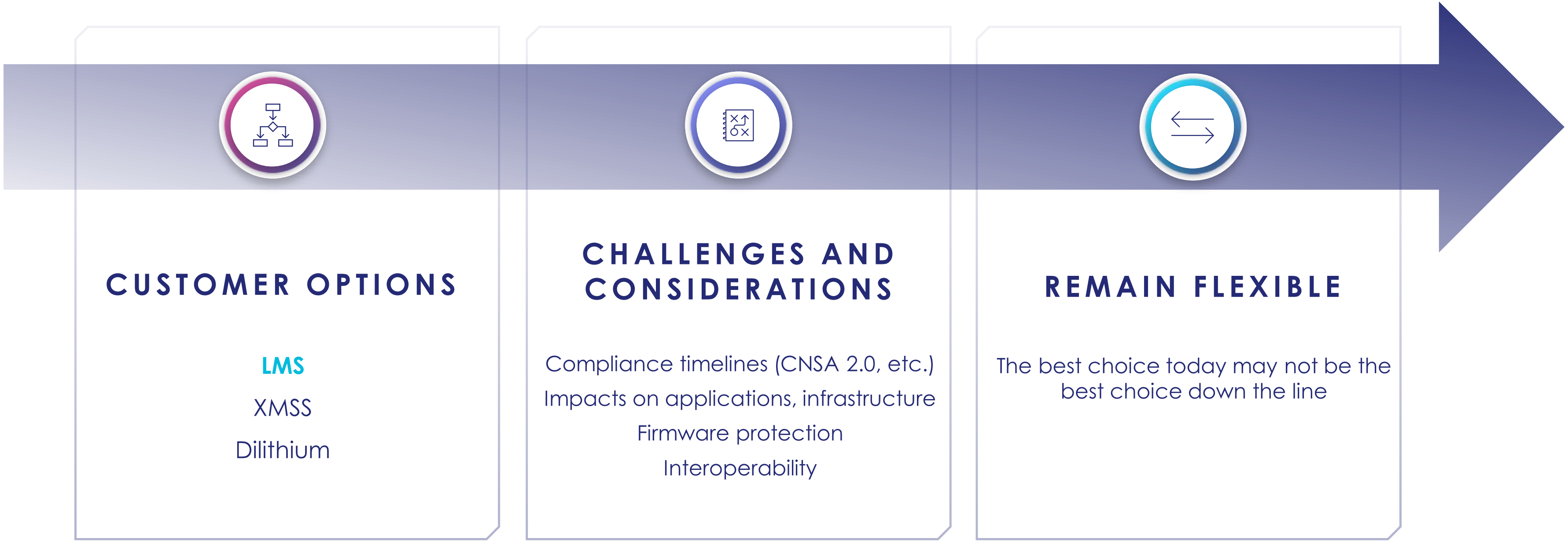
▨ CNSA 2.0 added as an option and tested

▬ CNSA 2.0 as the default and preferred

✓ Exclusively use CNSA 2.0 by this year

LMS & XMSS prescribed for use in **Software/firmware signing** as specified in NIST SP 800-208

Code Signing Case Study: Moving from speculation to implementation



CUSTOMER OPTIONS

LMS

XMSS

Dilithium

CHALLENGES AND CONSIDERATIONS

Compliance timelines (CNSA 2.0, etc.)

Impacts on applications, infrastructure

Firmware protection

Interoperability

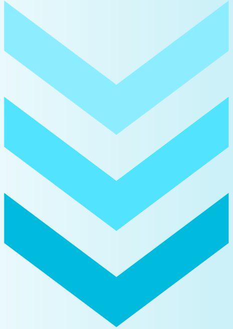
REMAIN FLEXIBLE

The best choice today may not be the best choice down the line

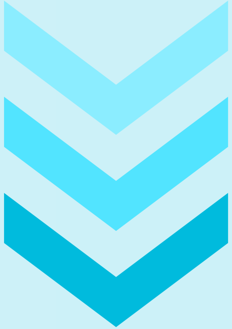
Comparing LMS to Classical Algorithms

Advantages

Public & Private Key Sizes

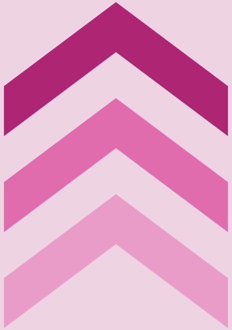


Signature Generation, Verification Times

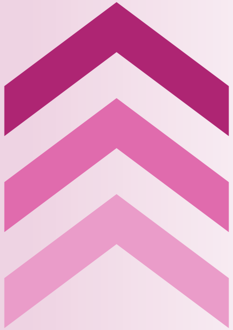


Quantum Resistant

Disadvantages



Signature Sizes

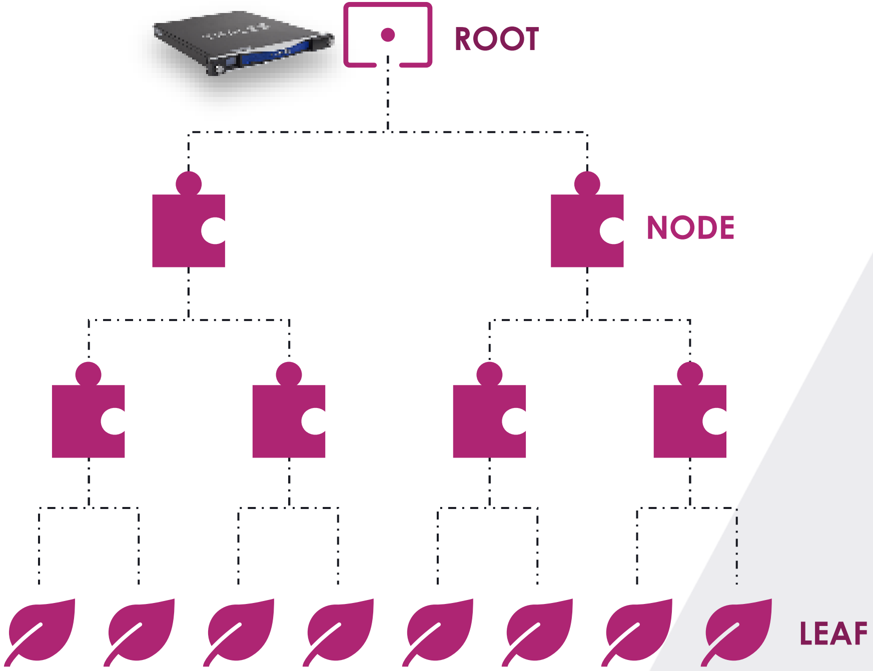


Key Generation Time

THALES
Building a future we can all trust

as compared to RSA & ECDSA

LMS Merkle Trees



An LMS system has the following characteristics:

- The height of the Merkle tree
  - Total OTS capacity = 2^h
- Interior nodes of certain byte lengths
  - Each a hash of its two children
- A second-preimage-resistant cryptographic hash function (e.g., SHA256; SHA256-192)

A Collective Approach to Quantum Readiness

Work with your Technology Partners

- PKI certificate models
- Integrations, APIs
- Systems Integrators

Work with standard bodies

- OASIS for PKCS#11
- IETF
- PKI Consortium
- NCCoE
- IEEE
- X9
- CA/Browser Forum

Sandbox Testing

- CNSA 2.0 – SP800-208 Firmware and S/W
- PQC FM3.1 (ml-dsa & ml-kem ipd + lms/hss + xmss/xmssmt)
- OpenSSLV3.2 provider
- PKCS11 v3.x
- Tools

Hybrid PQC in production

- LMS-HSS
- ML-DSA/ML-KEM
- NTLS PQC
- SLH-DSA
- FN-DSA

After all the work is done, important to remain crypto agile.

Customer Case Study: Wells Fargo

Planning is Essential: PQC Project Planning 101

1. Stakeholders & Staffing

- Exec Sponsorship
- Current staff expertise
- External SMEs
- Seek knowledge

2. Budget for success

3. Project Management

4. Current vs. Desired State

5. Crypto Discovery

- Crypto Assets, vulnerabilities, priority-based approach

6. Ecosystem support from vendors & industry

- Ongoing testing between vendor platforms/solutions (e.g. TLS support)

APPROVED
APPROVED
APPROVED

THALES

Customer Challenge

About Wells Fargo, about their team

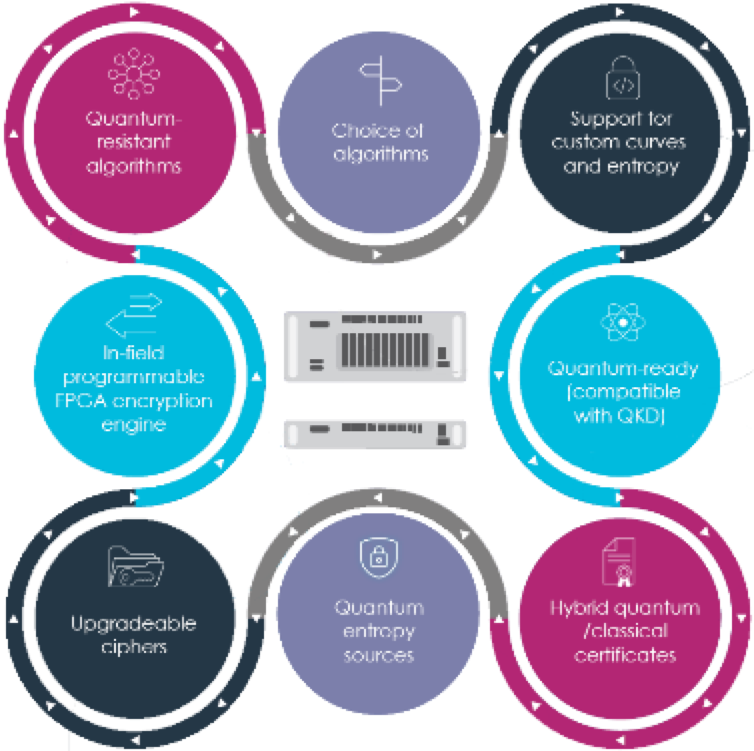
What problems we were faced with	Protecting customer and WFC proprietary data while minimizing disruption to the Enterprise	Establishing crypto-agility as a foundation for PQC mitigation	Developing the foundational layer of the PQC solution tech stack
IT challenges	Integrating quantum entropy into an inherently heterogeneous architecture	Developing a scalable, agile PQC approach to leverage Entropy as a Service for banking innovations and workflows	
Other considerations	Ubiquity for the entire financial ecosystem	Operational costs, technical expertise, resource availability, multi-party cooperation.	Reputational risk – of doing nothing or doing it ineffectually

Key Take-aways

The Best defence is Crypto Agility

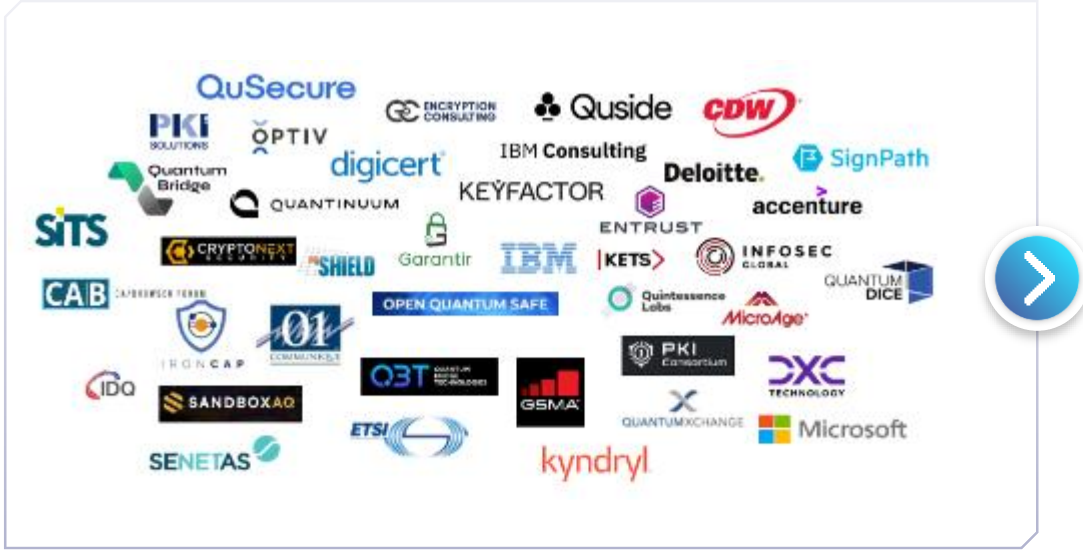
The definition of **Crypto agility** is evolving:

- ➢ Algorithmic flexibility
- ➢ Modular Crypto Framework
- ➢ Compliance & Adaptibility
- ➢ Automated Key/Certificate Management
- ➢ Forward Compatibility
- ➢ Interoperability
- ➢ Resilience



Quantum-resistant algorithms
Choice of algorithms
Support for custom curves and entropy
In-field programmable FPGA encryption engine
Quantum-ready (compatible with QKD)
Upgradeable ciphers
Quantum entropy sources
Hybrid quantum /classical certificates

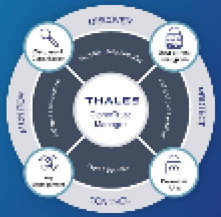
Thales' Growing Quantum Partner Ecosystem



VERIFIED SOLUTION
THALES

Luna HSM

HSE (High Speed Encryptors)



CipherTrust Platform

TRUST BUT VERIFY

APPROVED
APPROVED
APPROVED

- Ecosystem support from vendors & industry
  - Reasonable verification
  - Vetted staff and technology
- Compare with external sources
- Audit – when available
- Assess, Review
- Communicate

Thank you