eBook

Post-Quantum Cryptography

Preparing your organization for a quantum future today



cpl.thalesgroup.com

THALES

CYBERSECURITY

QUANTUM COMPUTERS ARE NOT SCIENCE FICTION

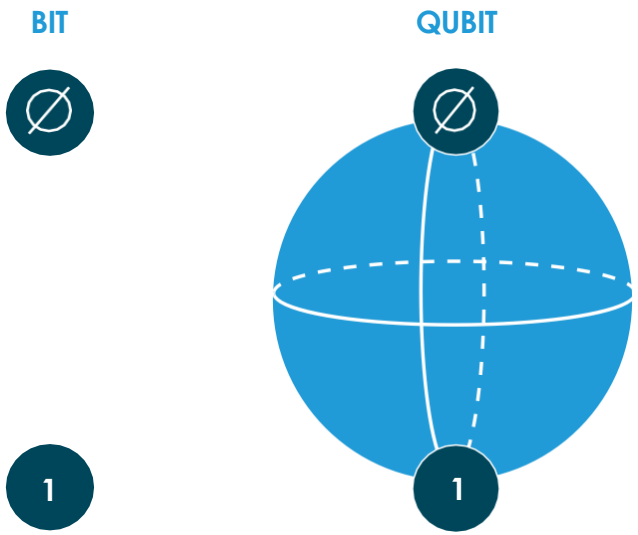
Rather than being reserved for science fiction movies, quantum computers exist today as organizations drive towards commercialization.

- As of Q1 2026, the most powerful quantum processors are generally considered to be the 1,121-qubit IBM Condor and the 1,180-qubit processor by Atom Computing.
- Other leading contenders include the 105-qubit Willow processor from Google and the 98-qubit Helios from Quantinuum.



QUBITS: THE BUILDING BLOCKS OF A QUANTUM COMPUTER

- Classical bit: 0 or 1
  Qubit: Superposition of 1 and 0
- 'N' Entangled qubits represent all 2N states simultaneously
- When measured, all states collapse but one
- Objective is to make the measured state represent something useful





NIST PQC Timeline



2015
Initiation, evaluation, and selection of PQC algorithms

2022

2024
Release the first PQC standards
FIPS 203 (ML-KEM)
FIPS 204 (ML-DSA)
FIPS 205 (SLH-DSA)

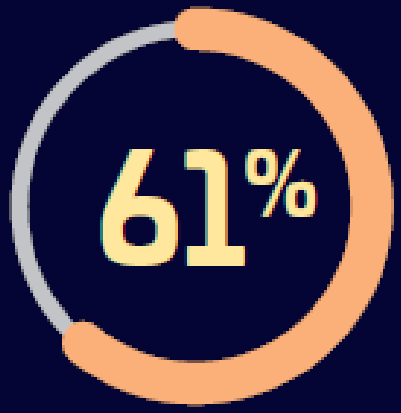
2030
Gradual phase-out and discontinuation of classical algorithms such as RSA-2048, ECC-256

2035
Traditional algorithms disallowed

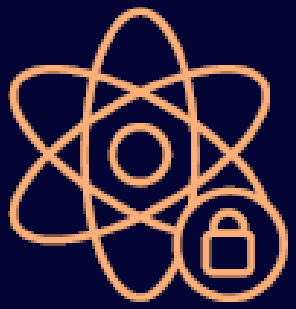
Complete migration of all systems to quantum resistant cryptography

FUTURE RISKS ARE HERE TODAY

Quantum concerns shift to the reality of harvest now, decrypt later (HNDL),



cited as the top concern.



Organizations are moving to mitigate quantum risk

59%

are prototyping and evaluating Post-Quantum Cryptographic (PQC) algorithms.

HARVEST NOW DECRYPT LATER MEANS DATA IS AT RISK NOW

When we talk about HNDL, we're really talking about long-lived value. Data harvested today may still have business, legal, or strategic value years from now. That includes regulated data, intellectual property, critical data flows, and trust chains such as signing and credentials.

This is not just a future-state cryptography issue. It is a current risk-management issue. All data can be harvested; the risk concentrates where value outlives today's crypto. Highest risk candidates for exposure today

- regulated and personal data (PII)
- long-retention records
- intellectual property
- citizen data
- software/signing chains
- critical data flows
- Any data with long confidentiality requirements



Quantum-safe security



Post-Quantum Cryptography

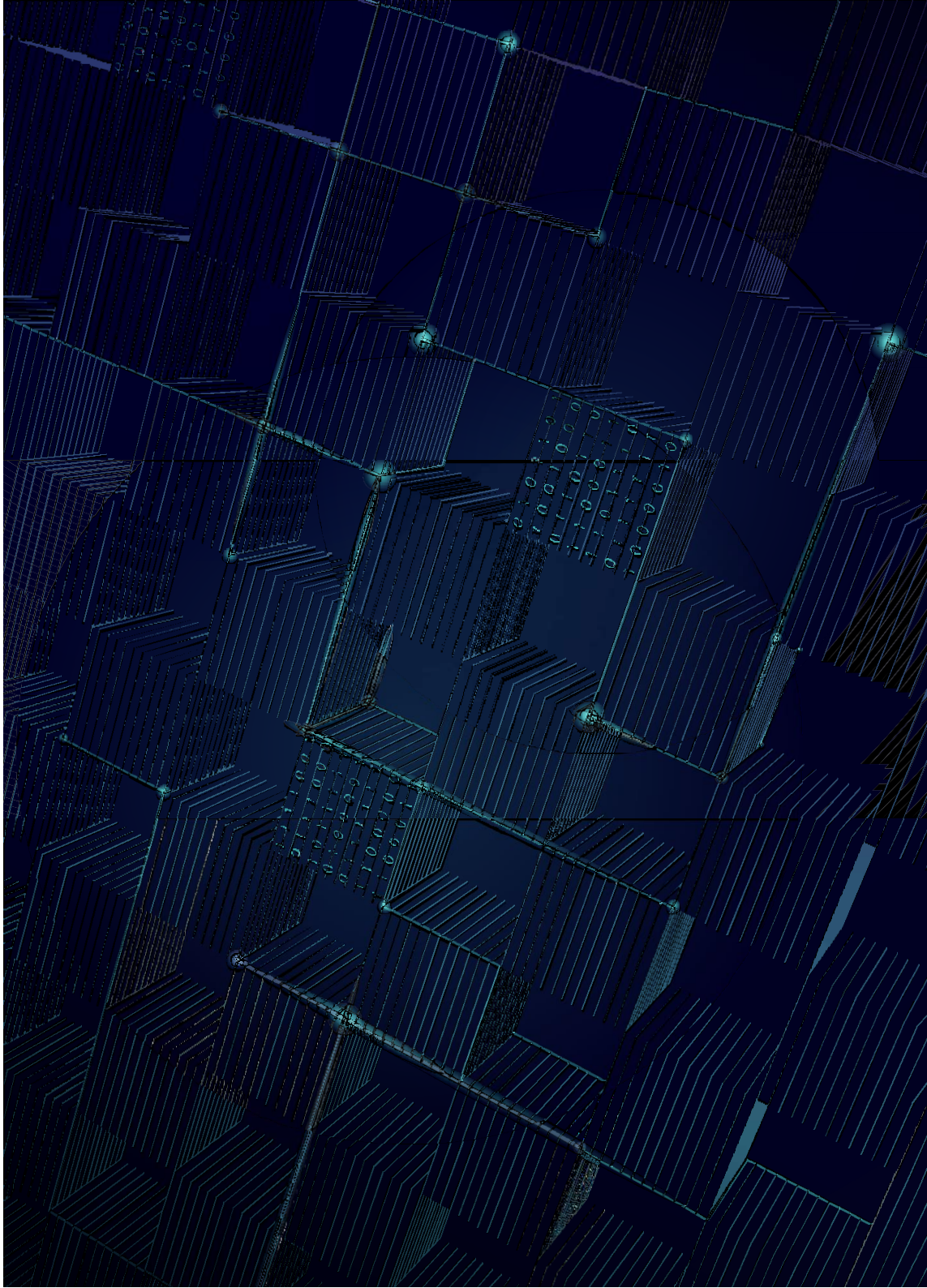
The introduction of post-quantum cryptography (PQC) will provide long-term protection for government and commercial data against the emerging threat of quantum computing. Quantum computers will render today's conventional public key encrypted infrastructures unsecure.

Using a hybrid encryption model, PQC enables customers to combine both classical and quantum-resistant algorithms in a single platform, providing a secure transition to a post-quantum world.

PQC is available to all current and future customers as part of Thales' crypto-agile platform. At Thales, we recognize organizations must adopt a strong post-quantum crypto-agile strategy. In preparation for the transition, Thales encourages organizations to practice crypto-agility now, to help your organization evolve and avoid expensive security retrofitting in the future as quantum computing becomes more established.

This design principle facilitates changes to the cryptography even after deployment and allows you to prepare for the transition to quantum-safe solutions once the NIST standardization process is completed.

To this end, Thales already offers crypto-agile high-speed network encryptors, hardware security modules, and key management solutions that you can take advantage of today.

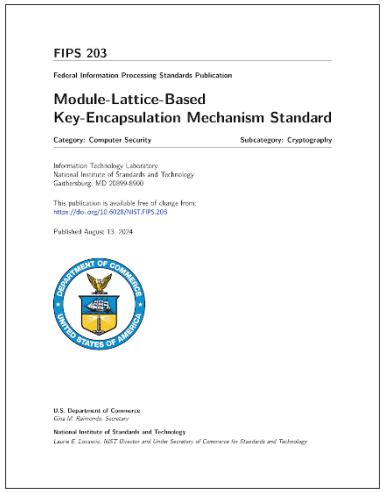


“Without quantum-resistant encryption, everything that has been transmitted, or will ever be transmitted over a network, will be vulnerable to eavesdropping and public disclosure.”

ETSI White Paper No. 8 Quantum Safe Cryptography and Security

WHO IS COMING TO THE RESCUE?

Currently, there are three NIST finalized post-quantum encryption standards and encouraged organizations to begin transitioning as soon as possible. Now that NIST has officially standardized these algorithms, governing bodies worldwide will issue compliance mandates based off the NIST PQC standards. The finalists are:


FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

FIPS 203

Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)


FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

FIPS 204

Module-Lattice-Based Digital Signature Standard (ML-DSA)


FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

FIPS 205

Stateless Hash-Based Digital Signature Standard (SLH-DSA)

THE IMPORTANCE OF CRYPTO-AGILITY & QUANTUM-READINESS

The world depends on Public Key Infrastructure (PKI) to establish trust.

PKI depends on asymmetric key protocols such as RSA, ECC and others.

Quantum computers and research will efficiently crack PKI and code signing.

Post-quantum cryptography (PQC) will ensure that sensitive data remains encrypted into the future.





Why Act Now?

Even if quantum-capable attacks are not here tomorrow, exposure is building now, migration takes time, and leadership increasingly expects proof before the full transition is complete.

Exposure is already compounding

Long-life data, credentials, and signing chains stolen now can be decrypted later — HNDL risk builds with time, not with a ‘quantum event’.

Migration time is the bottleneck

Inventory, interop testing, PKI alignment, and partner coordination take years; starting later compresses your runway.

Evidence is expected early

Boards, regulators, and partners want crypto inventories, heatmaps, and execution artifacts before full migration is complete.

Zero-regret moves

Take inventory, prioritize, and validate interoperability, then stage PQC migrations.

Prove progress early

Start with key use cases, then scale in waves.

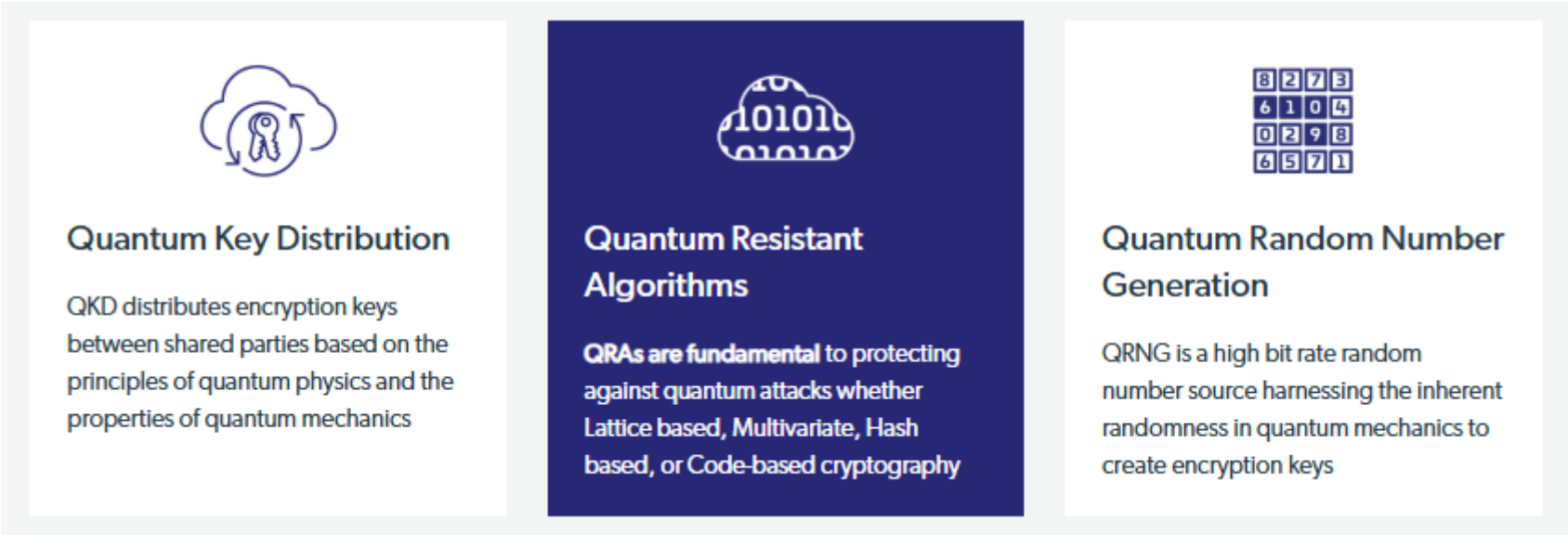
"The best way to start preparing is to ensure that all current and future systems have cryptographic agility – the ability to be easily reconfigured to add quantum-resistant algorithms."

Dr. Brian LaMacchia,
Distinguished Engineer and Head of the Security and Cryptography Group at Microsoft Research

Building a Future-Proof Post-Quantum Strategy

Post-quantum cryptography (PQC) comprises algorithms and protocols designed to resist quantum computer attacks. They remain compatible with current computing systems and support the transition from quantum-vulnerable algorithms such as RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman.

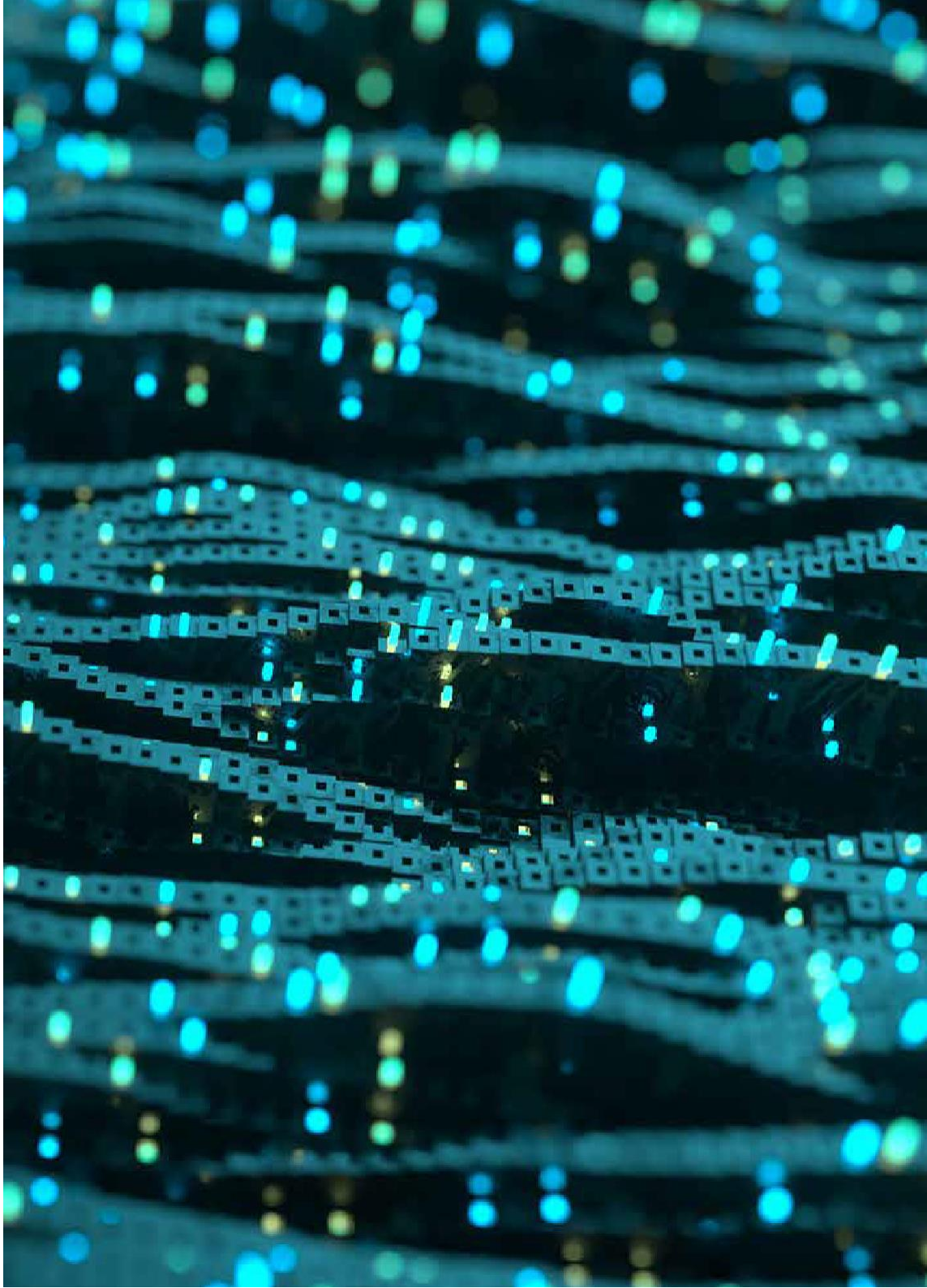
Securing an enterprise against quantum threats requires cybersecurity solutions that support Quantum Resistant Algorithms (QRA) plus offer options for Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG). Thales is committed to delivering solutions that support a Post-Quantum crypto agile strategy.

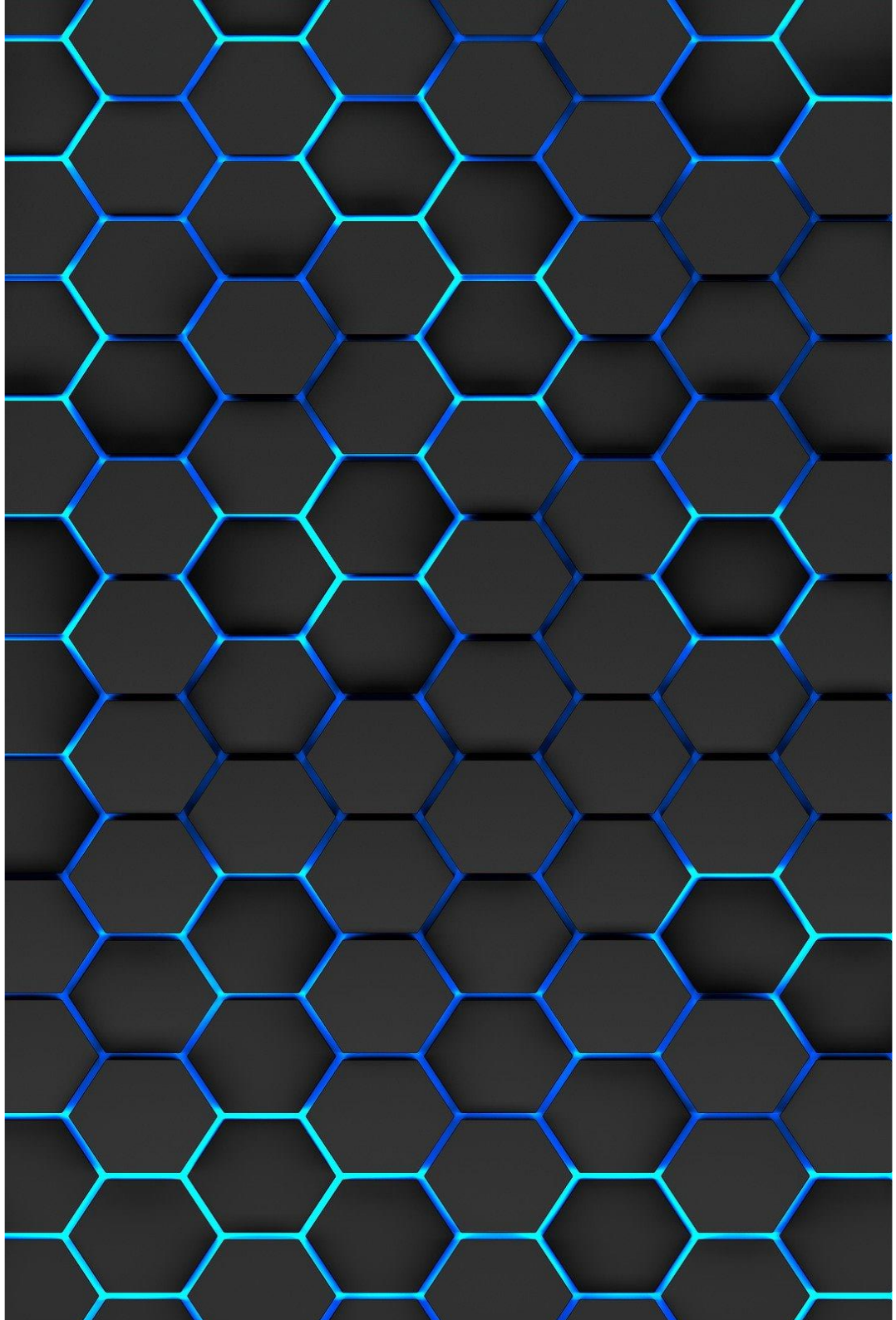


The Quantum Threat: Why preparation can't wait

Today's widely used public-key cryptographic systems and protocols, including RSA, ECC and Diffie-Hellman, rely on mathematical problems that are hard for classical computers to solve. Future quantum machines are expected to solve these problems much more efficiently, putting current algorithms and the systems that depend on them at risk. Because attackers can "harvest now, decrypt later," long-lived data is already exposed.

Organizations should begin PQC migration now by identifying quantum-vulnerable cryptography, prioritizing high-risk and long-lived data, and preparing for hybrid environments using both classical and NIST-standardized PQC algorithms.





Where To Start: Where Risk Becomes Action

It's critical that you start in the places where cryptographic failure has the highest operational impact today.

In practice, we see three strong starting points. One is the root of trust — PKI, signing, firmware, and the foundational services that must not break.

The second is data in motion, especially where sensitive data is constantly moving across critical networks and continuously exposed to collection programs and at risk of HNDL attacks.

And the third is visibility and proof — because if you can't see, prioritize, validate, and evidence your progress, it's very hard to scale a migration program. These three areas create immediate risk reduction and the executable runway for the broader program.

Where To Start: Where Risk Becomes Action

A pragmatic first migration wave (blast radius × change difficulty × lifetime)

Start in the places where cryptographic failure has the highest operational impact today.
In practice, we see three strong starting points.
One is the root of trust — PKI, signing, firmware, and the foundational services that must not break.

The second is data in motion, especially where sensitive data is constantly moving across critical networks and continuously exposed to collection programs and at risk of HNDL attacks. And the third is visibility and proof — because if you can't see, prioritize, validate, and evidence your progress, it's very hard to scale a migration program. These three areas create immediate risk reduction and the executable runway for the broader program.

Protect the Root of Trust

- PKI, signing, firmware
- Deep supply chain dependencies

Goal: controlled path + evidence

Reduce Exposure of Data in Motion

- Sensitive, high value data flows constantly across corporate networks

Goal: Protect data against collection programs and HNDL attacks now

Discover and Prove

- Discovery + policy + audit
- Validated interop before scale
- Audit artifacts aligned to regulated expectations

Goal: operate hybrid at scale

KEY TAKEAWAYS

Quantum is coming

Quantum capabilities are accelerating

NIST and others are preparing quantum-safe standards

PKI-based crypto will become obsolete

Know your risks

Long-term data is at risk, if using classic technologies

Consider that it is vulnerable to harvest now decrypt later attacks

Focus on crypto agility

Crypto-agility is the best practice; requires supporting infrastructure

Take a hybrid approach by using classic & quantum-safe crypto solutions

Start now

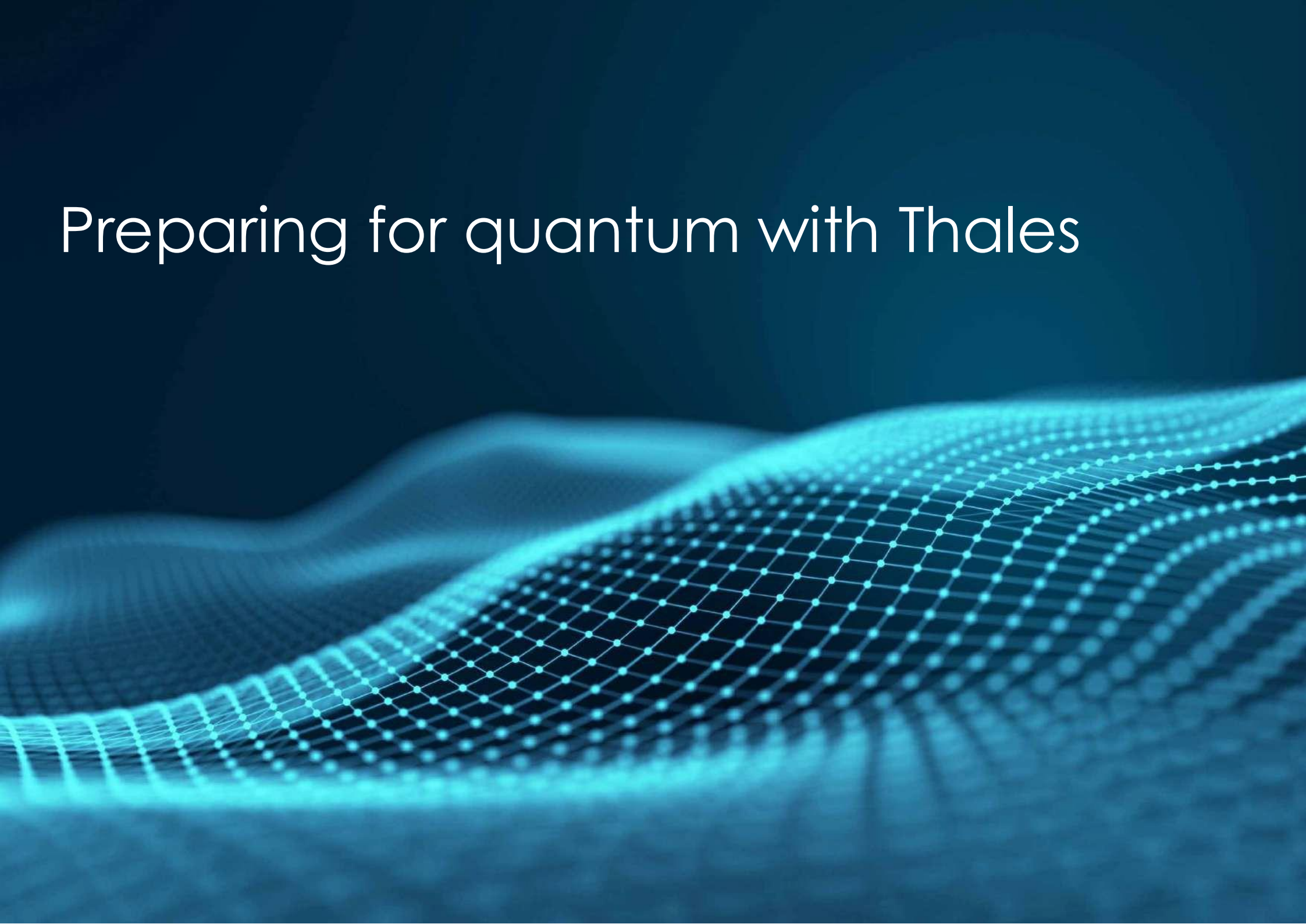
Assess your crypto-agility maturity and readiness

Design a quantum-safe architecture

Be ready for change, even after standards are established

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

Preparing for quantum with Thales



Constraint #1 Trust Anchors Must Not Break

Compliance/assurance + partner interoperability

Luna HSMs Foundation of Digital Trust

- Available Today: Luna 7 supports PQC-ready algorithms, quantum safe protocols, and QRNG injection
  Next: next-gen Luna HSM built for PQC crypto-agility
- Crypto-agile capabilities: PQC/hybrid profiles, strong entropy, and updateable protocols
- Thales-designed crypto processor: optimized for PQC

What we see

- Deep supply chain dependencies
- Lifecycle evidence: sign, rotate, revoke
- Interop with PKI providers + GSIs

What "good" looks like

- Stable trust services
- supply chain dependencies
- Clear evidence for signing, and other assurance
- Interop with PKI, firmware/code-signing and supply chain workflows

Solution pattern

- HSM as the foundation of trust for hybrid transition and assurance of core trust



THALES
CYBERSECURITY

Reduce exposure now while migration proceeds in waves

Constraint #2 Migration Takes Years—Threats Don't

High Speed Encryptors (HSE) Crypto-agile protection for long-lived data across networks

- Available today: PQC-ready now, reduces exposure to HNDL threats
- Drop in the network solution (physical or virtual); plus QKD integrations, and QRNG support
- Crypto-agile, future-proof to support evolving standards with no performance degradation

What we see

- Sensitive data moves constantly
- HNDL is a top concern (DTR)
- AI increases attacker speed and scale
- Protect high-value data in motion now and prevent HNDL

What "good" looks like

- Risk reduction of exposure on critical data in motion
- Interop + performance validated
- Deploy now, no need to wait for application or PKI migration
- Continued operability as standards evolve

Solution pattern

- Protect data in motion across networks now as broader PQC migration continues



THALES
CYBERSECURITY

Constraint #3 Prove Progress

Measurable, auditable, interoperable

CipherTrust Data Security Platform/Data Security Fabric

Quantum-Safe Visibility and Readiness

- Identify and inventory quantum-vulnerable assets across the DSF ecosystem - You cannot transition what you cannot see, prioritize, validate, and prove
- Critical areas will be identified, with prioritization based on data sensitivity and regulatory requirements
- Crypto APIs and JWT Authentication
- PQC PKI Certs for TLS Server/Clients and CA

What we see

- Inventory → validate → transition → operationalize
- Audit + policy + lifecycle controls
- Interop across PKI, cloud, GSIs

What "good" looks like

- Repeatable migration waves
- Audit artifacts aligned to regulated expectations
- Ecosystem-validated patterns

Solution pattern

- Create visibility, prioritization, governance, and evidence for phased PQC migration



THALES
CYBERSECURITY

PQC 2026: The Year of Action with Thales

PQC readiness is security posture + operational continuity

Be prepared for evolution

Build crypto-agility so you can adopt new profiles without disruption

Reduce risk now

Protect the foundation of trust, sensitive data, and critical networks while migrations progress

Stay compliant and auditable

Policy, lifecycle, and evidence aligned to security and regulatory expectations

Execute with the ecosystem

Validated patterns with GSIs, PKI providers, and cloud/platform partners

Start Now—Turn Your PQC Pilot into Production

THALES
CYBERSECURITY

Thales Cloud Protection & Licensing

Our Solutions

- Data Security
- Access Management & Authentication
- Software Monetization

Over **2,600** employees

25 countries presence

750 engineers worldwide

30,000 customers worldwide

Thales's technologies and services help secure more than 80% of all global payment transactions and increasingly valuable corporate and government information

The people we rely on to secure our privacy rely on Thales

#1 Worldwide in general-purpose HSMs	#1 Worldwide in data encryption
#1 Worldwide in payment HSMs	#1 Worldwide in key management
#1 Worldwide in cloud HSMs	#2 Worldwide in cloud authentication
#1 Worldwide in software protection	#1 Worldwide in software licensing

THALES

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data.

When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact Us

For contact information, please visit



cpl.thalesgroup.com/contact-us



cpl.thalesgroup.com

© Thales - July 2026 v5