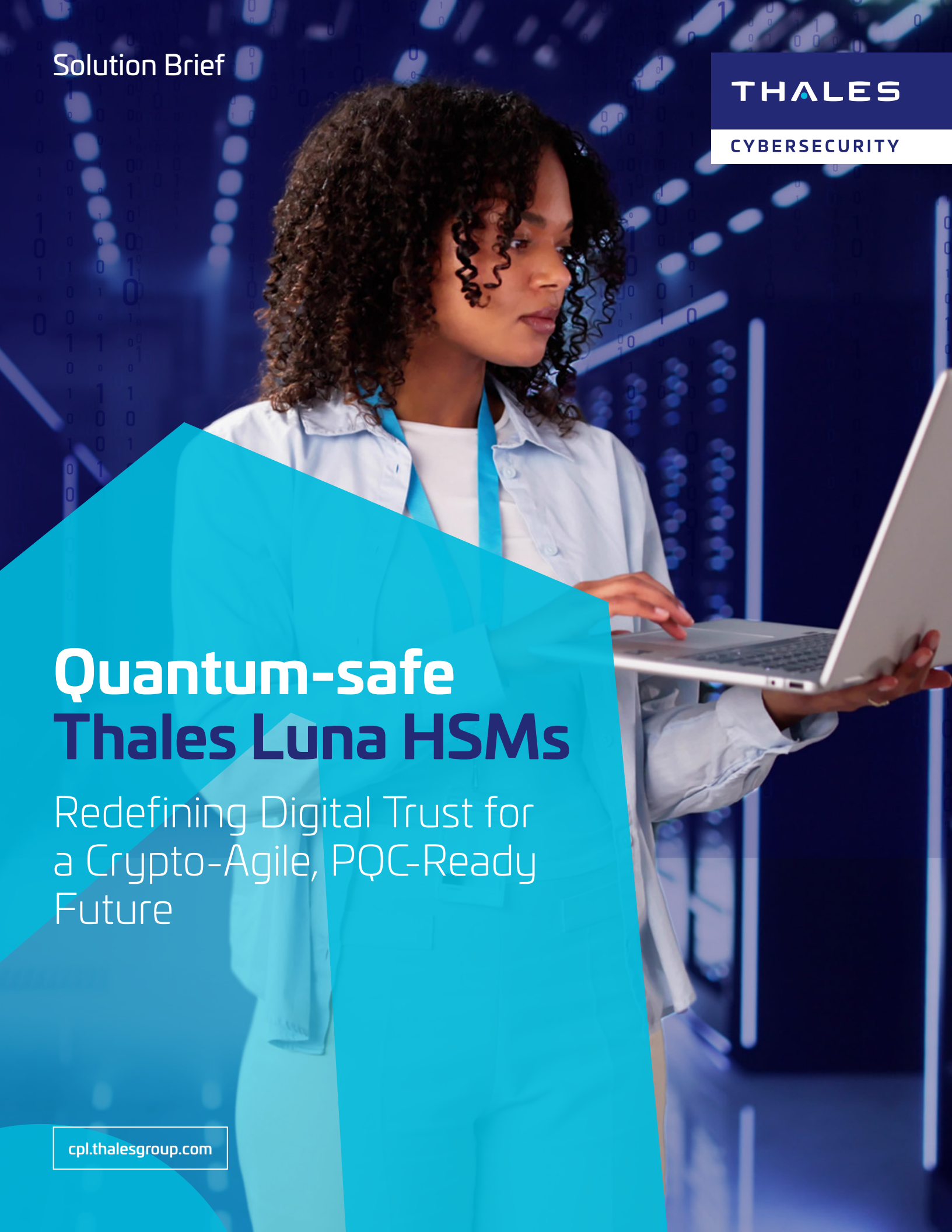
Solution Brief

THALES

CYBERSECURITY



# Quantum-safe Thales Luna HSMs

## Redefining Digital Trust for a Crypto-Agile, PQC-Ready Future

cpl.thalesgroup.com

THALES

CYBERSECURITY

## Highlights

**Thales Luna HSM offers:**

- Luna 7 HSMs have NIST standardized algorithms implemented directly into Luna HSM firmware including ML-KEM (FIPS 203) and ML-DSA (FIPS 204), with a crypto-agile foundation that supports continued adoption of additional algorithms as standards mature.
- Hybrid PQC key exchange mechanism for secure key synchronization, backup, and restore.
- Post-quantum protection for use cases such as TLS/SSL, key exchange, IoT, and database encryption, helping address the 'harvest now, decrypt later' risk.
- Built-in resistance to side-channel and physical attacks for high-assurance cryptographic protection.
- Strong entropy for high-quality key generation to support secure and reliable cryptographic operations.
- Thales is developing its next-generation HSM to be quantum-safe from the ground up, combining PQC agility, strong entropy, updateable protocols, and a Thales-designed crypto processor optimized for post-quantum performance.

## The Problem

Today's widely used public-key cryptographic systems and protocols, including RSA, ECC, and Diffie-Hellman, are secure against classical computers and play a central role in Public Key Infrastructure (PKI), supporting certificate issuance, authentication, and trust chains across digital ecosystems. Future quantum computers are expected to break the mathematical foundations these systems rely on, putting current algorithms and the systems that depend on them at risk. Because attackers are already harvesting encrypted data today with the intent to decrypt it later, long-lived data and digital trust assets are already at immediate risk.

## Challenge

Organizations should begin post-quantum cryptography (PQC) migration now by identifying quantum-vulnerable cryptography, prioritizing high-risk and long-lived assets, and preparing for hybrid environments that support both classical and NIST-standardized PQC algorithms.

That transition is a multi-year effort that spans teams, technologies, suppliers, and operational constraints. Discovery, prioritization, interoperability testing, vendor alignment, and phased rollout all take time, and those factors often shape the pace of progress as much as algorithm availability does. Migration timelines are also influenced by infrastructure maturity, supplier readiness, hardware limitations, and evolving standards and regulatory requirements.

Hardware Security Modules (HSMs) are especially important in this process because they secure key generation, storage, and cryptographic operations at the core of digital trust. As organizations prepare for PQC, HSMs increasingly need to support both classical and quantum safe keys and certificates, crypto agility, and NIST-standardized post-quantum algorithms. If the HSM cannot support the algorithms, interfaces, certificates, and operational models required for transition, the systems and workflows that depend on it cannot move forward. As a result, HSM selection has become a strategic part of PQC planning.

## The Solution

Thales Luna HSMs provide a trusted, tamper-resistant foundation for organizations preparing for the transition to post-quantum cryptography. They help security teams protect sensitive keys, support critical cryptographic operations, and introduce new post-quantum capabilities in a controlled, operationally sound manner. FIPS 140-3 Level 3 validated and Common Criteria EAL 4+ certified, Thales Luna HSMs support high-assurance cryptographic operations across PKI, certificate authority protection, code signing, firmware signing, and other trust-critical workflows.

Among the first HSMs to incorporate NIST-standardized post-quantum algorithms directly into firmware, Thales Luna HSMs support ML-KEM (FIPS 203), ML-DSA (FIPS 204), along with HSS as defined in NIST SP 800-208. This gives customers the flexibility to test, validate, and deploy hybrid or full PQC approaches based on their risk profile, operational requirements, and migration timeline. Luna HSMs also incorporate high-quality hardware-based entropy sources, including QRNG-based capabilities, to support high-assurance key generation. By integrating with leading crypto-agile platforms, they enable more controlled and interoperable adoption of new cryptographic algorithms as they emerge, helping organizations future-proof applications and use cases without requiring extensive rework as cryptographic standards evolve.

## Luna HSMs enable you to:

- Future-proof digital signature strategies for devices and software by preparing for quantum-safe signing approaches that help maintain trusted software and firmware updates far into the future.
- Use stateful hash-based signature schemes for high-assurance signing use cases, including standards-based approaches addressed by NIST SP 800-208 and aligned with NSA CNSA 2.0 software and firmware signing guidance.
- Validate NIST-standardized PQC algorithms in real-world environments, including ML-KEM (FIPS 203) and ML-DSA (FIPS 204) for key exchange, encryption, and digital signature.
- Adapt to evolving cryptographic models without forcing disruptive infrastructure changes, enabling a more controlled transition from classical to PQC.
- Strengthen the hardware root of trust behind critical keys, certificates, and signing operations.
- Advance PQC readiness across trust-critical environments such as PKI, TLS, code signing, IoT, and database encryption.
- Choose from a variety of quantum-safe hardware options to best meet your business needs (Luna Network, PCIe, USB and Backup HSM solutions).

## Key Benefits:

- Build a resilient foundation of digital trust by preparing high-value use cases such as code signing, firmware signing, PKI, and machine identities for the quantum transition.
- Securely generate and protect quantum-resistant keys inside certified tamper-resistant hardware.
- Support crypto agility with a platform designed to help organizations validate, adopt, and evolve cryptographic policies over time.
- Reduce migration risk by supporting classical, hybrid, and post-quantum environments in a controlled way.
- Maintain stronger governance and assurance for the systems and workflows that must remain trusted throughout the transition.

## Proven Across the PQC Ecosystem

PQC migration depends on interoperability across platforms, applications, and suppliers. With one of the broadest partner ecosystems in the market, Thales helps customers validate PQC readiness across PKI and key management environments and move forward with greater confidence.

Thales works closely with leading technology partners and select customers to test and validate PQC capabilities across real-world HSM use cases. This helps confirm operational readiness across diverse platforms and deployment models while giving customers a more practical path to quantum readiness. In one recent collaboration with a leading financial institution, Thales Luna HSMs helped establish a strong foundation for crypto agility by enabling secure, QRNG-based key generation within the cryptographic boundary of a FIPS-validated Thales Luna HSM using verified quantum entropy.

**Thales leadership in shaping a trusted PQC ecosystem through standards, alliances, and partnerships.**

## What to Do Next: Build an Iterative PQC Migration Program

Building on that readiness, PQC migration should be approached as an iterative program rather than a one-time checklist. An effective transition starts with identifying quantum-vulnerable cryptography across systems, applications, and supply chains, followed by risk assessment, policy review, and validation of whether critical infrastructure can support hybrid and post-quantum models. Through four levels of maturity, organizations can prioritize the most exposed assets, plan phased migration and mitigation paths, and strengthen crypto agility over time through continuous monitoring, governance, and refinement.

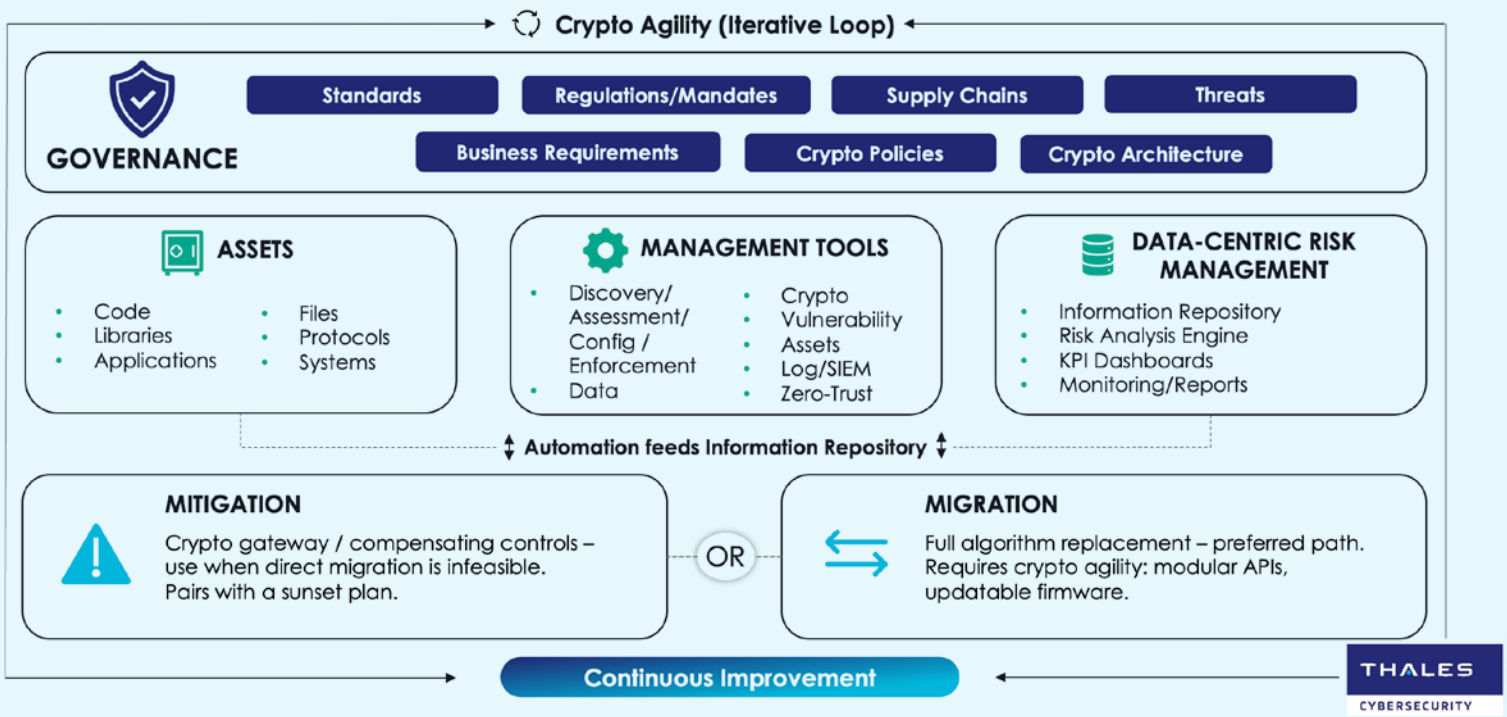
See how **Thales Luna HSMs** can help you strengthen the foundation for crypto-agile, quantum-safe migration.

## About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

## Crypto Agility: An Iterative Loop

### NIST CSWP.39 Crypto Agility Strategic Plan




**Source:** NIST CSWP.39 Crypto Agility Strategic Plan

cpl.thalesgroup.com

**Contact us –** For contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - June 2026 • AC v5