Solution Brief

Post-Quantum Readiness Begins with Crypto Agility

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Get ready for quantum

With quantum computers set to break traditional encryption, you need to take measures to protect your data now. Harvest now, decrypt later (HNDL) attacks where cyber attackers collect and store encrypted data with the goal of decrypting it in the future using quantum computers is already happening.

Prepare for Post-Quantum Cryptography (PQC) by creating a trusted environment for your business to test PQC-ready encryption and identify potential implications that quantum computing may have on the security of your infrastructure and develop plans to quickly adjust.

This year, NIST intends to publish and standardize the Post Quantum Cryptography (PQC) algorithms of choice for organizations to adapt to protect from quantum computing attacks. Once NIST officially standardizes these algorithms, governing bodies worldwide will issue compliance mandates based off the NIST PQC standardization process. The mandates will then trigger compliance directives to be issued, leaving organizations scrambling to implement.

Secure data-in-motion with a network encryption solution for PQC with a built in crypto-agile architecture

Why PQC now?

Transforming current cryptography methods to PQC takes significant time and the best strategy is to **prepare now**. By getting a head start, you'll minimize disruption for your organization and your customers, reduce costs and risks, and ensure business continuity during the transformation. It will also position your organization to be fully compliant with NIST and other industry PQC regulations as soon as they're announced. Quantum attacks are already happening today with HNDL, and it's wise to start now with interim solutions like using longer symmetric key lengths, or out-of-band keys. Not only will this protect your organization from HNDL today, you'll be better prepared to implement post-quantum cryptography when available.

Scan to request an HSE PQC Starter Kit

Take the first step with the PQC Starter Kit

The PQC Starter Kit with Thales High Speed Encryptors (HSE) is a low-cost solution that helps organizations create a test environment to accelerate the process of testing quantum-resilient measures in a safe environment. In this PQC lab, you can simulate running your applications, transferring data, etc. with post-quantum cryptography and entropy, helping you validate architecture . By preparing today, you'll be creating a plan of action to ensure operations will continue to run smoothly when the algorithms are finalized in firmware.

Easily set up your quantum-safe test environment with:

- ✓ **NIST Post-Quantum algorithms pre-implemented**
- ✓ **Out of band key management, NIST approved KDF method**
- ✓ **Optional Quantum Key Distribution via ETSI eQKD v14.01**
- ✓ **Optional QRNG (Quantum random number generation) or External Entropy Source (BYOE—Bring your own encryption)**

What's included in the HSE PQC Starter Kit

The starter kit is made up of fully featured HSEs which can be dropped into a production environment to provide additional security and improved performance to existing networks.

- **3 HSE network encryption appliances selected from the Thales HSE portfolio**
  - **CN4010/CN4020:** up to 1 Gbps Network Encryptors, certified, high-performance, small form factor ideal for remote locations such as CNI, SCADA, voice/video
  - **CN6010:** 1 and 10 Gbps Network Encryptors, rack-mountable, fully redundant robust design, ideal for private networks and data centers
  - **CN6140:** Up to 4x10 Gbps Network Encryptors, 4 independent encryption channels for scale, supports high scalability and multi-link networks
- **CM7 Network Manager – Encryption management platform (downloadable from customer portal)**
- **Recommended additions**
  - Power Cords (CN6000 series models)
  - Transceivers (Specifically for the CN6000 and CN4020 units)
  - Maintenance and support
  - Remote install and configuration