Solution Brief

THALES

CYBERSECURITY

Quantum-Safe Network Encryption

Thales High Speed Encryptors

cpl.thalesgroup.com

THALES

CYBERSECURITY

Quantum-safe protection starts with the network

Post-quantum cryptography and crypto agility for high-value data in motion.

PROTECT NOW
High-assurance network encryption

MIGRATE
Standardized post-quantum cryptography + network-independent encryption

STAY AGILE
Evolve cryptography over time

Protect long-life data now, while building a controlled path to quantum-safe network security.

Sensitive data is already crossing data centers, clouds, AI infrastructure, backup and recovery networks, operational environments and critical sites. The network encryptors organizations select today will remain in service for years. If that data must remain confidential into the post-quantum era, Harvest Now, Decrypt Later (HNDL) means the exposure is already building. The time to protect the critical network links you control with quantum-resistant network encryption is now.

01 **Long-lived data**

Intellectual property, government information, operational data, PII and AI assets may need confidentiality for years.

02 **AI moves the trust boundary**

Models, training data, prompts and inference traffic move across infrastructure organizations may not own. Key control matters.

03 **Migration is accelerating**

Standards are finalized and national roadmaps increasingly set planning, procurement and migration milestones

Thales High Speed Encryptors (HSE)

Quantum-resistant options available today

NIST-standardized post-quantum cryptography (PQC)

HSE supports NIST-standardized PQC: ML-KEM (FIPS 203) for quantum-resistant key establishment, and ML-DSA (FIPS 204) and SLH-DSA (FIPS 205) for digital signatures. A quantum-resistant certificate can be used as the primary certificate*, enabling a PQC-first profile where the environment is ready.

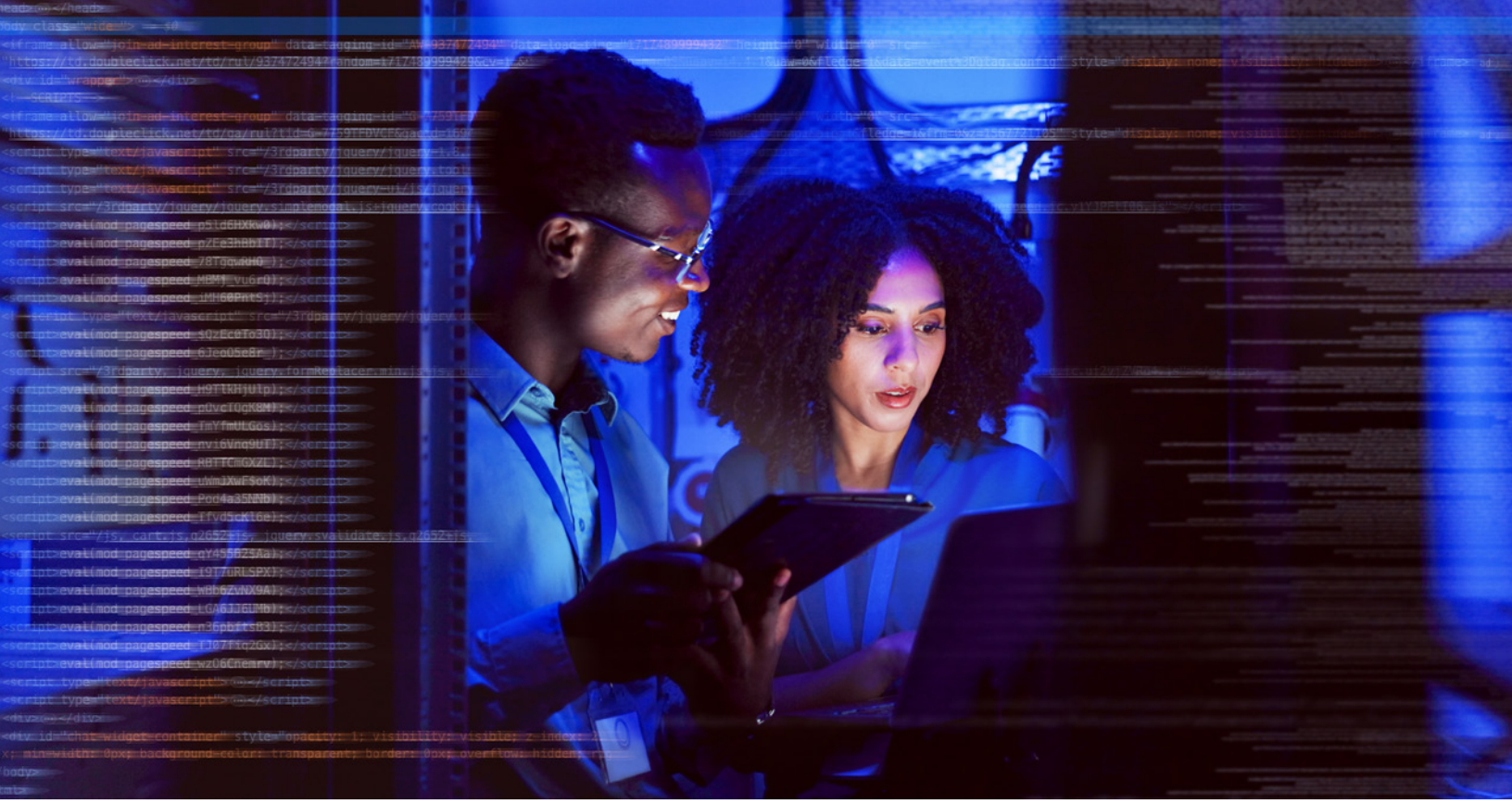
Transport Independent Mode (TIM)

Transport Independent Mode (TIM) is HSE's transport-independent network encryption mode. Instead of certificate-based public-key exchange across the protected network, it uses a key-provider model and NIST-approved key derivation. TIM is not PQC; it provides a distinct approach to reducing Harvest Now, Decrypt Later exposure by avoiding on-wire public-key key establishment.

*Available with 5.7.0 firmware and later
Feature availability may vary by HSE model and configuration

Transition and Complementary Options:

Where interoperability requires classical and post-quantum environments to coexist, HSE supports hybrid operation as an interim bridge, with a path to retire classical dependencies. For selected architectures, HSE can also integrate compatible Quantum Key Distribution (QKD) key material and Quantum Random Number Generation (QRNG)-sourced entropy.



Quantum-safe without compromising the network

The objective is not simply to add Post-Quantum Cryptography (PQC). It is to transition to quantum-resistant cryptography while preserving performance, control, assurance and operational continuity.

PQC out of the high-speed data path

Post-quantum mechanisms secure connection establishment. Once established, high-speed network traffic is protected on the symmetric Advanced Encryption Standard (AES) data path. This strengthens authentication and key establishment without making PQC a data-plane bottleneck.

Network encryption foundation

- Up to 100 Gbps, depending on platform and configuration
- Protection at Network Layers 2, 3 and 4
- Physical and virtual deployment options
- Customer-controlled keys, policies and encryption infrastructure
- Independent validations and approvals by applicable platform and configuration

Crypto-agility in practice

HSE uses field-programmable gate array (FPGA) technology and field-upgradable firmware so cryptographic capabilities, connection profiles and security policies can evolve as standards and requirements change.

- **MOVE** to a PQC-first certificate profile where the environment is ready.
- **ADAPT** connection profiles and security policies as interoperability requirements change.
- **USE TIM** where an architecture without on-wire public-key exchange is appropriate.
- **UPDATE + PROTECT** cryptographic capabilities in the field, including quantum-resistant integrity protection for device software upgrades.

GLOBAL POLICY + MIGRATION MOMENTUM

Quantum-safe migration is moving from strategy to implementation worldwide. Standards bodies, governments and national cyber authorities are setting migration milestones, procurement expectations and implementation guidance. These are market and planning drivers, not claims of HSE regulatory compliance.

AMERICAS | STANDARDS + MILESTONES

- **UNITED STATES / NIST**
  NIST's finalized PQC standards are ready for implementation now, while current guidance emphasizes migration planning and crypto-agility.
- **CANADA | 2026 / 2031 / 2035**
  Federal roadmap set April 2026 for initial departmental migration plans, 2031 for high-priority systems and 2035 for remaining systems.

EUROPE | COORDINATED TRANSITION

- **EUROPEAN UNION**
  The EU coordinated implementation roadmap calls for Member State transition plans and phased migration, prioritizing high-risk use cases and critical infrastructure.
- **UNITED KINGDOM | 2028 / 2031 / 2035**
  NCSC targets an initial migration plan by 2028, highest-priority migrations by 2031 and completion by 2035.

ASIA-PACIFIC | IMPLEMENTATION + PROCUREMENT

- **AUSTRALIA | 2026 / 2028 / 2030**
  ASD calls for transition planning by end-2026, critical-system migration underway by 2028 and completion by 2030; new cryptographic equipment intended beyond 2030 should support approved PQC.
- **JAPAN | 2035**
  Government and related agencies aim, in principle, to transition to PQC by 2035, with a national roadmap being developed in FY2026 and earlier action for especially sensitive or long-lived information.
- **SINGAPORE**
  Singapore identifies PQC as the mainstream approach to quantum-safe migration, using NIST standards as a baseline, with QKD positioned as complementary for selected high-assurance use cases.

GLOBAL + SECTOR | CONVERGING DIRECTION

- **G7 FINANCIAL SECTOR | ~2035**
  The 2026 G7 Cyber Expert Group identifies 2035 as a prudent overall planning horizon for financial-sector transition, while emphasizing risk-based prioritization and crypto-agility.

Start with the network links you control.

Quantum-safe migration does not have to start everywhere at once. High-value network links where you control both endpoints can provide a practical place to reduce exposure and move from planning to deployment.

Prioritize high-value data-in-motion paths

Start where the confidentiality horizon, business value and network control make action practical.

- Data center interconnects
- Cloud and multi-cloud connectivity
- AI / GPU infrastructure
- Backup and disaster recovery
- Operational and critical-infrastructure links
- Selected partner connections

Thales High Speed Encryptors (HSE) combine high-assurance network encryption, standardized post-quantum cryptography, Transport Independent Mode and crypto-agility to help organizations move these links toward quantum-safe protection without sacrificing performance or operational control.

Talk to Thales

Prioritize the critical network links you control and define a Crypto-agile path to quantum-safe network encryption.

cpl.thalesgroup.com/encryption/data-in-motion

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us