Thales and Quantum Xchange: Delivering Quantum-Safe, Data-in-Motion Security without Compromise

Phio TX from Quantum Xchange Makes Thales Network Encryptors Immediately Quantum-Resistant, Bringing to Market the First Quantum-Safe HSE

The Problem

Advances in computing and mathematics continue to push the boundaries of how best to secure data in motion. The arrival of a quantum computer will easily break the encryption that protects most of our digital world. Meanwhile, present-day Public Key Encryption (PKE) – the conventional method for protecting transmitted data, i.e., TLS/SSL – suffers from weaknesses and vulnerabilities beyond the quantum threat. With PKE, the encryption keys and data travel together. An attacker needs only to compromise one connection to obtain secret information.

As the industry debates the arrival time of a quantum computer, and the most commonly used crypto algorithms are in the process of standardization and open for public review, organizations recognize the importance of crypto agility and quantum-safe key distribution for future-proofing their crypto infrastructure and keeping their most critical asset – data – better protected now and ready for the age of quantum computing.

QUANTUMXCHANGE

The Challenge

Security upgrades can be expensive and disruptive. Most organizations want to avoid a capital-intensive "rip and replace" scenario in favor of a gradual approach to quantum readiness, one where organizations can take incremental steps in the direction of quantum safety based on risk tolerance, specific data-security requirements, or other business drivers.

As NIST works to finalize its post-quantum cryptographic (PQC) candidate algorithms for standardization, another two to three years away, and quantum encryption struggles to overcome its complexity and expense, nefarious actors continue to harvest critical data, stockpiling it for the day when a quantum computer can easily break its encryption.

Today's IT environment begs the question: why would you not install a quantum-safe high-speed encryptor (HSE)? An ideal solution is one that integrates seamlessly into your existing crypto environment; immediately boosts your cybersecurity posture with quantum-enhanced key distribution; can easily scale quantum-protection levels in lockstep with the threat landscape and risk mitigation requirements of the organization; and is economically sound, providing an immediate return on investment.

The Solution

Phio Trusted Xchange (TX) from Quantum Xchange gives companies choice and an affordable, crypto-agile key infrastructure to easily upgrade defenses as the threat landscape evolves. It is the first key exchange to support quantum-keys in any format (PQC, QKD, QRNG or combination). Using its patent-pending, out-of-band symmetric key delivery technology, Phio TX is uniquely capable of making existing, classical keys quantum-safe – delivering an immediate and infinitely stronger cybersecurity posture to any network environment.

Phio TX used in combination with Thales HSE arms customers with a powerful and dynamic enterprise security solution and the only key distribution system capable of making native encryption keys quantum-safe today. The joint solution addresses PKE vulnerabilities head-on with quantum-enhanced keys and quantum-safe out-of-band key delivery that can easily scale to meet the risk mitigation needs of the business at any time.

The first-of-its-kind security appliance can be deployed across any network media, i.e., fiber, wireless, satellite or copper to provide quantum-safe key distribution without Quantum Key Distribution (QKD) using Phio TX. If an organization desires QKD, Phio TX is the only solution in the world capable of overcoming the technology's distance and delivery limitations, and it provides FIPS 140-2 compliance that QKD alone lacks.

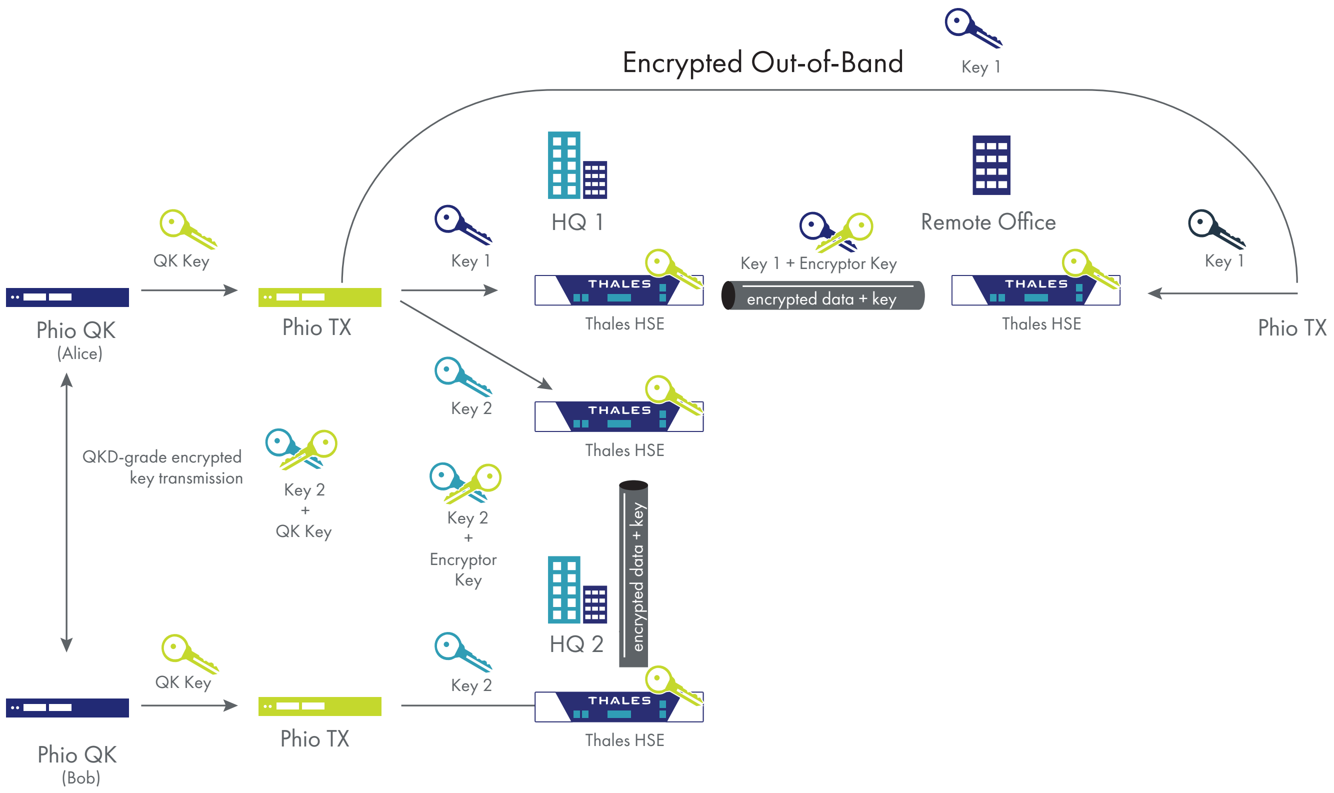
Thales Network Encryptor Family

Thales offers a range of Network Encryptors to ensure the right mix of features and capabilities tailored to your needs and budget. The products in our portfolio are fully interoperable, so a single platform can be used to centrally manage encryptors across single customer links or distributed networks. Each of the encryptors offered can support up to 512 concurrent encrypted connections. Hardware encryptors are certified for FIPS 140-2 Level 3 and Common Criteria EAL +2, EAL 4+*.

Why Use Thales HSEs with Phio TX?

Key advantages and features include:

- Extend the life of your Thales Network Encryptors by making HSE keys quantum-safe now.
- HSE in quantum-safe mode has same performance and reliability as classical mode.
- Multi-layered or defense-in-depth approach to secure key transfer protected by PQC and/or QKD in a FIPS 140-2 validated implementation.
- Avoid brute-force, side-channel, and SSL/harvesting attacks with out-of-band, quantum-safe key delivery. With Phio TX, keys are used as a key-encrypting-key (KEK) for impenetrable protection.
- Shore up risks and vulnerabilities of modern-day PKE. No data loss even if KEK is stolen – the attacker must still figure out when, where, and how it was used.
- Dramatically improve key entropy with quantum-enhanced options i.e., QKD, QRNG or combination.
- Multipath key routing, fault-tolerant and load-balanced point-to-multipoint key transmissions. Supports key transmission IPv4 or IPv6 network – copper, fiber, 4G, 5G, satellite, etc.
- Future-proof and crypto-agile key distribution system. Enables users to quickly change to any NIST PQC algorithm and provides an onramp to maximum-level QKD security if desired with no distance limitation.
- Delivers an instant and infinitely stronger, quantum-safe security posture for protecting transmitted data across communications networks and links today and in the quantum future.



How It Works – Simple Overlay Architecture

- Single Phio TX appliance supports multiple HSEs at each location
- Phio TX delivers secondary keys to HSE, used to protect native HSE key
- Phio TX keys can be secured with PQC and/or QKD if fiber is available
- Attacker cannot monitor single HSE tunnel to try to steal keys
- If secondary key is somehow stolen, no data is exposed
- Attack surface reduced from entire length of network down to the physical HSE

Thales and Quantum Xchange Can Help

Security-forward organizations that are looking to get a practical jump on quantum readiness should start preparing now. Don't know where to start? Take the Thales Post-Quantum Risk Assessment to learn if your organization is at risk of a post-quantum breach. Begin preparing for the quantum era with solutions that are available today. Contact Quantum Xchange to learn more about Phio TX at info@quantumxc.com. To learn more about Thales High-Speed Encryption advantages contact Thales at sales@thalessec.com.

About Quantum Xchange

Quantum Xchange gives commercial enterprises and government agencies the ultimate solution for secure communications and protecting data in motion. Its complete key distribution system, Phio Trusted Xchange (TX), is uniquely capable of making existing encryption keys quantum safe and supports both post-quantum crypto (PQC) and Quantum Key Distribution (QKD) for true crypto agility and quantum readiness. With a dynamic security infrastructure in place, organizations can enhance their existing encryption environment, select the level of protection needed based on their risk tolerance, and if desired seamlessly scale to QKD at any time, across any distance, between multiple transmission points. To learn more about being quantum-safe today and quantum-ready for tomorrow's threats, visit QuantumXC.com or follow us on Twitter @Quantum_Xchange.

About Thales

The people you reply 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.

> cpl.thalesgroup.com <

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