cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Luna Post-Quantum Crypto (PQC) Functionality Module (FM)

Starting Your Quantum-Safe Crypto Agility Transformation with Luna Hardware Security Modules (HSMs)

The Problem

Our modern, digital world depends on Public Key Infrastructure (PKI) to establish and ensure trust, particularly in IT areas such as:

- Code signing technology that guarantees software and firmware integrity and authenticity;
- Document signing technology that guarantees non reputability;
- Major internet communication protocols such as TLS, IPSEC, S/MIME;
- Information rights management solutions

However, the nature of technology is that newer technologies are constantly being invented, each one having an impact, large or small. Quantum computing is one of those new technologies currently under development, and it will be able to break the security of all current public key cryptography used today. It could also weaken the current strength of symmetric cryptography, requiring the use of longer keys.

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. Devices already put into customer's hands for use will be vulnerable to malware attacks and an individuals' digital identity associated with that device, essential to modern day-to-day interactions, will also be at risk.

Challenges:

1. Crypto agile transformation takes significant time

For organizations, updating their cryptographic mechanisms is a long process that needs to be carefully prepared and validated along the way. As an example, one can refer to the difficulties of deprecating the use of DES, SHA-1 or RSA 1024 bits keys. Organizations need to make sure the new Post-Quantum mechanisms will be supported by every key infrastructure component. Furthermore, the larger the organization, the more complex their infrastructure usually is with data residing in different locations or in hybrid environments of cloud and on-premises that complicates the upgrade process. To mitigate this challenge, it is essential to start testing the deployment of these new mechanisms as soon as possible to be ready before the quantum day. Having a crypto agile strategy in place now will prepare an organization to pivot faster and securely when it is needed.

2. Protecting connected devices

It is critical to protect connected devices, both now and in the future, using standardized quantum-safe security measures. While securing connected devices requires a multi-faceted approach, one important measure for robust security is to embed a root of trust which requires storing the keys within a tamper-resistant HSM.

Today, asymmetric algorithms, such as RSA or ECC, are used for digital signatures which are vulnerable to the quantum threat. Fortunately, quantum-safe replacements exist today but they present new, yet manageable, implementation challenges that need to be considered.

The solution

The Luna HSM Post-Quantum Crypto FM allows for use of the round 3 NIST finalists quantum-safe crypto mechanisms to be used today for use cases such as code-signing or others that rely on PKI. The PQC FM can be installed on both your PCIe and Network HSM without having to make any hardware changes or upgrades. It includes key management capabilities for both stateless and stateful key types, complying with SP 800-208 requirements.

Key benefits

- Deploy PQ safe code signing to protect your high value devices today with confidence they'll be safeguarded from the quantum threat, without requiring costly recalls and physical updates in the future
- Benefit from tamper-resistant HSMs to securely create and manage quantum-resistant keys
- Generate digital signatures seamlessly using standardized quantum-safe public key cryptography, both stateful hash-based signatures and stateless
- Validate your crypto agility by setting up quantum safe PKI, TLS, or VPN with a wide variety of Thales technology partners

Stronger together: start validating your crypto agility today

We are working with public and private partners to validate the introduction of quantum safe cryptography and quantum safe protocols and standards. As part of Thales' commitment to ensuring our products function optimally in today's modern world, we are validating the integration of the Thales Luna Post-Quantum Crypto FM with our key partners.

The Luna HSM PQC FM enables you to:

- Future-proof and standardize quantum-safe digital signature algorithms for all your long-lived devices today, to ensure you can deliver secure and authenticated software/ firmware updates far into the future:
    - Use stateful hash-based signatures standardized by the IETF, such as HSS (Hierarchical Signature System) IETF RFC 8554, and XMSS (eXtended Merkle Signature System) IETF RFC 8391
    - Both HSS and XMSS have been standardized by the IETF and approved by NIST under SP 800-208 and recommended by the NSA (CNSA 2.0) that provide crypto agility in the face of quantum threats for identity use cases such as document and code signing
- Validate stateless quantum safe crypto mechanisms standardized by NIST that provide quantum safe mechanisms for key exchange, encryption, and digital signature:
    - Falcon, SPHINCS+, Crystal-Kyber, Crystal-Dilithium

Free Post-Quantum Crypto Agility Risk Assessment Tool

Use our free Post-Quantum Crypto Agility Risk Assessment Tool which will help you have a better understanding of whether your organization is at risk of a post-quantum breach, learn about the scope of work required, and what you should be doing today to be post-quantum ready.

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.