Solution Brief

Securing QKD-HSM connectivity by pQCee and Thales

Combining Quantum-Secure Key Exchange with FIPS-140-3 Secured Key Management

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

pQCee
Be . Quantum . Ready

With the impending arrival of quantum computers, applications need an easy and reliable way to be upgraded with quantum-secure cryptographic keys and protocols to ensure that digital communication remains protected against quantum attacks.

The Challenge

The use of secret keys is very important for modern day digital communications and data protection. Quantum Key Distribution (QKD) provides applications with the means to generate and exchange quantum-safe keys amongst communicating parties to protect against eavesdropping or data tampering attacks. The challenge is how to integrate QKD infrastructures into existing application workflows with seamless interoperability and zero disruption to business operations.

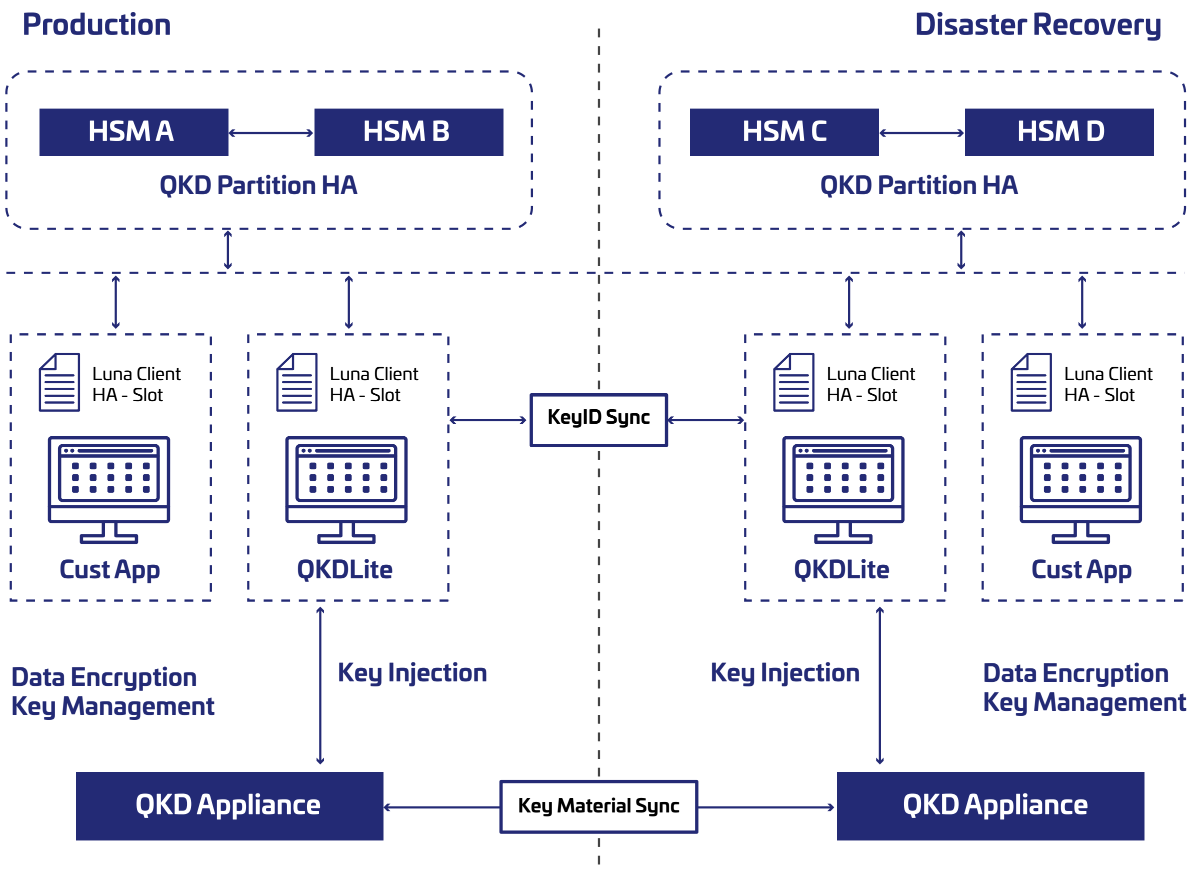
The Solution – QKDLite and Luna HSM for Quantum connectivity

Thales and pCQee have partnered to help customers address the quantum computing challenge by combining QKDLite with Thales Luna HSMs; organizations can quickly start to use quantum technologies to enhance the security of their applications while retaining much of their existing workflow processes. The following are some of the possible customer applications using QKDLite with Luna HSMs for Quantum connectivity:

- **PPK for RFC 8784 IPSEC VPNs**
  Virtual Private Networks (VPNs) are used to create encrypted communication tunnels between two locations. To make VPNs quantum-safe, the RFC 8784 standard stipulates that the key exchange mechanism must be enhanced with an additional Post-quantum Pre-shared Key (PPK) which can be made seamless with the QKDLite-HSM package.

QKDLite

QKDLite, by pQCee, is a set of middleware modules that are designed for businesses to connect easily and securely to QKD infrastructures with minimal changes to the applications. It abstracts away the protocol complexities for integrating with technical standards such as ETSI QKD 014, PKCS#11, RFC 8784, FIPS 197, and PCI-DSS to present a unified interface that focuses on secure key generation and management.



Solution Features

Certified Key Storage

Thales Luna Network Hardware Security Module (HSM) is a high-assurance, tamper-resistant, network-attached appliance that accelerates cryptographic operations, secures the crypto key lifecycle, and provides a root of trust for the entire encryption infrastructure. Luna HSMs are certified for FIPS 140-2 Level 3 and Common Criteria EAL +2 and EAL 4+. Rely on Luna HSMs as the market-leading crypto agile foundation of digital trust to reduce risk, ensure flexibility, easily manage keys, and simplify integrations.

Quantum-Generated Secrets

Current random number generation is deterministic based on pseudo-random number generators. This may not be sufficient for high-value applications which require true and unbiased random number generation that is secure against quantum attacks, QKDLite will provide an easy and seamless way for such applications to gain access to quantum entropy sources offered by QKD infrastructures.

About pQCee

pQCee.com is a quantum cybersecurity startup that designs and builds post-quantum products and solutions to strengthen and protect the next generation of computing against quantum attacks. Please contact info@pqcee.com for more offerings.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Key Benefits

- Use Quantum-Secure keys to strengthen your data security
- Extend the functionality of Hardware Security Modules (HSM) with new quantum use cases
- Zero disruption to business operations
- Provide seamless interoperability with existing Key Management processes
- Offer standards-based integration
- Deploy without changing existing architecture
- Agile range of encryption methods offered with different assurance levels

cpl.thalesgroup.com

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