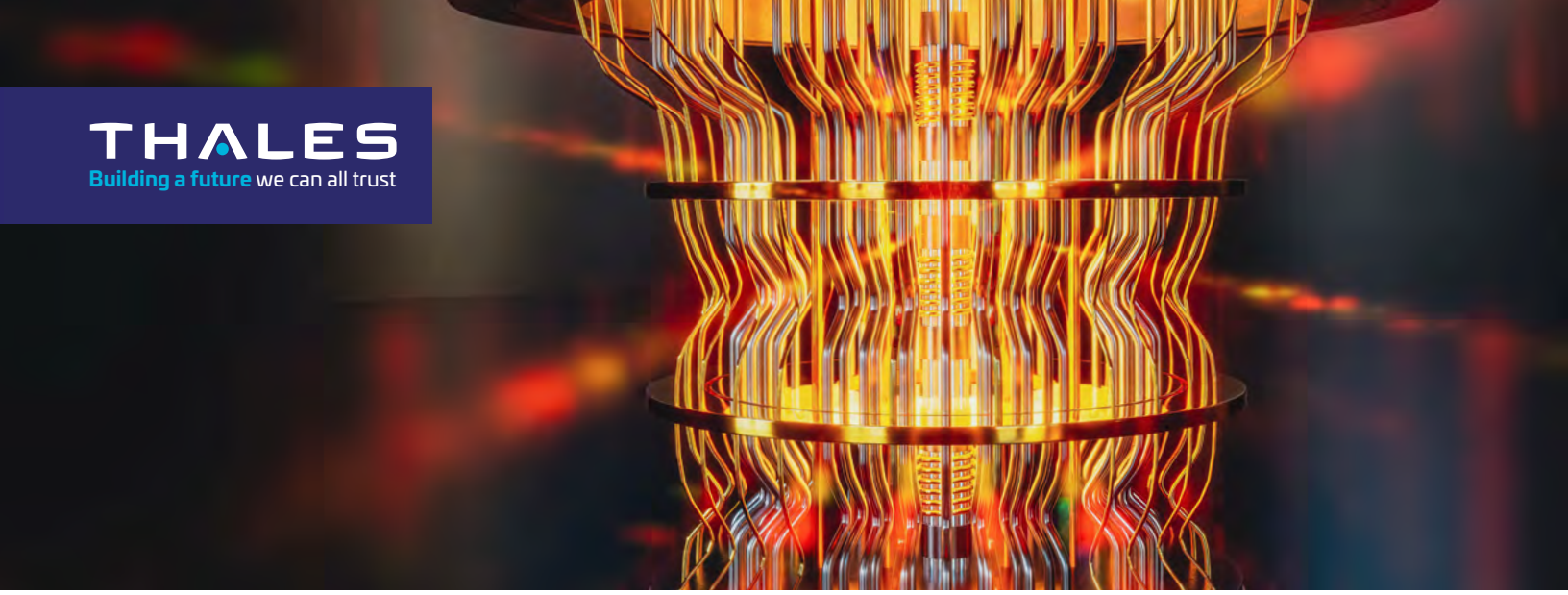
Case Study

Thales Luna HSMs and Quantinuum for Financial Service Company

Leading Financial Services Company Develops Quantum-Safe Cryptography Solution with Thales

cpl.thalesgroup.com

THALES
Building a future we can all trust



As quantum computing gets considerably closer to viable commercial use, standard public key cryptography will face significant security challenges. Some of today's current algorithms could likely be hacked within hours or even minutes on a quantum computing platform. For this reason, to ensure the longevity of data security, many businesses are leveraging Post-Quantum Cryptography (PQC) solutions to build resilience and crypto-agility. While adopting these quantum-safe algorithms and processes provides organizations with steadfast data protection even against ever-evolving future threats many are intimidated but what seems like a potentially effort-intensive process and costly retrofit.

The challenge

A multinational financial services company sought to proactively formulate strategic and robust technical solutions so that the data, systems, and applications their customers rely upon can remain safe.

They wanted to establish PQC-ready security measures in their banking and innovation workflows using provably secure key generation to protect against data harvesting threats. With legacy hardware, system-wide applications, related certificates, and solutions from multiple vendors – any new solution they selected had to easily integrate into their existing IT environment with minimal disruptions to daily operations. Exploring their options, this team wanted to develop a scalable and agile PQC approach that could work across the entire enterprise.

The solution

The customer, Quantinuum, and Thales partnered together to collaboratively develop a quantum-safe commercial solution for secure key generation, management, and protection.

Quantinuum offers the ability to generate highly unpredictable keys with its Quantum Origin solution which leverages quantum-computing-strengthened entropy. In cryptography, entropy is leveraged for random number generation, the foundation for strong keys. Powered by a quantum computer, this platform provides a high-quality inherent randomness for secure key generation. Companies like this leading financial services company can generate quantum-resilient cryptographic keys on-demand based on a mathematically verifiable process that exceeds typical industry standards, resulting in a security uplift when compared to keys issued with true random number generators (TRNGs) and first-generation quantum random number generators (QRNGs).

To protect the keys both physically and logically, Thales Luna Hardware Security Modules (HSMs) are leveraged. Luna HSMs serve as the foundation of digital trust, enabling crypto agile flexibility, today and into a PQC future. Luna HSM customers benefit from its agility, usability, and scalability, purposely designed to provide a balance of security and high performance for both traditional and emerging technologies and can be deployed on-premises, in the cloud, or across hybrid environments. Luna HSMs provide the highest level of security by always storing cryptographic keys in hardware. They provide a secure crypto foundation as the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance. Since all cryptographic operations occur within the HSM, strong access controls prevent unauthorized users from accessing sensitive cryptographic material.

To further fortify against quantum threats, Quantum Origin integrates seamlessly within the Thales Luna HSM. The Quantum Origin platform seeds its Quantum-enhanced entropy into the Luna HSM's existing Deterministic Random Bit Generator (DRBG). This integration enables the generation of quantum-computing hardened cryptographic keys directly from Thales Luna 7 HSM.

The result

This Quantum-safe solution allows the customer to generate quantum-safe encryption keys that are strongly generated, securely stored, and deployed at-scale across a large IT infrastructure with minimal disturbances to existing procedures.

Leveraging this solution from Quantinuum and Thales, this customer benefits from the ability to generate quantum-safe asymmetric keys within a FIPS 140-2 level 3 certified appliance.

Importantly, this leading financial services company showcases how it's possible to prepare for a PQC world by developing crypto agile quantum-safe protections for existing and evolving infrastructures. In parallel, the customer is also working with Thales and Quantinuum on securing its networks for data-in-motion encryption. Leveraging a crypto agile solution today ensures that they can avoid an expensive security retrofit down the line as standards for quantum-safe protection become finalized.

Conclusion

Quantum computing poses significant data security risks. To protect against these emerging threats and ensure that the systems their customers rely on will remain safe today and into the future, this leading financial services company has established a PQC strategy to ensure crypto- agility for legacy and post-quantum cryptographic (PQC) algorithms, leveraging solutions from both Quantinuum and Thales. Together, Thales and Quantinuum can help organizations build sustainable quantum resilience, to protect their business against ever-evolving quantum computing cybersecurity threats.

Quantinuum

Quantinuum is the world's largest quantum computing company, formed by the combination of Honeywell Quantum Solutions' world-leading hardware and Cambridge Quantum's class leading middleware and applications. Science led and enterprise driven, Quantinuum accelerates quantum computing and the development of applications across chemistry, cybersecurity, finance, and optimization. Its focus is to create scalable and commercial quantum solutions to solve the world's most pressing problems, in fields such as energy, logistics, climate change, and health.

About Thales

Today's enterprises depend on the cloud, data, and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

We are the worldwide leader in data protection, providing everything an organization needs to protect and manage its data, identities and intellectual property – through encryption, advanced key management, tokenization, and authentication and access management. Whether it's securing the cloud, digital payments, blockchain or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales Cloud Protection & Licensing is part of Thales Group.

For more information visit https://cpl.thalesgroup.com/about-us or follow @ThalesCloudSec on Twitter.