QUANTINUUM

Quantum Origin and Thales Luna 7 HSM Solution Brief

Seamlessly bolt-on quantum-computing-hardened encryption keys in the cloud, on-premises, or across hybrid platforms

March 2023

Summary

Enterprises of many sizes across all industries rely on secure cryptographic technologies and methodologies to protect their customers and themselves from sophisticated cybersecurity vulnerabilities. Cryptographic algorithms rely on the unpredictability of the secret keys used, which should be derived from a high-quality source to remain unpredictable.

Traditional key generation processes depend upon random number generators which are known to be deterministic, creating a vulnerability that could compromise the security guarantees and unpredictability of the keys. As cryptographically relevant quantum computers (CRQCs) gradually enter the commercial and research landscapes, addressing this problem will become critical to reduce the impact of encryption-based attacks by sophisticated threat actors.

Quantinuum's patented cybersecurity solution, Quantum Origin, enables enterprises to address these challenges. Quantum Origin is a unique solution that generates quantum-computing-hardened cryptographic keys from a unique quantum-computer generated seed. As the only solution of its kind, Quantum Origin uses a verifiable process to generate keys that go beyond typical industry standards, producing the strongest cryptographic keys in the market.

Integrating Quantum Origin with Thales Luna 7 Hardware security modules (HSMs) enables organisations to leverage a trusted platform to manage and scale quantum-computing-hardened key generation, minimising the impact of advanced encryption-based cyber-attacks on their most valuable data and systems.

The Challenge

As cyber threats continue to advance, traditional encryption methods are becoming less effective. Cybersecurity and risk management leaders must implement measures to build stronger resilience. Although CRQCs cannot yet overcome conventional encryption protocols, the quantum era is underway and governing bodies are already demanding that enterprises build appropriate resilience. Enterprises can start embracing quantum-enhanced solutions that harden their security foundations today.

Security providers should begin choosing products and services to meet the increasing customer and regulatory need to strengthen resilience, whether in the cloud, on-premises or in hybrid environments. As customer data is only as secure as the encryption keys used for protection, it has become increasingly important to use best-in-class encryption keys, especially since sensitive customer data tends to have long-retention requirements.

The unpredictability of an encryption key is important for protecting the confidentiality and integrity of data in transit and at rest. Unfortunately, traditional key generation measures have proven to be vulnerable to advanced attacks in the past. For instance, the NIST Dual Elliptic Curve Deterministic Random Bit Generator contained weaknesses that led to significant cyber-attacks.[1]

Enterprises that hold sensitive data with long shelf lives must ensure their security measures offer the highest protection against today's threats and emerging threats. Proactively implementing

[1] "Dual EC DRBG." Wikipedia, Wikimedia Foundation, 18 July 2022, https://en.wikipedia.org/wiki/Dual_EC_DRBG

© 2022 by Quantinuum. All rights reserved.

technologies to safeguard valuable data and systems creates resilience and builds trust with customers, partners, and compliance bodies.

The Solution

Quantinuum and Thales deliver a seamless plug-and-play integration that enables organizations to generate, store, and manage quantum-computing-hardened cryptographic keys. This collaboration combines the innovation behind Quantum Origin with the high-level security assurances provided by the Thales Luna 7 HSMs, a proven leader in the market.

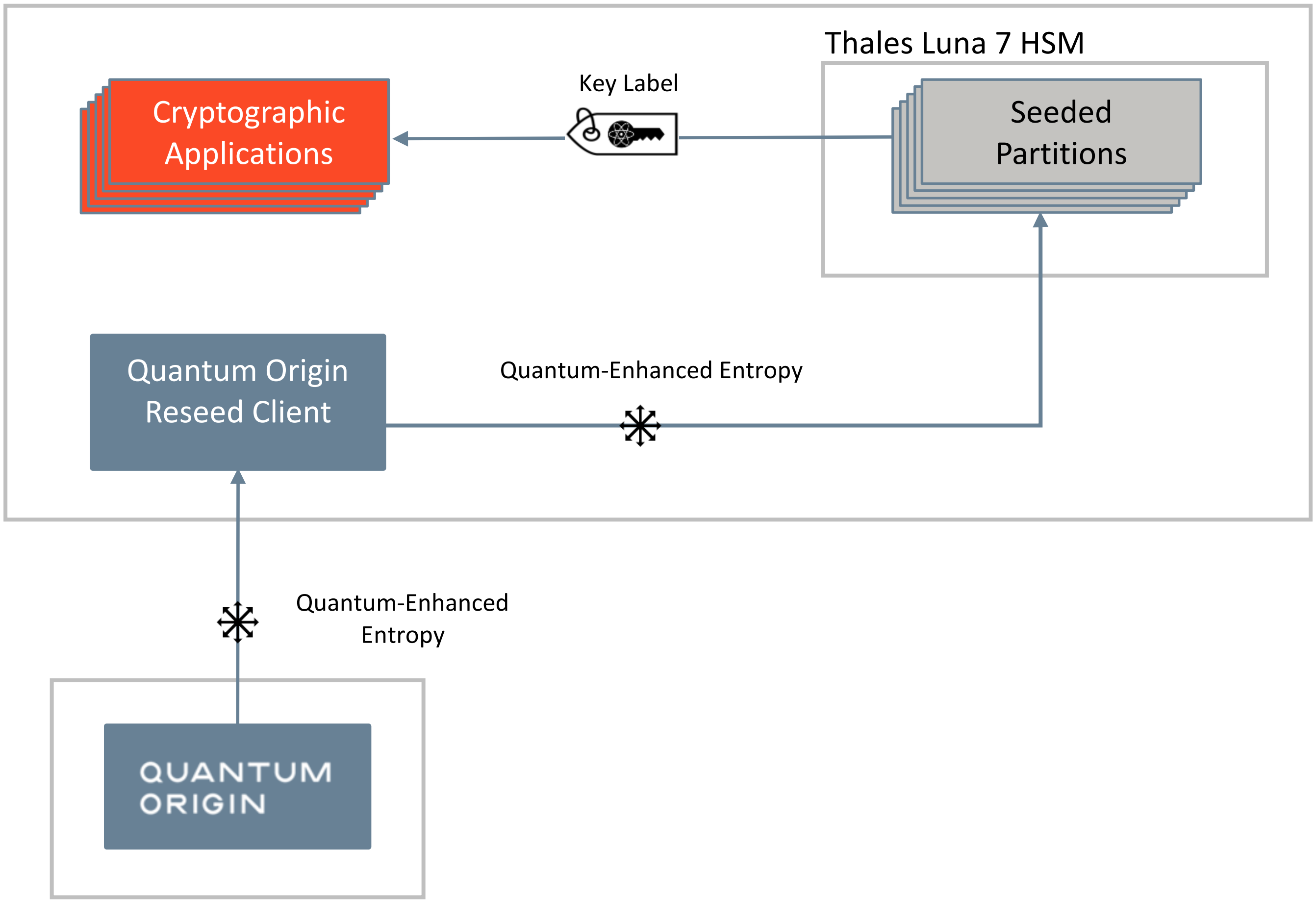
Quantum Origin generates the only quantum-computing-hardened cryptographic keys in the market using Quantinuum's in-house quantum computer. Not only does the platform generate unpredictable cryptographic keys that help resist advanced cyber-attacks, but it also provides organisations with the assurance of the unpredictability of keys through the industry's only mathematical verification process. This unique process delivers the confidence of an enhanced security strength when compared to true random number generators (TRNGs) and quantum random number generators (QRNGs). The product has been deployed by companies in industries ranging from energy to cybersecurity, and across use cases such as network security and public key infrastructure.

Quantum Origin integrates into the Thales Luna 7 HSM through the Reseed Client, a software application deployed within an organisation's secure environment. The client injects quantum-enhanced entropy from Quantum Origin directly into the Luna 7 HSM's deterministic random bit generator. The quantum-computing-hardened entropy is mixed with the HSM's onboard entropy to generate the strongest cryptographic keys in the market. This architecture allows organisations to enhance cryptographic key strength without altering existing infrastructure or impacting compliance with FIPS 140-3.

This collaboration brings the expertise of two leading players across critical security domains together into one device without the need for changes to code, infrastructure, or applications.

© 2022 by Quantinuum. All rights reserved.

Quantum Origin - Thales Luna 7 HSM Integration Architecture



Solution Benefits

Strengthened Resilience: Organisations can generate, store, and manage quantum-computing-hardened cryptographic keys, strengthening foundational data protection measures without compromising performance at scale in production environments.

Proven Assurance: Organisations can be certain that cryptographic keys used in production have been mathematically verified for quality and unpredictability, which is a benefit no existing random number generation methods such as TRNGs and QRNGs can deliver.

System-agnostic Implementation: Quantum Origin interfaces with the Thales Luna 7 HSM using a Reseed Client developed by Quantinuum so that organisations do not need to change their existing architecture.

Future-proof Resilience: Cryptographic keys, both classical and post-quantum, generated by the enhanced Thales Luna 7 HSM will remain unpredictable even as quantum machines become more powerful.

© 2022 by Quantinuum. All rights reserved.