SOLUTION BRIEF

Quside Entropy Module for Thales HSMs

Delivering Observable Quantum Entropy

The Current Landscape

As the volume of data increases exponentially, digital assets must be secured to ensure the integrity and confidentiality of the data. As the most used cryptographic algorithms today are standardized and open for public review, the foundation of modern digital security systems lies in the quality of the cryptographic keys used to encrypt and decrypt data. If these keys are compromised, then the entire foundation of security, and the organization, are at risk.
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 current entropy provision is such that it cannot be reliably monitored and depends on statistical batteries of tests to ascertain its suitability. NIST has stated that the use of such statistical tools as set out in SP800-20 should not be used for testing entropy and randomness for use in cryptography.

The Challenge

Entropy -– the Core Foundation

How can you ascertain if you are using quality entropy? How do you know if you have enough quality entropy? Quside offers real-time updates on the quality of generated entropy using physics-based techniques, offering actionable insights for CISOs, Security Operations Managers and Security Professionals.

Entropy starvation

Consider entropy to refer to the quality and source of random data that is available to an instance. Cryptographic technologies typically rely heavily on randomness, requiring a high-quality pool of entropy to draw from. It is typically hard for a machine to get enough entropy to support these operations, which is referred to as entropy starvation. Entropy starvation affects the quality and robustness of generated security keys used in PKI making applications vulnerable as shown in various breaches (links). Quside Quantum Entropy sources overcome this limitation by providing high-rate, continuously monitored random numbers.

Zero Trust Architectures / Zero Trust Network Access

To achieve true zero trust there can be no part of a security ecosystem that has to be trusted. Quside has taken a proven approach to reliably monitor and test the entropy provision in real time. We can therefore provide the only solution that can meet this requirement today.

The Solution

Quside offers an advanced patented QRNG (Quantum Random Number Generation) solution to meet the increasing demand for high-quality entropy in cryptography, including upcoming

PQC standards. Quside's latest generation PCIe One is capable of 1 Gb/s raw randomness generation from a single quantum entropy source chip producing over 90% quantum min-entropy bounds.

Quside's distinctive offering lies in its assurance of randomness, achieved through vigilant monitoring of the quantum signal source.

Working with the Thales HSM product, we offer a fully integrated solution that can sit inside or alongside your HSM device that you fully control, manage and monitor. Through local monitoring and assurance, no third party needs to be trusted in the process of entropy generation.

Start validating your crypto agility today

Quside alongside Thales are working in partnership with public and private partners to validate the introduction of quantum safe cryptography, quantum safe protocols, advanced randomness generation and entropy monitoring. This provides for the validation of the integration of the Thales Luna Post-Quantum Crypto FM and standard cryptographic libraries with Quside Quantum Entropy Sources.

The Quside and Thales HSM integration enables you to:

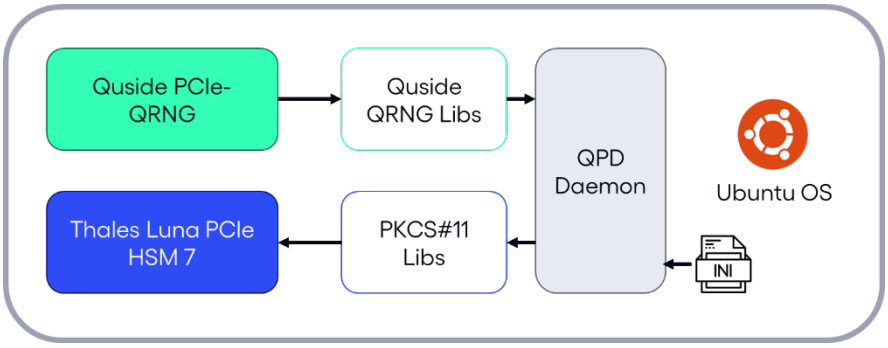
Future-proof and standardize quantum entropy source for all cryptographic algorithms on all your long-lived devices today, to ensure you can deliver secure PKI infrastructure:

- 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, including:

- Falcon, SPHINCS+, Crystal-Kyber, Crystal-Dilithium.

In addition to signature and other quantum-safe algorithms, embed also a high-rate source of randomness with continuous entropy monitoring capabilities.



Thanks for joining us on the quantum side!

To learn more about our products visit www.quside.com and contact sales@quside.com