Trusted Cyber Technologies

THALES
Building a future we can all trust

Quantum Enhanced Keys

HSM-Provided Quantum Entropy

As the volume of data increases exponentially, digital assets must be secured in order to ensure the integrity and confidentiality of the data. As the most commonly used crypto 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 ultimately the organization, are at risk.

The most secure cryptographic keys are generated using random number generators. ID Quantique's Quantis Quantum Random Number Generator (QRNG) chip on board Thales Trusted Cyber Technologies' (TCT) high-assurance Luna T-Series Hardware Security Modules (HSMs) generates unique and truly random numbers in order to secure an organization's cryptographic infrastructure.

This high entropy and secure key storage solution addresses critical applications where high quality random numbers are absolutely vital such as: cryptographic services; numerical simulations; cloud; compliance; IoT-scale device authentication; and trusted digital signatures.

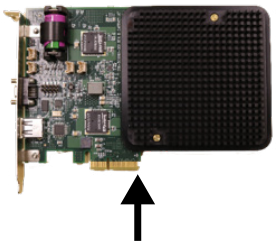
ID Quantique Quantis QRNG Chip

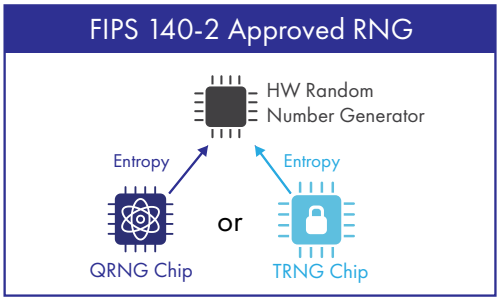
The Quantis QRNG chip embedded in Thales TCT's Luna T-Series HSMs securely generates and delivers high quality random numbers (entropy) for use by the Luna HSM cryptographic module. At its core, the QRNG chip contains a light-emitting diode (LED) and an image sensor. Due to quantum noise, the LED emits a random number of photons, which are captured and counted by the image sensor's pixels, giving a series of raw random numbers that can utilized by the HSM.

Integration Within a FIPS 140 Cryptographic Module

Due to the strict NIST FIPS 140-2 requirements and standards related to entropy and random number generation, a standalone QRNG chip must be integrated with a FIPS-approved Random Number Generator (RNG) method in order to achieve FIPS 140-2 certification. The Thales TCT T7 Cryptographic Module used in all T-Series Luna HSMs is believed to be the industry's first FIPS 140-2 certified crypto module to include a QRNG entropy source within its cryptographic boundary. Using the entropy produced by either the Quantis QRNG chip or an onboard True RNG (TRNG) chip to seed a hardware based RNG, the integrated solution meets the FIPS 140 requirements for entropy quality while complying with the NIST SP 800-90A requirements for random number generation.

Thales TCT
Luna T-Series HSM





Quantum Enhanced Keys

By embedding the Quantis QRNG chip within the Luna T-Series HSM, Thales TCT offers a FIPS 140-2 Level 3 compliant HSM capable of generating Quantum Enhanced Keys. The QRNG chip produces high quality entropy which is the basis for all random numbers and cryptographic keys generated by the HSM. Regardless of how an application makes use of the HSM, all keys and random numbers generated within the HSM are enhanced by the security of the quantum random numbers that are the foundation of the key generation process.

Crypto-Agility

Use of Quantum Enhanced Keys is part of an overarching strategy of using crypto-agile products like the Luna T-Series HSM to combat emerging technical threats as the age of the quantum computer looms. Organizations must remain vigilant in this changing cybersecurity landscape by ensuring that their selected cryptographic platform supports both today's standards-based algorithms and future-developed quantum resistant algorithms.

Luna T-Series HSMs support a wide range of algorithms and provide the flexibility to quickly react to cryptographic threats by implementing alternative methods of random number generation, key generation, and encryption. In addition to implementing dual entropy sources, the HSM's crypto agile architecture supports in-field introduction of new crypto algorithms. Large amounts of memory (inside the crypto module) support growth to larger key sizes and CPU capabilities support new, compute intensive algorithms and features.

About ID Quantique

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organizations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries – such as security, encryption, critical infrastructure and IoT- where trust is paramount.

Additionally, IDQ is a leading provider of optical instrumentation products, most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com