Q→NU
Proactively
Quantum™

SOLUTION BRIEF

Secure and High Entropy Key Protection and Cryptographic Operations Backed by Quantum Randomness

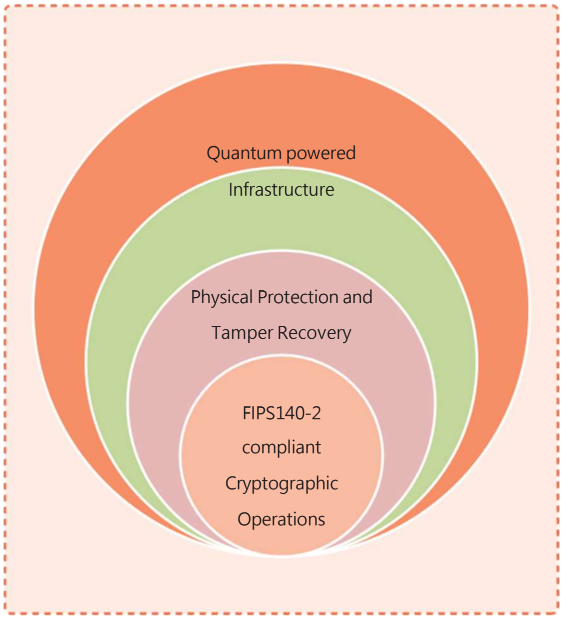
QNu Labs Tropos QRNG (Quantum Random Number Generator) and Thales Luna HSMs (Hardware Security Module)

Customer Need

Nearly all secure online traffic and digital assets - from shopping to banking to communications to healthcare - relies on a technique of randomly generating a number that serves as a key to encrypt communication/digital asset. Digital cryptography relies greatly on randomness in providing the security requirements imposed by various information systems. Just as different requirements call for specific cryptographic techniques, randomness takes upon a variety of roles in order to ensure the proper strength of these cryptographic primitives. Unfortunately, some of today' s most commonly used sources of "random" data depend on inputs that have the potential to inject predictable data, and therefore weakness, into the process. Low-entropy data sources produce encryption keys that can be attacked much more easily than a truly random key. Even high-performance pseudorandom number generators that have been certified as "cryptographically secure" may prove to be insufficiently random once large-scale quantum computers become available. If compromised, then the entire foundation of security, and ultimately the enterprise, are at risk.

Seeding Thales Luna Network Hardware Security Module (HSM) with QNu Labs Quantum Random Number Generator (Tropos QNRG) provides a quantum secure method for cryptographic operations and for generating high strength keys. This high entropy, secure key storage and generation solution addresses critical applications where high-quality random numbers are absolutely vital such as: cryptographic services; OTP generation, tokenization, numerical simulations; cloud; compliance; gaming and lotteries; IoT-scale device authentication, IAM and managed end-to- end encryption.

VERIFIED SOLUTION
THALES



Challenge: Deficiencies and shortcomings of current TRNGs (True Random Number Generator) and PRNGs (Pseudorandom Number Generator)

Physical RNGs produce data at unacceptably low throughput (number of bits generated per second) due to limitations in the phenomena being measured. Organizations relying on these devices must compromise on either the level of entropy in their data or the speed at which cryptographic functions can be completed, either one of which can put sensitive information at risk.

Pseudorandom number generators that depend on system information as an entropy source can encounter performance issues during and shortly after the device has started up, when system activity is relatively predictable and user activity is lower than normal. PRNGs running on virtual machines face an even greater challenge, as they often lack direct access to information on the system activity or user interactions that could be used to populate their entropy pool. Furthermore, if PRNGs are running on multiple machines, images that were created with the same initial state, they are likely to produce identical output. In addition, PRNGs suffer from the limitations such as deterministic design, potential for hidden defect, implementation issues and vulnerability to compromise (The Dual_EC_DRBG algorithm, for example, was in widespread use until 2014, when it was removed from NIST guidance due to a backdoor reportedly inserted by the NSA).

Solution:

Tropos - Quantum Random Number Generator (QRNG) measures unpredictable quantum phenomena to generate truly random data. As quantum phenomena are random by definition, the data generated by a QRNG has full entropy and cannot be predicted by any means

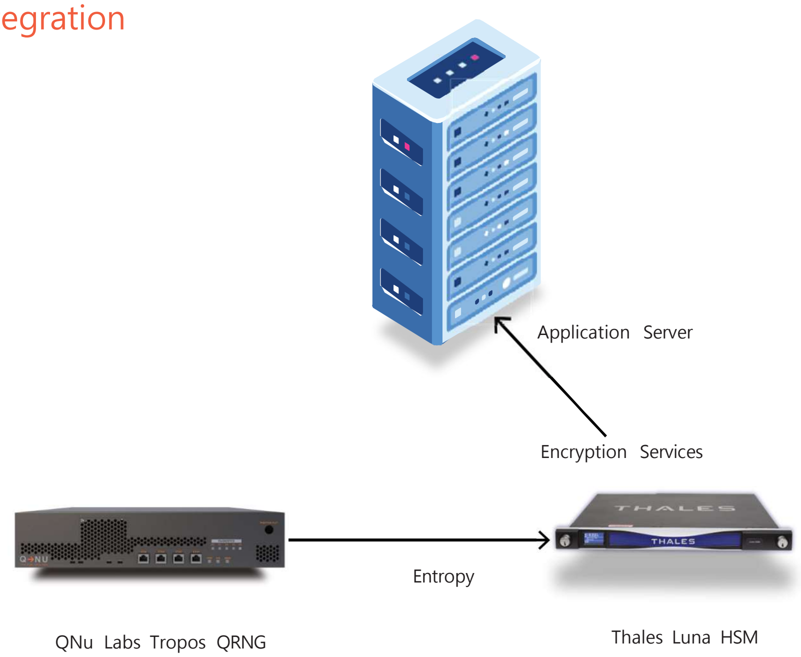
— High entropy secured quantum-powered solution

— FIPS 140-2-validated hardware

— Utilisation of two non-correlated randomness sources (Thales’ s Luna HSM RNG and QNu’ s Tropos QRNG) for stronger key generation and cryptographic operation

The operation of Tropos is continuously monitored and if a failure is detected the random bit stream is immediately disabled. In addition, Tropos provides full entropy (randomness) instantaneously from the very first bit.

Tropos – Luna HSM Integration



The Luna HSM and Tropos are linked across a Local Area Network (LAN), generating and delivering high quality random numbers for cryptographic applications across all industries. Tropos generates a continuous stream of random bits at

100Mbps which is fed to Luna HSM at a chosen rate of random numbers. The Luna HSM, using the quantum random source, generates and stores key material in a tamper-resistant FIPS-validated hardware root of trust and performs crypto operations.

Highlight of QNu Labs Tropos QRNG:

— Trusted source of quantum randomness providing extremely high rate of entropy

— Operation is continuously monitored, if failure is detected the random stream is immediately disabled

— Inexhaustible entropy at high throughput

— Simple, web-based configuration and management

— Best in class of random number generators

— The source of randomness is derived from the time of arrival of the photons, which is a true quantum phenomenon. We can extract 16 bits of entropy from the time of arrival of one photon, which is a benchmark for this method. This gives an edge on the throughput of Tropos QRNG in comparison to the other PRNGs/TRNGs.

About QNu Labs

QuNu Labs Private Limited (QNu Labs) is a leader in developing quantum cryptography based products and solutions; Founded in 2016, through an incubator at Indian Institute of Technology-Madras, QNu Labs now based out of Bangalore provides quantum safe data encryption, secure key generation and distribution solutions to the financial industry, telecom service providers, large and medium enterprises, defense and government organizations worldwide to protect their assets from current vulnerabilities and future attacks.

Q→NU

Proactively Quantum™

Indeterministic input driving unpredictability

Uniform distribution of the bits in sequence

Lack of patterns in the sequence

Perfect Random Keys

High Rate of Entropy

High Throughput Key Rates

Multiple Application Usage

qnulabs.com

sales@qnulabs.com