SOLUTION BRIEF

High-Assurance Key Protection Backed by Quantum Randomness

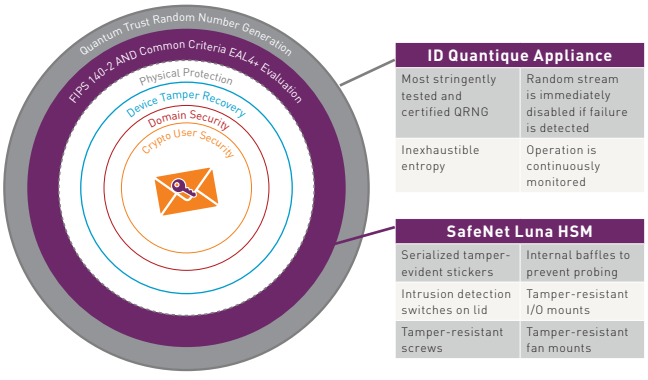
Trusted Quantum RNG from ID Quantique and Gemalto HSMs

With the continuously increasing rise in digital data, securing digital assets is more vital than ever in order to ensure its integrity and confidentiality. 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 encryption keys. If compromised, then the entire foundation of security, and ultimately the enterprise, are at risk.

Generating unique and truly random numbers with ID Quantique's Quantis Quantum Random Number Generator (QNRG) appliance, together with Gemalto's SafeNet Luna Network Hardware Security Module (HSM) high-assurance key protection appliances, is a powerful combination to securing an enterprise. 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; gaming; and IoT-scale device authentication and managed end-to-end encryption.

Why Strong, Secure Quantum Random Number Generation?

A true random number is a number generated by a process whose outcome is unpredictable, and which cannot be subsequently reliably reproduced. The only way to produce true randomness is by understanding and validating the physical process by which that randomness was produced. In other words, randomness can only be based on physical phenomena. Since quantum physics is intrinsically random, it is logical to use it as a source of true randomness.



Trusted Quantum RNG Multi-Layered Security

Trusted Quantum:

- Best cryptographic practices mixing two non-correlated randomness sources for stronger keys
- Secure quantum-powered solution with market-leading HSMs and QRNG
- Multi-layered approach to HSM security with FIPS 140-2-validated hardware
- Higher resistance to brute force attacks with an additional layer of quantum-level RNG security
- Meet wider compliance requirements (FIPS/AIS31 level TPG.3-validated randomness)

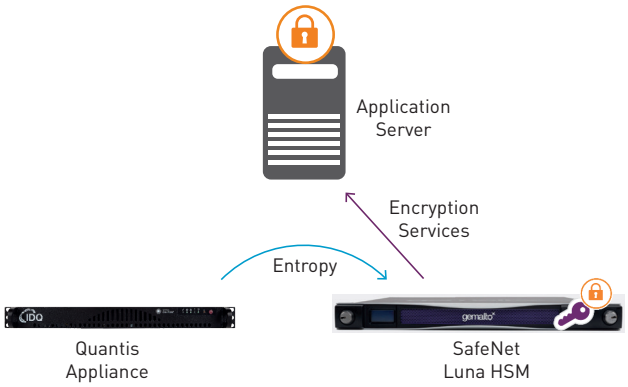
ID Quantique QRNG for Networked and Security Applications

The Quantis appliance is a network-attached device, which securely generates and delivers high quality random numbers for cryptographic applications in enterprise, government, academic, gaming and cloud environments.

QRNGs are invulnerable to environmental perturbations and of allowing live status verification. The operation of the Quantis QRNG is continuously monitored and if a failure is detected the random bit stream is immediately disabled. In addition, the Quantis appliance provides full entropy (randomness) instantaneously from the very first bit.

High-Assurance Key Generation and Protection with SafeNet Luna HSMs

Organizations that require a high level of assurance can protect their cryptographic keys in FIPS 140-2 Level 3 certified SafeNet Luna Network HSMs - tamper-resistant, network-attached appliances. Gemalto's keys-in-hardware approach ensures your key are securely generated in hardware, and always remain centrally and securely stored, free from rogue administrators and hackers. Additionally, SafeNet Luna HSM scalability enables you to meet performance and availability requirements, regardless of the size of your deployment.



Quantis Appliance seeding random numbers to SafeNet Luna HSM

How the Solution Works

The Luna HSM and Quantis Appliance are linked across a Local Area Network (LAN), where after:

- ID Quantique enables direct seeding of the SafeNet Luna HSM with strong quantum entropy
- Quantis Appliance is configured to deliver a chosen rate of random numbers to the HSM
- The SafeNet 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

Gemalto and ID Quantique Can Help

Security conscious organizations rely on strong, unique, random encryption key generation together with FIPS 140-2-validated hardware root of trust protection in order to ensure their entire security foundation remains secure. To learn more about tamper-resistant SafeNet Luna HSMs contact Gemalto at info@gemalto.com, or ID Quantique at info@idquantique.com to benefit from true randomness.

About Gemalto's Safenet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

ID Quantique QRNG Highlights:

- Most stringently tested and certified QRNG including AIS31
- Trusted source of quantum randomness (Swiss Quantum)
- Operation is continuously monitored
- If failure is detected the random stream is immediately disabled
- Live status verification
- Inexhaustible entropy
- Simple, web-based configuration and management
- Hot pluggable and swappable, ensuring seamless integration even within an operating network

SafeNet Luna HSMs:

- Ensure against unauthorized access of cryptographic keys with FIPS 140-2 Level 3 validated hardware protection
- Superior Performance:
  - Fast HSM with over 20,000 ECC and 10,000 RSA operations/s for high performance use cases
  - Lower latency for improved efficiency
- Highest Security & Compliance:
  - Keys always remain in tamper-resistant hardware
  - Meet compliance needs
  - De facto standard for the cloud
  - Multiple roles for strong separation of duties
  - Multi person MofN with multi-factor authentication for increased security
  - Secure audit logging
- Reduce costs and save time with remote HSM management
- Reduced audit and compliance costs

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.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free