# Quantum-Enhanced Security:
# **Qrypt &** Thales Luna HSM

Fortifying Thales Luna HSM with Qrypt's Quantum Entropy

In an era where digital security is paramount, Qrypt empowers Thales Luna HSMs with an additional layer of quantum-enhanced security, ensuring that cryptographic operations are not just secure but fortified against the evolving landscape of cyber threats.

**Enhanced Security Posture**
Qrypt's Quantum Entropy immediately enhances security posture by providing an unlimited source of high-quality entropy, essential for secure key creation.

**High-Quality Randomness**
By leveraging multiple independent sources of quantum randomness, Qrypt ensures the delivery of high-quality true quantum random numbers and increase the redundancy and minimize the risk of a single source of entropy..

**Seamless Integration with Thales Luna Hardware Security Module (HSM) via PKCS#11**
Qrypt's Quantum Entropy integrates seamlessly with the industry-leading Thales Luna HSMs, utilizing the standard PKCS#11 compliant services to offer an immediate enhancement to its already robust security capabilities.

## The Quality of Randomness & The Risk to Cryptography

Randomness is the cornerstone of digital security, shielding systems from attacks and preserving user data and privacy. As machine learning evolves, it's becoming crucial to address vulnerabilities tied to deterministic processes in cryptographic systems. The integration of quantum entropy brings an added dimension of unpredictability, bolstering the robustness of security mechanisms without destabilizing existing infrastructures.

In contrast, quantum random number generators (QRNGs) leverage the inherent randomness of quantum mechanics to generate truly random numbers. The numbers produced by a QRNG are unpredictable and cannot be replicated, providing an essentially unlimited key space. This makes QRNGs ideal for tasks that require high security, such as encryption.

**True Randomness:** The unique characteristics of quantum mechanics stand out as a premier source of true randomness. QRNGs, due to the inherent unpredictability of quantum phenomena, are both less susceptible to side-channel attacks and generate numbers that are truly random and unpredictable.

**Unpredictability:** The numbers produced by a QRNG cannot be predicted or replicated. This unpredictability results from the inherent randomness of quantum mechanics, not a product of a complex algorithm or large key space.

Qrypt VERIFIED SOLUTION THALES

## What is Quantum Entropy as a Service (EaaS)?

Quantum Entropy as a Service (EaaS) by Qrypt is a cloud-based service offering true randomness from quantum phenomena, enhancing the security of cryptographic systems through accessible and convenient delivery of quantum entropy. Leveraging EaaS with Thales Luna HSMs ensures a continuous supply of high-quality entropy, vital for secure cryptographic operations and eliminating the possibility of entropy starvation.

## Why Use an EaaS?

Not all cryptographic solutions, including HSMs, are using true quantum entropy today. You can immediately improve your security posture by leveraging EaaS to provide an unlimited entropy source to your key generation, management, and other security solutions. Additionally, EaaS can be a more cost-effective and scalable solution than deploying on-premises QRNGs or upgrading existing hardware.

## Qrypt QRNGs:
## Built Through Partnerships with US and International Labs

Qrypt's partnerships with **Oak Ridge and Los Alamos National Labs** highlight Qrypt's commitment to national security interests and the development of reliable, secure quantum random number generators. The alignment with these esteemed national labs underscores the robustness and reliability of Qrypt's QRNG technology. Extending our research and development horizons, Qrypt also engages in strategic collaborations with international entities, including **École Polytechnique Fédérale de Lausanne (EPFL)** and **The Institute of Photonic Sciences (ICFO)**, enhancing our global perspective and commitment to advancing quantum security worldwide.

OAK RIDGE National Laboratory  Los Alamos NATIONAL LABORATORY  EPFL  ICFO

## Qrypt Advantage

Qrypt's Quantum Entropy offers unparalleled advantages in cryptographic security. Qrypt's cloud-based service is built upon multiple quantum sources, eliminating the risk of even a single quantum source failing or being characterized, and generates high-quality, true quantum random numbers.

**Fast, Globally Available, and Scalable**
Qrypt's EaaS is designed to provide random numbers quickly and efficiently. Our globally available service ensures devices from any location can access high-quality quantum randomness seamlessly. Moreover, our scalable infrastructure is designed to accommodate both small-scale and large-scale applications, ensuring extensive random number generation requests are handled efficiently.

Qrypt VERIFIED SOLUTION THALES

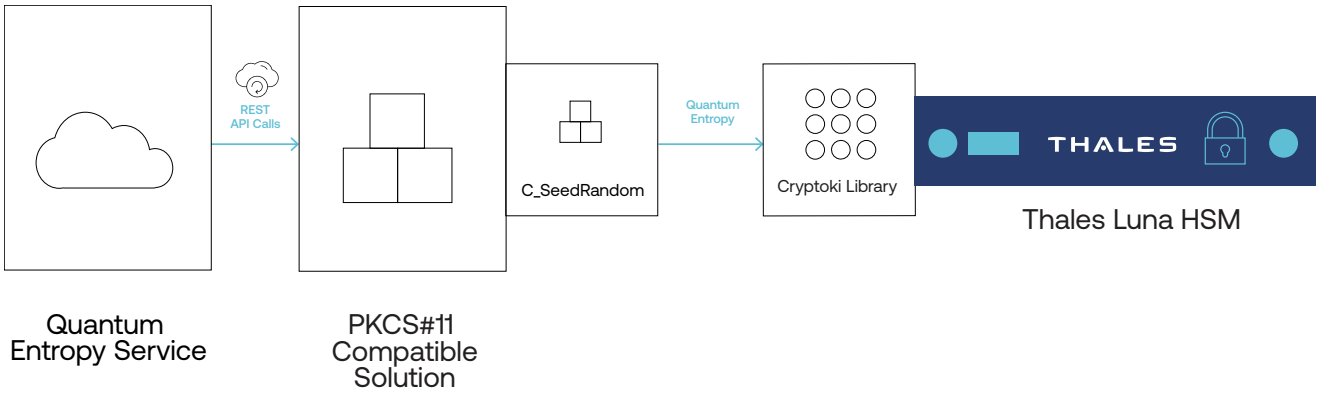
## Simple Integration Via PKCS#11

Organizations can efficiently leverage quantum entropy through the standard PKCS#11 Cryptoki interface, ensuring optimized integration. PKCS#11 compliant services, such as Key Management System (KMS) or Certificate Authority (CA), facilitate the interaction between Thales Luna HSMs and Qrypt's Quantum Entropy. This allows Thales Luna HSMs to seamlessly integrate and consume quantum entropy, enabling the immediate enhancement of cryptographic applications.

**Thales Luna HSMs Integration**
Thales HSMs can seamlessly integrate Qrypt's Quantum Entropy, facilitated by client applications, through the standard PKCS#11 Cryptoki interface. This integration allows cryptographic applications to be immediately enhanced by blending quantum-generated random numbers with existing entropy sources, fortifying the overall entropy pool.

Details on integrating our solution can be found on our documentation page for Quantum Entropy under Seed PKCS#11 HSMs ↗

# Qrypt's Quantum Entropy Service




Explore how Qrypt's Quantum Entropy can fortify the security posture of Thales HSMs

For more on the integration process, discuss your cryptographic needs with us at

**www.qrypt.com**

CONTACT QRYPT