Quantum Dice and Thales QRNG-Backed HSM Solution Brief

Verifiably strong cryptographic keys for quantum-resilient systems and enhanced auditability for the transition to post-quantum security

Key Benefits

Verifiably high-quality cryptographic keys: The quality of the entropy used to generate encryption keys matters. By integrating Quantum Dice's Quantum Entropy-as-a-Service (QEaaS) with Thales Luna 7 HSM, organisations benefit from verifiable entropy, backed by Quantum Dice's patented DISC™ protocol. This provides a unique ability for users to verify and quantify the security of their encryption keys in real-time.

Enhanced auditability for seamless post-quantum migration: Cryptographic keys based on verifiable entropy enables organisations to meet compliance standards and build auditable, resilient cryptographic systems, ensuring smooth and secure migration to post-quantum security.

The Business Challenge

The advent of quantum computing compels organisations to rethink their cryptographic resilience – particularly as the global migration to post-quantum security and upgrade of legacy cybersecurity infrastructure is underway. On 13 August 2024, the US National Institute of Standards and Technology (NIST) published new cryptographic standards for PQC.[1] At the core of post-quantum security implementation is randomness, or entropy, which forms the foundation of the cryptographic keys that encrypt our sensitive data.

Not only is entropy itself crucial for post-quantum security, but its **quality** directly impacts the strength and security of cryptographic keys. A whitepaper published by the Alliance for Telecommunications Industry Solutions (ATIS) with input from AT&T, titled 'Implications of Entropy on Symmetric Key Encryption Resilience to Quantum', highlights that cryptographic key strength depends not just on key length but on the quality of the entropy used. Without true randomness, even a 256-bit AES key can be vulnerable to quantum attacks like Grover's attacks.[2]

The Solution

Quantum Dice and Thales offer a QRNG-backed HSM solution that combines Quantum Dice's Quantum Entropy-as-a-Service (QEaaS) with the Thales Luna 7 HSM to provide enhanced security features. The Thales Luna 7 HSM allows users to connect Quantum Dice's QEaaS as an external entropy source for even stronger security, using a standard API.

QEaaS benefits from Quantum Dice's patented source-device independent self-certification (DISC™) protocol, which leverages the unique properties of quantum photonics to continuously measure and certify the amount of quantum entropy that is being produced in each sample.

This QRNG-backed HSM solution blends the market-leading cryptographic capabilities of the Luna 7 HSM with Quantum Dice's verifiably high-quality quantum randomness, providing an ideal setup for high-security applications, robust post-quantum security implementations, and quantum-resilient enterprise cryptography.

[1] National Institute of Standards and Technology (NIST) (2024) NIST releases first 3 finalized post-quantum encryption standards. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[2] Deakin, I., Krawec, W., and Trost, W. (2023) Implications of Entropy on Symmetric Key Encryption Resilience to Quantum. Alliance for Telecommunications Industry Solutions (ATIS). Available at: https://atis.org/wp-content/uploads/2023/02/Quantum-Entropy-Report-v6-1.pdf

VERIFIED SOLUTION
THALES

Solution Key Features & Benefits

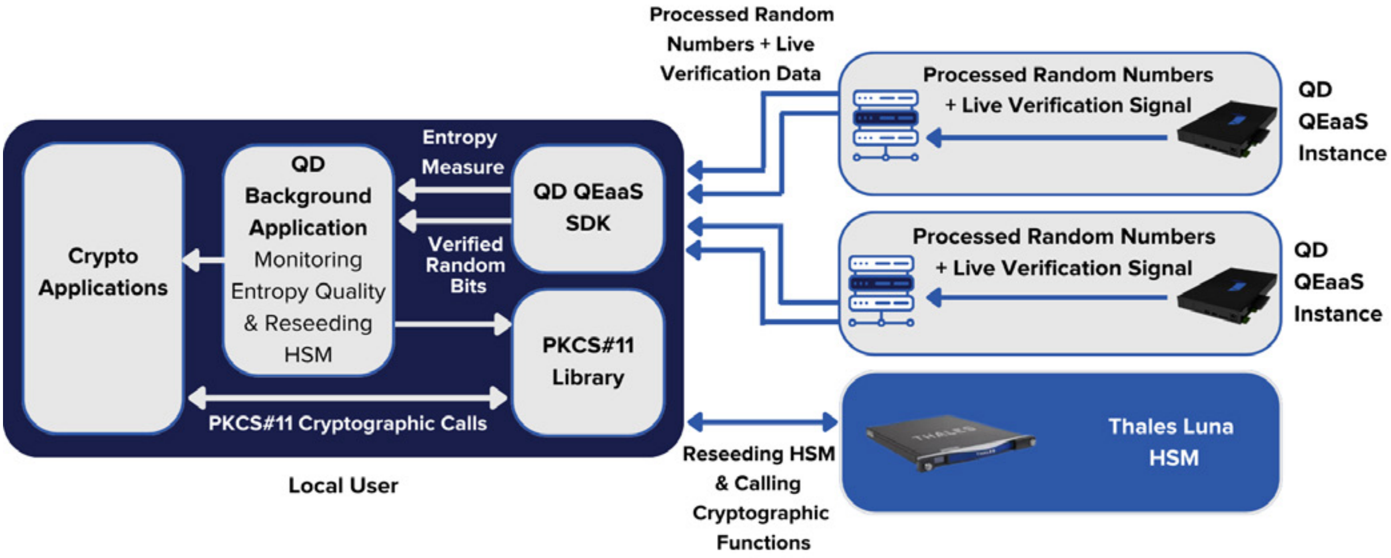
Enhanced protection: The QRNG-backed HSM offers improved security by providing high-quality entropy for cryptographic operations, making it harder for adversaries to compromise communication channels and gain unauthorised access to sensitive data.

Quantum-resistant security: As quantum computing threatens traditional encryption, this integrated solution provides reliably high-quality entropy for stronger cryptographic keys, protecting against potential vulnerabilities that could be exposed by advancing capabilities.

Certifiable entropy to enhance auditing: At the core of our QEaaS solution is our patented source-device independent self-certification (DISC™) protocol, enabling real-time quantification of entropy quality and enhancing the audit trail recommended by NIST.

Easy integration: The integration of QEaaS with the Thales HSM is straightforward and can be done with your cryptographic application using a few simple tools and a couple of easy-to-implement steps.

Quantum Dice's QEaaS Solution Integrated with the Thales Luna HSM


Processed Random Numbers + Live Verification Data
Processed Random Numbers + Live Verification Signal
QD QEaaS Instance
Processed Random Numbers + Live Verification Signal
QD QEaaS Instance
Entropy Measure
Crypto Applications
QD Background Application Monitoring Entropy Quality & Reseeding HSM
QD QEaaS SDK
Verified Random Bits
PKCS#11 Library
PKCS#11 Cryptographic Calls
Local User
Thales Luna HSM
Reseeding HSM & Calling Cryptographic Functions

Why Use the Quantum Dice and Thales QRNG-Backed HSM?

The QRNG-backed HSM solution provides a robust offering for organisations navigating the migration to post-quantum security. By integrating verifiable, high-quality entropy into cryptographic processes, organisations can ensure their encryption keys are quantum-resilient, reducing the risk of vulnerabilities. The real-time verification of entropy quality, powered by Quantum Dice's DISC™ protocol, offers an essential layer of security and compliance. This helps organisations build transparent, auditable systems as they transition to post-quantum security, ensuring long-term security and seamless compliance with evolving standards.

About Quantum Dice

Quantum Dice is working to solve one of the longest-standing problems in computing: generating trusted and reliable randomness. The company is developing the world's first scalable source-device independent continuously assuring quantum random number generator (QRNG). With applications in both cybersecurity and stochastic computing, the technology has a wide range of use cases in numerous sectors ranging from communication security to AI optimisation. For applications in cybersecurity, Quantum Dice aims to protect a connected future by harnessing the fundamental quantum properties of light to enable secure encryption.

QUANTUM DICE

Would you like to learn more about our DISC™-powered QRNG technology or find out how we can help you protect a connected future?

GET IN TOUCH

info@quantum-dice.com

@QuantumDiceUK

@quantum-dice

www.quantum-dice.com