Q→NU

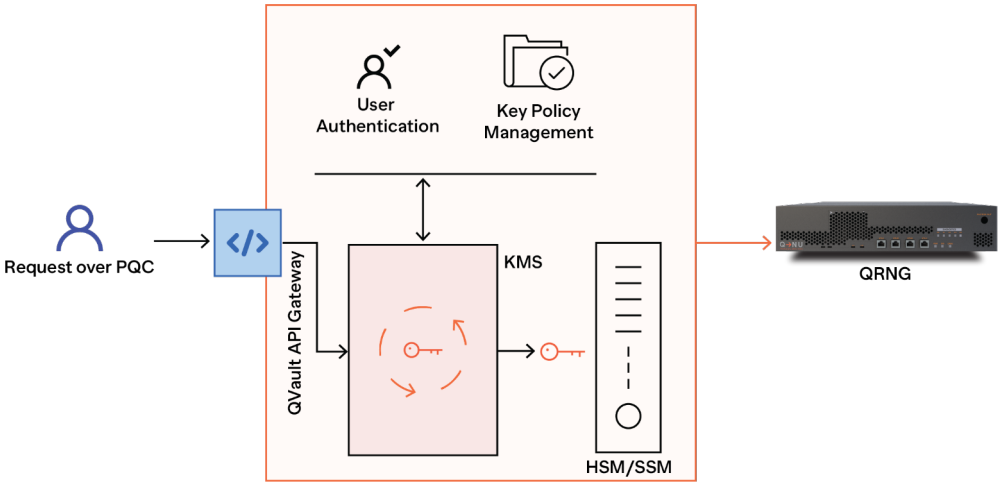
Next - Generation Quantum-Safe Key Management

Uncompromised Security for Cryptographic Keys to Protect Transactions and Sensitive Data

QHSM

Introduction

QNu Labs' **Quantum Hardware Security Module (QHSM)** is engineered to offer the highest level of protection for encryption keys and transaction of sensitive data, specifically addressing the needs of government and defence sectors. Built with cutting-edge **Post-Quantum Cryptography (PQC)** algorithms, QHSM provides an impenetrable shield against both current and future quantum threats. With QHSM, defence and government entities can future-proof their encryption systems, safeguarding sensitive data against evolving cyber threats and maintaining operational security in the quantum era.



QNu Labs offers unique capabilities that will help organizations move in the direction of technology adoption and provide data security as their competitive advantage

Gartner®

Key Features

Secure Key Management: QHSM generates, stores, and manages cryptographic keys in a tamper-proof environment, ensuring security for mission-critical applications.

Compliance: QHSM meets FIPS and other stringent security standards, supporting organizations with regulatory compliance.

Quantum-Safe Protection: QHSM uses quantum-safe algorithms, protecting commu-nications and cryptographic processes against future quantum threats.

Sign and Verify: QHSM securely handles signing and verification, ensuring the integrity of sensitive data and communications.

Data Sovereignty: QHSM gives organizations full control over cryptographic operations and key storage, ensuring data sovereignty.

Defence Applications

Secure Communication for Defence Forces:

QHSM securely stores cryptographic keys for encrypting and decrypting military communications, protecting sensitive data like emails and real-time information, ensuring authenticity and integrity through signing and verification.

Classified Document Signing and Verification:

QHSM securely manages cryptographic keys for digitally signing documents, ensuring their authenticity and preventing forgery, so sensitive orders and communications come from authorized officials.

Key Management for Military Cryptographic Systems:

QNu Labs' QHSM manages cryptographic keys for secure transmission, signing, and verification, with hardware-based protection for military data and communications.

National Security - Secure Access to Classified Systems:

QHSM securely manages cryptographic keys for multi-factor authentication, ensuring only authorized personnel access sensitive systems, enhancing database and network security.

Key Features Comparison

Feature	QNu Labs QHSM	Traditional HSM
Quantum-Safe Encryption	Built with Post-Quantum Cryptography (PQC) algorithms, providing protection against both current and future quantum threats.	Vulnerable to quantum attacks, as it lacks quantum-safe encryption.
Performance	Optimized for speed, capable of over 14,000 RSA operations per second, ensuring high-speed cryptographic processes.	Typically slower, not optimized for environments demanding high cryptographic throughput.
Future-Proof Security	Designed to withstand both current and emerging quantum threats, securing your data now and in the quantum future.	Limited to current cryptographic standards and susceptible to obsolescence as quantum threats emerge.
Centralized Key Management	Integrated with the Maestro Command Module, offering centralized, intuitive management of cryptographic resources.	May involve complex management processes, often lacking centralized control.
Scalability	Highly scalable, ideal for enterprises managing large volumes of cryptographic operations across distributed systems.	Less scalable and efficient, often not designed to handle high volumes or complex cryptographic needs.
Compliance with Future Standards	Built to meet both current and upcoming cryptographic standards, ensuring long-term regulatory compliance.	Adheres to existing standards but may require costly updates to meet future compliance requirements.

Specifications

Feature	Details
OS	Linux
Cryptography	— Asymmetric: RSA, DSA, Dilithium (2/3/4), SPHINCS+, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES), Kyber (512, 768, 1024) — Symmetric: AES, AES-GCM, Triple DES — Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3, and more — Key Derivation: SP800-108 Counter Mode — Key Wrapping: SP800-38F — Random Number Generation: HW based true random number using built-in QNu QRNG
Cryptographic APIs	— PKCS#11, Java (JCA/JCE), OpenSSL — REST API for Administration
Rack Mountable	Standard 2U 19” rack mountable appliance
Dimensions	17” x 21.3” x 3.5” (432.8 x 541.8 x 88.8 mm)
Weight	22 kg
Input Voltage	AC Input: 100-240V, 50-60Hz
Power Consumption	300W 1+1 redundant power supply
Temperature	Operating temperature: 0°C(32°F) ~ 35°C(95°F) Storage temperature: -10°C(14°F) ~ 60°C(140°F)
Relative Humidity	5%~95% non-condensing
Reliability	— Hot-swappable power supply — 4 x 40x56mm hot swap fans — Temper prevention structure (Temper switch, Blind Standoff) — Anti-Probing structure — Mechanic reinforce structure
Security Certification	FIPS*
Safety and Environmental Compliance*	— UL, CSA, CE — FCC, CE, VCCI
Host Interface	2 Gigabit Ethernet Ports (RJ45) | 2 USB 3.0 Type A
Management	— CLI, GUI (Maestro) — Remote power on/off/reset — Biometric authentication based system startup
Logging	syslog
Monitoring	— Remote system Monitor and Management — Temperature, Voltage and Fan speed montoring — System ID and System Failure indicator

Q→NU

QNu Labs is revolutionizing cybersecurity with cutting-edge quantum-safe solutions, making India a leader in quantum cryptography. Through its patent-protected products - Armos and Tropos, QNu Labs is at the forefront to enable quantum secure key generation & distribution for secure data transmission.

With its innovative QShield platform, which is based on NIST complaint PQC algorithms, QNu offers quantum-secure services such as VPN, messaging, file sharing & key management (QHSM).

QNu Labs is at the forefront of quantum security, shaping the future of secure communications & protecting critical infrastructures like finance, defence, and telecom from future quantum threats.

Have a trusted advisor get in touch with you to explore how QHSM can protect your operations from quantum cyber threats.

Request a Demo

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629