Q→NU
Proactively
Quantum

QShield

QVault

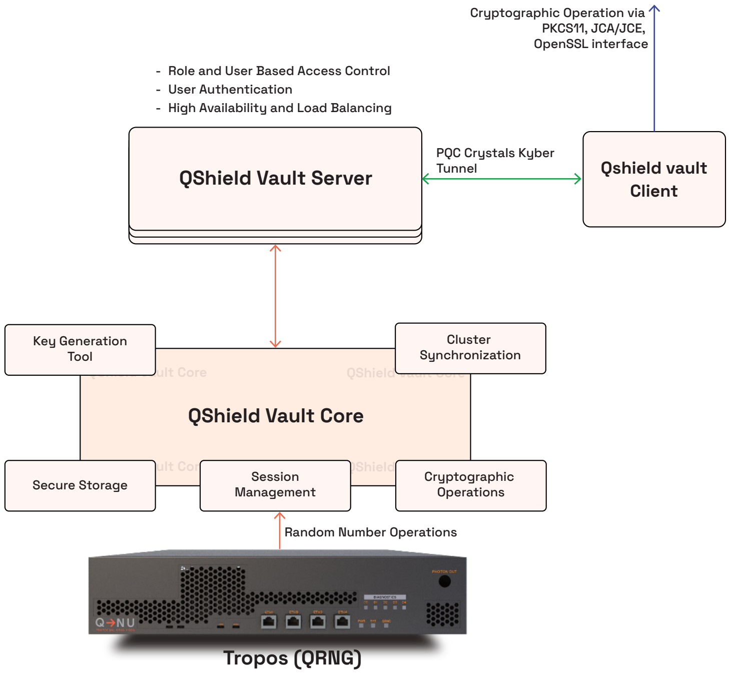
QNL QVAULT SL-G

Post Quantum Cryptography | One-Click Installation | Quantum Generated Key

Introduction:

Qshield Vault is a QRNG enhanced digital key vault to securely store and manage access to cyptographic keys. Qshield vault leverages high entropy QRNG keys with auto rotation policy to guard secrets.

Highest Entropy keys are stored into encrypted Storage, called Qshield vault. It enables key rotation at customer defined frequency keeping the Key Encryption Key (KEK) and Data Encryption Key (DEK) in encrypted format.



Key Features and its Benefits:

Key Features	Key Benefits
Key Generation and Storage	A PQC based key generation and management -supporting both Classical and Quantum keys
Cryptographic Operations	Supports Several types of cryptographic transaction like Encryption,Decryption,Signing ,Verification, etc..,
Random Number Operations	Leveraging QRNG to provide Unbiased and Truly random number to strengthen the Quality of Cryptographic Keys
NIST PQC Algorithms	Leverage NIST PQC Algorithms for secure communications and Cryptographic Operations
Supports PKCS#11 Interface	Defines the interface between an application and a cryptographic device
Performance(Cryptographic Operations)	1000 Cryptographic Transactions per second
Scalable	Horizontal & Vertical with minimal network Disruption
Hardware Independent	It can be deployed over any hardware of required specification
Single Click Installation	Server and Client

Specifications

Items	Feature	Details
Secure Classical Cryptographic Operations	FIPS Compliant Cryptography Support	— AES(128/192/256) — RSA(1024/2048/4096) — DSA(1024/2048/3072/4096) — ECDSA(224/256/384/521) — ECDH(224/256/384/521)) — 3-DES(56/112/168) — SHA-2,SHA-3
	10000 Sign Ops/Sec for RSA-2048 (In Cluster mode with multiple multi core machines)	
	Supported Algorithms(Asymmetric/ Symmetric/HASH/MAC)	
Secure Post Quantum Cryptography Operations	Public-Key Encryption/KEMs	CRYSTALS-KYBER-(512/768,1024)
	Digital Signatures	— CRYSTALS-Dilithium- 2,3,5 — FALCON-512, FALCON-1024, FALCON-2048
	Digital Signature Performance	500 Dilithium-2 Sign Ops/Sec
Standardized Interface	PKCS11, JCE/JCA, OpenSSL	
Secure Communication	PQC Enabled secure client-Server Communication	
Quantum Entropy	Random Entropy sourced from QRNG	
Secure Storage	Key Encryption Key,Master Key ,Key Encryption Key Rotation,Configurable secret sharing	
High Availability and Load Balancing	Cluster Mode	— Load Balancing to up to 5 QKVs — Load Balancing for Single and Multi-Part Operations
Client Authentication	Multi Factor Authentication	
Audit Logs	Encrypted Audit Logs	
Key Management Utility	CLI (Command Line Interface)	
Client and Server Environment	OS Support	Ubuntu
Server Specifications	Ubuntu - Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, 32GB RAM, 512GB SSD SATA	