Quantum-Safe Encryptor

Post Quantum Security

The Quantum-Safe Encryptor is a next-generation, quantum-ready solution engineered for high-assurance protection of data in transit across critical infrastructure. Built on a high-performance FPGA architecture, it delivers ultra-low latency and high-throughput Layer 2 encryption and supports both Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) readiness. Designed for mission-critical sectors, it safeguards data confidentiality even against “Harvest Now, Decrypt Later” threats.

Certified to FIPS 140-3 Level 3 and built for Common Criteria validation, the encryptor integrates tamper resistance, active zeroisation, and real-time anomaly detection. Its architecture enables seamless integration with Security Operations Centres (SOCs), providing unified visibility, remote health monitoring, and faster incident response. Whether deployed point-to-point or across multipoint networks, it delivers scalable protection without compromising performance.

With its ability to secure critical infrastructure covering national communications, financial transactions, and ICS/OT networks, the Quantum-Safe Encryptor offers a future-proof investment for organisations seeking to safeguard operational continuity and regulatory compliance against emerging quantum cyber threats.

KEY FEATURES

- **Quantum-ready encryption with PQC and QKD readiness** safeguarding against current and future quantum threats.
- **FPGA-based encryption engine** delivering hardware-level assurance.
- **FIPS 140-3 Level 3** certification ensuring compliance across highly regulated environments.
- **Centralised Security Management** with SOC integration for real-time monitoring, anomaly detection, and policy enforcement.

Specifications

Quantum-Safe Encryptor

Performance	• Scalable throughput of 100/10/1 Gbps
Network Interfaces	• 4x 100 Gigabit ethernet ports (2x Trusted, 2x External) with QSFP28 interfaces • 8x 10/1 Gigabit ethernet ports (4x Trusted, 4x External) with SFP+ interfaces
Cryptography	• Confidentiality, integrity and replay protections • Advanced Encryption Standard (AES256) • Galois Counter Mode (GCM) encryption algorithm • Hardware Random Number Generator (HRNG) • Supports PQC and QKD
Key Management	• Proprietary key management system's • Parameter loading using smartcard / laptop
Device Management	• OOB management port: 1 x 1Gbps Ethernet RJ45 for remote monitoring configuration • Key Load port: 1 x 1Gbps port with any SFP interfaces • QKD port: 1 x 1Gbps port with any SFP interfaces • Local CLI console port
Physical Security	• Tamper resistant chassis • Tamper detection and response • Active zeroisation of cryptographic data upon tamper detection • High temperature detection
Operating Environment	• Operating temperature: 0°C to 40°C • Storage temperature: -10°C to 50°C • Humidity: Relative 10% to 80%, non-condensing • EMI/EMC: FCC Part 15 Class A / EN50082-1
Physical Characteristics	• Dimension: 1U height, fits 19" rack • Weight: 10Kg • Redundant hot-swap PSU module options: • 100 to 240V AC @ 50/60Hz • 2) -36 to -75V DC, 250W (Max)
Networking Features & Protocols	• Ethernet Layer 2 encryption • Support for jumbo frames up to 9596 bytes, point-to-point, multipoint-to-multipoint
Security/Configuration	• Designed to meet FIPS 140-3 Level 3 • Element Management System with 2FA authentication • Management through NetConf protocol • Audit logging, Alarm detection and reporting
Key Management System (KMS)	• Hardware Key generation Platform • Software system for keys parameter generation
Smartcard	• Configuration card for cryptographic key parameters
Element Management System (EMS)	• Web-based application that manages deployed encryptor connected to the network, including inventory and control, service information, faults, and monitoring of equipment and its transmission capabilities.

ST Engineering

SECURE WHAT MATTERS

www.stengg.com/cybersecurity
cybersecurity@stengg.com