

Quantum Safe Optical Encryptor

Secure Optical Communications



Sensitive data transmitted over public infrastructure face a growing Harvest Now, Decrypt Later (HNDL) threat. Adversaries can intercept and archive encrypted traffic today, anticipating future quantum capabilities that may render current cryptographic algorithms vulnerable.

Quantum Safe Optical Encryptor protects data in transit at the optical transmission layer. By transforming digital payloads into spectrally distributed optical noise prior to transmission, the solution renders intercepted optical signals unintelligible, preventing unauthorised receivers from sampling, recording, or reconstructing the original transmitted data stream.

By enforcing interception resistance directly within the fibre channel, Quantum Safe Optical Encryptor eliminates opportunities for data harvesting before cryptographic compromise becomes possible. This physics-based protection complements conventional encryption and emerging quantum resilient technologies such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) to strengthen long-term confidentiality of sensitive communications.

KEY CAPABILITIES



Photonic Signal Transformation

Transforms digital payloads into spectrally distributed optical noise, preventing creation of a usable, recordable optical signal.



Optical Layer Protection

Protects data directly at the optical transmission layer, eliminating opportunities for data harvesting before cryptographic compromise.



Harvest Proof Transmission

Creates an unrecordable transmission scheme designed to counter HNDL threats.

TECHNICAL HIGHLIGHTS



100–200 Gb/s Uplink

High capacity secure optical transmission with photonic encryption.



100–400 GbE / OTU4

Supports high speed Ethernet and optical transport network protocols.



Flexible Optical Topologies

Supports Point to Point, Ring and Mesh networks via external LAN connectivity.



Up to 100 km

Supports unamplified optical links of up to 100 km.



High Assurance Security

Single air-gapped crypto engine; designed for FIPS 140-3 certification.



SPECIFICATIONS

Quantum Safe Optical Encryptor

Uplink	• 100-200 Gb/s uplink with photonic encryption
Product Topologies	• Point-to-Point, Ring, and Mesh topologies supported via external LAN connectivity
Service Ports Interface	• Up to 4 QSFP-28 Service ports
Service Supported Protocols	• 100-400 GbE, OTU4
Modulation Formats	• DP-QPSK, DP-16-QAM
Uplink FEC Type	• oFEC
Spectral Stealth Capability	• Tailored to the optical link's requirements and restrictions
Optical Cryptographic Keys	• No change required
Dimensions	• 132.4mm H, 481.0mm W, 685.5mm D, 35kg
Link Length	• Up to 100 km (unamplified)
Spectral Band	• C-Band, spread over 1-2 THz
Management Ports	• RJ45, Web management application
Client API	• RESTful
Environmental Conditions	• Operation: 0 °C to +55 °C • Storage: -25 °C to +70 °C (with enclosure) • 0%-95% humidity (non-condensing)
Electrical Interfaces	• Two independent hot-swappable dual redundant power inlets • AC input, 100 to 240 VAC, 50/60 Hz • DC input, -36 to -70 VDC
Laser Safety	• Class 1M
Security Compliance	• Designed for FIPS-140-3 certification • Single air-gapped Crypto-Engine • Optional ML-KEM (PQC) support available upon request
Operation, Transport and Storage Conditions	• ETSI EN 300 019-1-1 Class 1.2 • ETSI EN 300 019-1-2 Class 2.3 • ETSI EN 300 019-1-2 Class 3.2
EMI Compliance	• Telcordia GR-63-CORE • ETSI EN 300 386 Class B • Telcordia GR-1089-Core • ETSI EN 55032 class A • ETSI EN 55034 • AS/NZS CISPR 22

