Applications/ Use Cases

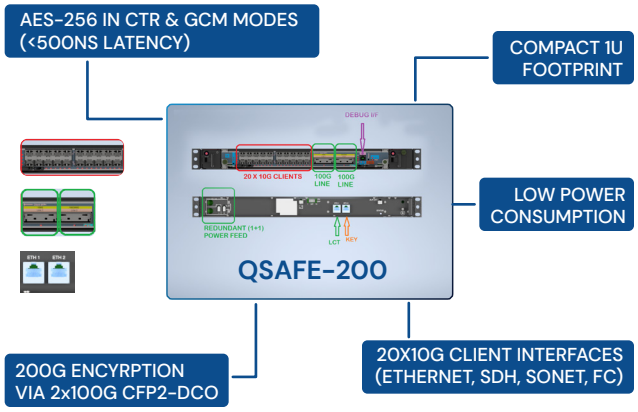
- Defense & Security Communication Networks
- Banking & Financial Institutions (core banking, ATM networks)
- Telecom & Transport Networks
- Critical Infrastructure (Power, Railways, Smart Cities)
- Data Centers & Cloud Interconnects

Certifications & Compliance

- Designed as per industry standards and best practices
- Aligned with NIST-Approved PQC standards
- Fully compatible with Quantum key distribution (QKD) frameworks

Deployment Flexibility

- Supports Hybrid Key Exchange (PQC + ECDH)
- Optional use of external QKD keys
- Legacy-compatible : ECDH-only mode for classical deployments



सी-डॉट
C-DOT

Centre for Development of Telematics

Telecom Technology Centre of Govt. of India

www.cdot.in

C-DOT Campus, Mehrauli,
New Delhi-110030, India
(+91) 11 26598262 | +91-9821488871

C-DOT Campus, Electronics City Phase 1,
Bengaluru-56100, India
+91-8028520050

export@cdot.in
C-DOT_India
Centre for Delevopment of Telematics

सी-डॉट
C-DOT

QSafe-200

Quantum-Safe Layer-1 Optical Encryptor

Future-proof Security for High-Speed Optical Networks

Product Overview

In the age of increasing cyber threats and emerging quantum computers, traditional IPsec or MACsec encryption is no longer enough. QSafe-200 is India's first Quantum-Safe Layer-1 Optical Encryption solution. It protects critical infrastructure, defense, and telecom networks from even the most advanced quantum threats—securing sensitive data in-flight at line speeds up to 100 Gbps with AES-256 encryption using keys derived from an in-built Post-Quantum Cryptography (PQC) engine.

- ETHERNET
- SDH
- OTN
- SONET

Key Features & Benefits

Feature	Benefits
Layer-1 Optical Encryption	Ensures complete data confidentiality, including IP and MAC headers
AES-256 CTR/GCM Modes	Ultra-fast, Low latency, industry-standard protection
Quantum-Resistant PQC	NIST-approved ML-KEM (Kyber) + ECDH hybrid encryption
Supports Multiple Protocols	Ethernet, OTN, SDH, SONET, Fibre Channel – No protocol dependency
External QKD Compatibility	Seamless integration with Quantum Key Distribution system
Transparent Encryption	Works without altering or affecting existing fiber infrastructure
Made in India	Designed & developed by C-DOT for strategic national and global use

Technical Specifications

Specification	Details
Encryption Standard	AES-256 in CTR & GCM modes
Encryption Throughput	Up to 200 Gbps via 2×100G CFP2-DCO
Client Interfaces	20×10G (Ethernet, SDH, SONET, FC, etc.)
Quantum-Safe Algorithms	Hybrid PQC (ML-KEM CRYSTALS Kyber + ECDH) or ECDH-only modes
Form Factor	Compact 1U rackmount
Power	Low power consumption for energy-efficient operations (Typical 150W)

How It Works

QSafe-200 encrypts all data directly at the physical layer (Layer 1). This stops potential threat actors from exploiting metadata (e.g., IP addresses, server certifications, or protocol types), even when they directly tap the fiber. The Layer-1 encryption works transparently and adds zero latency.

BEFORE

AFTER