

Quantum Safe SCADA Encryptor

Serial Communications



The Quantum Safe Serial Link Encryptor is a purpose-built serial link encryption solution that protects sensitive SCADA communication links against current and emerging quantum threats. Designed for operational technology environments, it combines Post-Quantum Cryptography (PQC) with Quantum Key Distribution (QKD) readiness to strengthen cyber resilience while preserving existing SCADA infrastructure.

Powered by ST Engineering's in-house *d'Cryptor SC* cryptographic core, certified to FIPS 140-2 Level 4, it provides high assurance hardware security, secure key management and tamper resistant protection. Support for ML-KEM, AES, ECDSA, ECDH and SHA3, together with ETSI GS 014-compatible QKD key retrieval, enables secure, future ready SCADA communications.

KEY FEATURES



Quantum-Safe Cryptography

Supports ML-DSA and ML-KEM alongside established cryptographic algorithms for protection against current and future threats.



QKD Ready Key Management

Supports key retrieval from ETSI GS QKD 014-compliant Quantum Key Distribution (QKD) systems.



Secure Serial Communications

Purpose built async-to-async serial link encryption for protecting protocol agnostic SCADA communications.

TECHNICAL HIGHLIGHTS



High Assurance Hardware Security

Uses ST Engineering's *d'Cryptor SC* cryptographic core, certified to FIPS 140-2 Level 4.



Secure Key Management

Cryptographic keys are generated, stored, and protected within a FIPS-certified HSM, ensuring the highest level of security and trust.



Platform Integrity Protection

Integrates Secure Boot, security-hardened Operating System, Built-in Self-Test (BiST), active tamper response, and tamper-resistant / tamper-evident construction to protect platform integrity.



SPECIFICATIONS

Quantum Safe SCADA Encryptor

Configuration	Point-to-Point Asynchronous Serial Link Encryption (Protocol Agnostic)	
Electrical	Power source: 12V / 24V / 48V DC	
Connections / Peripheral Interfaces	Serial Link Interfaces: 1 x RJ50 connector for DTE interface / 1 x RJ50 connector for DCE interface Bit Rate: 2400 - 115200 bps	
	Configuration and Key Loading Interface: 1 x RJ45 connector with Serial Interface Bit Rate: 115,200 bps	
	Two-pin power supply connector	
	QKD System Interface: 1 x RJ45 connector with 1000 BASE-T Ethernet port	
	LED indicators	
Security	- Secure Boot - Security-Hardened Operating System - Built-in Self-Test (BiST) feature - Unique immutable Factory ID - One-Time Programmable User ID	- Real-Time Clock - Code loading verification - Tamper-Resistant and Tamper-Evident Construction - Active tamper response - Cryptographic core certified to FIPS 140-2 Level 4
Cryptography	Algorithms:	Key Length:
	ECDSA	256, 384, 521
	ECDH	256, 384, 521
	ML-DSA	ML-DSA-87 (Category 5)
	ML-KEM	ML-KEM-768 (Level 3)
	AES	128, 192, 256
	SHA3 and HMAC-SHA3	224, 256, 384, 512
	- Equipped with in-house designed FIPS 140-2 Level 4 cryptographic chip - Supports Post-Quantum Cryptography - Key retrieval compatible with Quantum Key Distribution System (ETSI GS 014) - Key Management using FIPS-certified Hardware Security Module	
	Operating temperature	0°C to +60°C
	Storage temperature	0°C to +80°C
Environmental	Humidity	Maximum 80% non- condensing
Qualifications	IEC 61000-4-2 Level 4 • IEC 61000-4-3 Level 3 • IEC 61000-4-4 Level 4 • IEC 61000-4-5 Level 4 • IEC 61000-4-6 Level 3 • IEC 61000-4-8 Level 5 • IEC 61000-4-10 Level 5 • IEC 61000-4-16 Level 4 • IEC 61000-4-18 Level 3 • IEC 61000-4-29 • IEEE Std C37.90 Clause 8 500Vac • IEC 60255-21-1 Class 1 • IEC 60255-21-2 Class 1 • IEC 60255-21-3 Class 1	
Mechanical	Small form factor	120 x 75 x 22 mm
	Ingress Protection	IP40
	Mount Option	DIN Rail / Screw mount

