Solution Brief

Thales CN4020 Network Encryptor

Cost Effective, High-Performance Encryption

thalestct.com

THALES
Building a future we can all trust

THALES

The Thales CN4010 Network Encryptor (CN4010) provides an optical interface and high-assurance FIPS and Common Criteria certified encryption over Ethernet at full line rate speeds. The CN4020 is a versatile and simple to use platform that is user configurable to provide highly secure, full line rate of network encryption to the x (FTTx) configurations. A purpose built hardware encryption solution, it ensures low cost, high-efficiency network encryption, utilizing cutting edge high performance, optical interface connectivity, low voltage electronics to provide wire speed encryption of all voice, video and data communications. In a compact desktop profile, the CN4020 is designed as an entry-level High Speed Encryption (HSE) solution for commercial Small to Medium Enterprise (SME) sector customers or larger organizations with optical interface network needs up to 1 Gbps; and is also suited to widely distributed computing environments and multiple branch office locations.

CN4020 is available for sale to the U.S. Federal Government through Thales Trusted Cyber Technologies.

Why CN4020 Encryptors?

Trusted Security

- True end-to-end, authenticated encryption
- State-of-the-art automatic zero-touch key management
- Designed for FIPS 140-3 L3, Common Criteria, NATO, DoDIN APL

Maximum Network Performance

- Microsecond latency (<10 µS)
- Near-zero overhead
- Self-Healing capabilities for maximum up time

Scalable and Simple

- Point-to-Point, Hub and Spoke and Full Mesh
- Fully auditable alarm and event logs from 3rd party management tools

Performance

The CN4020 is a highly secure encryptor, operating in full duplex mode at 100/1000 Mbps full line rate network encryption without any packet loss in point-to-point, hub & spoke or meshed environments inside a sleek desktop profile (optional rack-mount conversion kit included). As a high-assurance appliance, the CN4020 also has the following benefits:

- Secure, tamper-proof,dedicated hardware
- Standards-based encryption algorithms
- End-to-end, authenticated network encryption
- Automatic 'zero-touch' encryption key management Technical Specifications

Scalability

The 'bump in the wire' design and variable speed licenses up to 1 Gbps make the CN4020 easy to install and highly cost effective.

"Set and forget" simplicity and network transparency are underlying design themes, ensuring easy implementation, operation and management, and minimal resource requirements.

The CN4020 is fully interoperable with the Thales Network Encryptor family of products, enabling customers to standardize on one platform to secure network data in motion. In addition to the CN4020's optical interface, it also includes an optional electrical (copper) interface converter to provide a future-ready solution for customers currently using copper, to meet a broad range of FTTx scenarios.

Certified Security

The tamper resistant CN4020 is certified Common Criteria and FIPS 140-3 Level 3, and supports standards based, end-to-end authenticated encryption, automatic key management, and utilizes robust AES 256-bit algorithms. In order to future proof the appliance, the encryptor is compatible with Quantum Key Distribution to guarantee secure communication between devices.

State-of-the-Art Key Management

The CN4020 removes reliance on external key servers and provides a robust fault-tolerant security architecture and tamper-resistant chassis. Physical and virtual separation of duties ensures that only authorized users can access the keys. Encryption keys are generated and stored securely in hardware within the device's tamper-resistant enclosure, and any unauthorized attempts to physically extract the keys will result in device zeroization.

The CN 4020 supports hardware based random number generators and can use externally generated entropy for intrinsic key generation and distribution. For future-proofing, the encryptors support Quantum Key Distribution (Quantum Cryptography) and Quantum random number generation.

Next Gen High Speed Encryption

Crypto-Agility

Thales Network Encryptors are crypto-agile, meaning they support customizable encryption for a wide range of elliptic and custom curves support. The appliances also allow bring your own entropy capabilities. The crypto-agile platform is future proof, allowing for responsive deployment of next-gen or custom algorithms. In response to the Quantum threat, Thales Network Encryptors already leverage Quantum Key Distribution (QKD) capabilities for future-proof data security.

Transport Independent Mode

Transforming the network encryption market, Thales Network Encryptors are the first to offer Transport Independent Mode (TIM) - network layer independent (Layer 2, Layer 3, and Layer 4) and protocol agnostic data in motion encryption. By supporting Layer 3, Thales Network Encryptors offer network operators more configuration options using TCP/IP routing for securing critical data.

CN4020 Encryptor At-A-Glance

Model	CN4020
Maximum Speed	1 GBPS
Support for Jumbo frames	✓
Protocol and application transparent	✓
Encrypts Unicast. Multicast and Broadcast traffic	✓
Automatic network discovery and connection establishment	✓
Tamper resistant and evident enclosure, anti-probing barriers	✓
Flexible encryption policy engine	✓
Per packet confidentiality and integrity with AES-GCM encryption*	✓
Automatic key management	✓
AES 128 or 256 bit keys	128/256
CFB, CTR, GCM Encryption modes	✓
Policy based on MAC address or VLAN ID	✓
Supports optional 3rd party quantum key distribution (QKD)	✓
Self healing key management in the event of network outages	✓
Common Criteria, FIPS, DoDIN APL	✓
Low overhead full duplex line-rate encryption	✓
FPGA based cut-through architecture	✓
Latency (microseconds per encryptor)	< 10µS
Front panel LED display notifications	✓
Centralized configuration and management using SMC and CM7	✓
Support for external (X.509v3) CAs	✓
Remote management using SNMPv3 (in-band and out-of-band)	✓
NTP (time server) support	✓
CRL and OCSP (certificate) server support	✓
In-field firmware upgrades	✓
External plug pack	✓

Technical Specifications

Cryptography

- AES 128 or 256 bit key X.509 certificates
- Fully compliant with Public Key Infrastructure (PKI)

Device management

- Dedicated management interface (out-of-band)
- Or via the encrypted interface (in-band)
- SNMPv3 remote management
- IPv4 & IPv6 capable
- Alarm, event & audit logs
- Command line serial interface

Installation

- Desktop and rackmount kit included
- Size: (WxHxD) - (W:180mm/7.1", D:126mm/5.0", H:32mm/1.3")
- Weight: 0.5kg /1.1 lbs.

Interfaces

- SFP interfaces
- Serial console at 8-pin Modular Jack
- RJ45 LAN connectors

Power Requirements

- DC input 12V DC, 7W consumption
- AC plug pack 100-240V AC; 60-50Hz; 0.7A

Physical Security

- Active/Passive tamper detection and key erasure
- Tamper evident markings
- Anti-probing barriers

Regulatory

- EN 60950-1 (CE)
- IEC 60950-1 Second Edition
- AS/NZS 60950.1
- UL Listed
- EMC (Emission and Immunity)
- FCC 47 CFR Part 15 (USA)
- ICES-003 (Canada)
- EN 55022 (CE)
- AS/NZS CISPR 22 (RCM)
- EN 61000-3-2 (CE)
- EN 61000-3-3 (CE)
- EN 55024 (CE)

Environmental

- RoHS Compliant
- Max operating temperature: 40°C /104°F
- 0 to 80% RH at 40°C/104°F operating

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

Contact us - For office location and contact information, please visit thalestct.com/contact-us