Solution Brief

Thales CN4020 Network Encryptor

Cost Effective, High-Performance Encryption

thalestct.com

THALES
Building a future we can all trust

THALES

Setting a new benchmark for price and performance, the Thales CN4010 Network Encryptor (CN4010) is a versatile, cost-effective, and simple to use platform that is user configurable to provide transparent and high-assurance FIPS and Common Criteria certified network encryption at full line rate speeds. The CN4010 is a purpose built hardware encryption solution that ensures high-efficiency Ethernet encryption, utilizing cutting edge high performance, low voltage electronics to provide wire speed encryption of all voice, video and data communications.

The CN4010 provides optimal defense-grade security in a cost effective value proposition. A desktop device, the CN4010 is designed as an entry-level HSE solution for commercial Small to Medium Enterprise (SME) sector customers or larger organizations with modest network needs; and is also suited to widely distributed computing environments and multiple branch office locations.

Why CN4010 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 CN4010 is a high-performance encryptor, operating in full duplex mode at 10/100/1000 Mbps full line rate without any packet loss in point-to-point, hub & spoke or meshed environments. Using Field Programmable Gate Array (FPGA) technology, the CN4010's cut-through architecture processes data frames as they are received, ensuring consistent low latency across all packet sizes for optimal performance. As a high-assurance appliance, The CN4010 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

Scalability

The CN4010 is fully interoperable with industry standard network equipment from leading vendors, and with 'bump in the wire' design and variable speed licenses up to 1 Gbps, it is easy to install and highly cost-effective. "Set and forget" simplicity and application

and protocol transparency are underlying design themes, ensuring simple implementation, operation and management, and minimal resource requirements. Devices can be field upgraded on site with ease, for maintenance, feature enhancements and security updates. The CN4010 also supports unicast, multi-cast, and broadcast domains.

Certified Security

The tamper resistant CN4010 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 also compatible with Quantum Key Distribution to guarantee secure communication between devices.

State-of-the-Art Key Management

The CN4010 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 CN4010 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

hales 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) and Quantum Random Number Generation (QRNG) 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.

CN4010Encryptor 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	✓
Self healing key management in the event of network outages	✓
Common Criteria, FIPS	✓
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
- SNMPv2c traps
- SNMPv1 read only monitoring
- IPv4 & IPv6 capable
- Alarm, event & audit logs
- Command line serial interface

Installation

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

Interfaces

- RJ45 interfaces
- RJ-45 serial console
- Dual USB

Power Requirements

- DC input 9-15V DC, 6W consumption
- AC plug pack 100-240V AC; 47-63Hz

Physical Security

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

Regulatory

- UL Listed, EMC (Emission and Immunity)
- FCC 47 CFR Part 15 (USA)
- EN 60950-1 (CE), EN 55022 (CE), EN 61000-3-2 (CE), EN 61000-3-3 (CE)
- EN 55024 (CE), EN 61000-3-3 (CE), EN 55024 (CE)
- CES-003 (Canada), AS/NZS CISPR 22 (C-Tick

Environmental

- RoHS Compliant
- Max operating temperature: 50°C /122°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