thalescpl.com

THALES

SafeNet Ethernet Encryptor CN4010

Cost Effective, High-Performance Encryption

Setting a new benchmark for price and performance, the SafeNet Ethernet Encryptor CN4010 by Gemalto 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 encryption over Ethernet at full line rate speeds. The CN4010 is a purpose built hardware encryption solution that ensures low cost, 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 140-2 L3, Common Criteria, NATO, UC APL
- Preferred by market leading commercial and government enterprises in over 35 countries

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 10/100/1000Mbps full line rate without any packet loss in point-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 140-2 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 guar

Metro Ethernet or Wide Area Ethernet Services

With the pervasive growth of Ethernet services, the SafeNet CN4010 Ethernet Encryptor is the ideal solution for any organization with branch and remote locations, small to large enterprises, and government or cloud service providers.

The CN4010 provides exceptional cost benefits to any organization needing to secure modest data volumes from speeds of 10 Mbps to 1 Gbps.

The CN4010 addresses the need for highly secure, highly resilient wire speed encryption of Ethernet traffic across both dark fiber and metro or wide area Ethernet services.

Supporting over 500 concurrent encrypted connections, the CN4010 operates at full line speed without packet loss to ensure the confidentiality of encrypted data regardless of frame size or application.

The intrinsic key generation and distribution capability of the CN4010 removes any reliance on external key servers, and provides robust fault-tolerant security architecture, while its rugged and tamper resistant chassis gives uncompromising protection to key material held in the encryptor. Full interoperability with the SafeNet High Speed Encryptor family products means customers can standardize on one platform to secure data in motion across large hub & spoke or meshed networks from the branch to head office.

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.

User-Friendly Encryptor Management

SafeNet High Speed Encryptors are easily managed through a simple to use local and remote encryptor management application that provides users with comprehensive and intuitive management functionality. The encryptors can be securely managed either out-of-band—using a dedicated Ethernet management interface or in-band—using the encrypted Ethernet port. Local management using a command line interface is available via a serial console connector.

TACAS+ and RADIUS protocols are supported to allow for Authentication, Authorization, and Accounting (AAA) operations. This provides end users with additional flexibility and security for day to day operations and large scale deployments.

The built-in operational flexibility provides customers a choice and avoiding additional costs of third party optical transport equipment in their network (e.g. OTN provider backbone).

CN4010 Encryptor At-A-Glance

Model	CN4010
Protocol	**Ethernet**
Protocol and Connectivity	
Maximum Speed	1 Gbps
Support for Jumbo frames	✓
Protocol and application transparent	✓
Encrypts Unicast. Multicast and Broadcast traffic	✓
Automatic network discovery and connection establishment	✓
Security	
Tamper resistant and evident enclosure, anti-probing barriers	✓
Flexible encryption policy engine	✓
Per packet confidentiality and integrity with AES-GCM encryption*	✓
Automatic key management	✓
Automatic key management	✓

Encryption and policy	
AES 128 or 256 bit keys	128/256
Supports optional 3rd party quantum key distribution (QKD)	✓
CFB, CTR, GCM Encryption modes*	✓
Policy based on MAC address or VLAN ID	✓
Self healing key management in the event of network outages	✓
Certifications	
Common Criteria, FIPS	✓
Performance	
Low overhead full duplex line-rate encryption	✓
FPGA based cut-through architecture	✓
Latency (microseconds per encryptor)	< 10μS
Management	
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	✓
Maintainability & Interoperability	
In-field firmware upgrades	✓
External plug pack	✓

* Pending firmware release

All specifications are accurate as at the time of publishing and are subject to change without notice.

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 ports
- RJ45 LAN/AUX connectors

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)
- ICES-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 Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored—from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com