PRODUCT BRIEF

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.

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
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).

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

**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.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

gemalto
security to be free

©Gemalto 2017. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. PB (EN)-Oct.18.2017 - Design: ELC

CN4010 Encryptor At-A-Glance

<table>
<thead>
<tr>
<th>MODEL</th>
<th>CN4010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>

**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.