gemalto
security to be free

PRODUCT BRIEF

SafeNet Ethernet Encryptor CN9100

100 Gbps high speed mega data in motion encryption

Delivering 100,000,000,000,000 bits per second of high-assurance data encryption, the SafeNet Ethernet Encryptor CN9100 (CN9100) provides mega data security (100 Gbps) and high speed network performance with ultra-low latency (<2 µS). Safeguard data in motion with high speed Layer 2 encryption proven to meet network performance demands for real-time low latency and near-zero overhead, ensuring security without compromise for big, or even mega data transmitted over networks across data centers and the cloud.

With the ever-increasing growth in data volumes and demand for higher bandwidth Ethernet services, the CN9100 is the ideal solution for organizations that are racing ahead at full speed, at 100 Gbps. The CN9100 is a high-assurance encryptor designed to provide 100 Gbps highly secure, full line rate transparent encryption of all voice, video and data communications moving across dark fibre, and metro or wide area and Carrier Ethernet networks (MAN or WAN). It supports all topologies including fully meshed.

Performance

The CN9100 is an ultra-high-performance encryptor, operating in full-duplex mode at 100 Gbps line rate speed. Using Field Programmable Gate Array (FPGA) technology, the CN9100's architecture enables real-time data processing and high throughput. This ensures consistent low latency across all packet sizes for optimal performance. Throughput is maximized in a zero protocol overhead mode. A 1U unit, it operates with minimal power and rack space consumption.

Scalability

Ethernet standards compliant, the CN9100 is fully interoperable with industry standard network equipment from leading vendors. The 'Bump in the Wire' design provides a vendor-agnostic and drop in the network approach to 100 Gbps encryption. The CN9100 is easy to install and highly cost-effective. "Set and forget" simplicity, and application and protocol transparency are underlying design themes, ensuring easy implementation, operation and management, and minimal resource requirements. Devices can be field upgraded on site with ease, for maintenance, feature enhancements and security updates.

Certified Security and Crypto-Agility

Designed for security conscious organizations, the tamper resistant CN9100 is in process for Common Criteria and FIPS 140-2 Level 3 certifications and supports automatic zero-touch key management.

Enabling crypto-agility, the CN9100's advanced security features include support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). Custom curves and custom entropy are a standard feature of the encryptors' software.

VLAN based encryption provides unique key pairs in hub and spoke environments to protect against misconfigured traffic.

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 (<2 µS)
- Near-zero overhead including zero overhead mode
- 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
- Field serviceable with hot swappable supplies

State-of-the-Art Key Management

The CN9100 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 CN9100 supports support 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.

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

Physical security

- Active/Passive tamper detection and key erasure

Cryptography

- AES 256 bit key X.509 certificates (CTR mode)
- Hardware based random number generator

Device management

- Dedicated management interface (out-of-band)
- Encrypted interface (in-band)
- SNMPv3 remote management
- IPv4 & IPv6 capable
- Supports Syslog, NTP
- Alarm, event & audit logs
- Command line serial interface
- TACAS+ support
- RADIUS support

Installation

- Size: 435mm, 43mm , 480m /17.1", 1.7", 18.9"
- 1U 19" rack mountable
- Weight: 8kg /17.6 lbs

Power Requirements

- AC Input: 100 to 240V AC;1.5A; 50/60Hz
- Power Consumption: 80W typical

Regulatory Safety

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

Environmental

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

CN9100 Encryptor At-A-Glance

Model	CN9100
Protocol	**Ethernet**
Protocol and Connectivity:	
Maximum Speed	100 Gbps
Support for Jumbo frames	Yes
Protocol and application transparent	Yes
Encrypts Unicast, Multicast and Broadcast traffic	Yes
Automatic network discovery and connection establishment	Yes
Network interfaces	CFP4
Security:	
Tamper resistant and evident enclosure, anti-probing barriers	Yes
Flexible encryption policy engine	Yes
Automatic key management	Yes
Encryption and Policy	
AES 256 bit keys	Yes
Encryption mode	CTR
Policy based on MAC address or VLAN ID	Yes
Self-healing key management in the event of network outages	Yes
Certifications: In progress	
Designed for Common Criteria, FIPS, NATO, UC APL*	Yes
Performance:	
Low overhead full duplex line-rate encryption	Yes
FPGA based architecture	Yes
Latency (microseconds per encryptor)	<2 µS
Management:	
Front panel access for all interfaces	Yes
Centralized configuration and management using SMC/CM7 and SNMPv3	Yes
Support for external (X.509v3) CAs	Yes
Remote management using SNMPv3 (in-band and out-of-band)	Yes
NTP (time server) support	Yes
CRL and OCSP (certificate) server support	Yes
Maintainability/Interoperability:	
In-field firmware upgrades	Yes
Dual hot-swappable AC power supplies	Yes
User replaceable fans and batteries—dual redundancy	Yes
Interoperable with all CN Series Encryptors	Yes

*In process

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.COM

gemalto
security to be free