gemalto
security to be free

PRODUCT BRIEF

SafeNet Ethernet Encryptor CN6100

10 Gbps scalable, high-assurance data in motion encryption

Safeguard data in motion with high speed Ethernet Layer 2 encryption proven to meet network performance demands for realtime low latency and near-zero overhead, providing security without compromise for data traversing networks across data centers and the cloud.

With the rapid growth of 10 Gbps Ethernet services, the SafeNet Ethernet Encryptor CN6100 (CN6100) is the ideal solution for small and large enterprise, government, and service provider clouds. The CN6100 is a versatile, high-assurance encryptor designed to provide up to 10 Gbps of highly secure, full line rate transparent encryption for all voice, video and data communications moving across dark fibre, and metro or wide area Ethernet networks (MAN or WAN)

Performance

The CN6100 is a high-performance encryptor, operating in full-duplex mode at full speed without loss of packets. Using Field Programmable Gate Array (FPGA) technology, the CN6100's cut-through architecture processes data frames as they are received. 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 30–60% less power consumption than typical 10 Gbps encryptors.

Scalability

Compliant with Ethernet standards, the CN6100 is fully interoperable with industry standard network equipment from leading vendors. The 'Bump in the Wire' design and variable speed licenses up to 10 Gbps Ethernet make the CN6100 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. Full compatibility with the entire SafeNet High Speed Encryptor family of products provides end-users with secure data transmission across any Ethernet network environment.

Certified Security

Preferred by the world's most secure organizations, the tamper resistant CN6100 is certified to Common Criteria and FIPS 140-2 Level 3 requirements and supports standards based, end-to-end authenticated encryption and client-side key management. Advanced security features include traffic flow security, support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). VLAN based encryption provides unique key pairs in hub and spoke environments to protect against mis-configured traffic. For high-assurance environments, the encryptors also support nested encryption.

Why CN6100 Encryptors?

Trusted Security

- True end-to-end, authenticated encryption
- State-of-the-art automatic zero-touch key management
- Certified 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 (<6µS)
- 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
- Field serviceable with hot swappable fans and supplies

State-of-the-Art Key Management

The CN6100 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 CN6100 supports hardware based random number generators and can use externally generated entropy for intrinsic key generation and distribution.

User-Friendly Encryptor Management

SafeNet High Speed Encryptors are easily managed through a simple to use encryptor management application, with local and remote access capabilities, that provides users with comprehensive and intuitive management functionality.

The devices 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 the ability to avoid the additional costs of third party optical transport equipment in their network (e.g. OTN provider backbone).

CN6100 Encryptor At-A-Glance

MODEL Protocol	CN6100 Ethernet
PROTOCOL AND CONNECTIVITY:	
Maximum Speed	10 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	✓
ENCRYPTION AND POLICY:	
AES 128 or 256 bit keys	128/256
CFB, CTR, GCM Encryption modes	✓
Supports optional 3rd party quantum key distribution (QKD)	✓
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)	< 6µS
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	✓
Dual redundant AC/DC power supplies	✓
Pluggable optical SFP	✓

Specifications

Physical security
- Active/Passive tamper detection and key erasure

Cryptography
- AES 128 or 256 bit key X.509 certificates (CFB, CTR or GCM modes)
- 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
- Alarm, event & audit logs
- Command line serial interface
- TACAS+ support
- RADIUS support

Installation
- Size: 447mm, 43mm (1U), 328mm /17.6", 1.7", 12.9"
- 19" rack mountable
- Weight: 8.5kg /18.7 lbs

Power Requirements
- AC Input: 100 to 240V AC;1.5A; 60/50Hz
- DC Input: 40.5 to 60 VDC, 2.0A
- Power Consumption: 50W typical

Regulatory Safety
- UL Listed
- EMC (Emission and Immunity)
- FCC 47 CFR Part 15 (USA)
- EN 55024 (CE, 60950-1 (CE), 61000-3-2 (CE), 61000-3-3 (CE)
- IEC 60950-1 Second Edition
- ICES-003 (Canada)

Environmental
- RoHS Compliant
- Max operating temperature: 50°C /122°F
- 0 to 80% RH at 40°C /104°F operating
- AS/NZS 60950-1, CISPR 22 (C-Tick)

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/contact-us/

Follow Us: blog.gemalto.com/security/

GEMALTO.COM

gemalto
security to be free