EKINOPS PM CRYPTO

Hardware Based Data Security Engine

DATA SHEET 02|2024

KEY FEATURES & BENEFITS

- AES-GCM 256 based encryption for highest level of data security
- Hardware based solution for wire-speed processing
- Ultra-low latency
- Multiprotocol multirate client support
- Evergreen solution based on Ekinops T-Chip — supports technology evolution with no hardware replacement required
- High frequency Elliptic Curve Diffie Hellman key exchange and authentication to ensure data security end-to-end

APPLICATIONS

- Business Continuance & Disaster Recovery *(BC/DR)*
- Virtual machine *(VM)* migration
- Data/disk mirroring
- Cloud services
- Secure managed connectivity services
- General Data Protection Regulation *(GDPR)* compliance

OVERVIEW

Communications networks are under continual attack from increasingly sophisticated actors making it difficult for service providers and enterprises alike to ensure the safety and security of their data. This is especially true as more data and applications move to the cloud.

In fact, most industry surveys show that data security issues rank first among barriers to adoption of cloud-based services. For the database group the primary concern is server security, protecting the integrity of the data and preventing unauthorized access to their company's information stored inside the data center. The network group has to protect the same data but with the added risk and complexity of doing it while the data is in-flight between locations. This risk is also shared by any network operator that is providing the connectivity service between those locations.

Transferring data and applications between physical locations means proprietary information is continually on the move and therefore more susceptible to intrusion than when it is behind the firewall. EKINOPS PM CRYPTO uses the strongest, industry proven AES-GCM 256 based encryption to provide the highest level of security from end-to-end.

EKINOPS PM CRYPTO protects data in-flight across high speed optical networks with a hardware based algorithm that operates at wire speed to fully encrypt the payload and guarantee the security of even the most critical data and applications. Because it is hardware-based, the Diffie-Hellman key exchange rotates the keys multiple times per minute to prevent in-flight interception while sub-microsecond added latency for encryption process provides hitless performance for all service types — capabilities not possible with software-based solutions.

Based on Ekinops' patented T-CHIP® technology, PM CRYPTO is also safe from obsolescence as new features can be updated directly on the existing module with a simple firmware download.

APPLICATIONS

Whether you are replicating data at multiple sites in a disk mirroring operation or for BC/DR purposes, migrating data between virtual machines, or moving data, applications and services into the cloud, EKINOPS PM CRYPTO provides the secure, high speed optical transport mechanism necessary to prevent unauthorized access and interception.

WIth support for 10G, 40G and 100G client services, it is designed to meet the demands of the strictest enterprise users including banks and other financials, healthcare operators, biotech and pharmaceutical companies as well as government institutions. EKINOPS PM CRYPTO provides the simplest, most cost effective solution for making your network compliant with the EU-mandated GDPR requirements. It can also be used by network operators, including cloud services providers and data center operators, to provide secure connectivity as a managed service to their end-user customers.

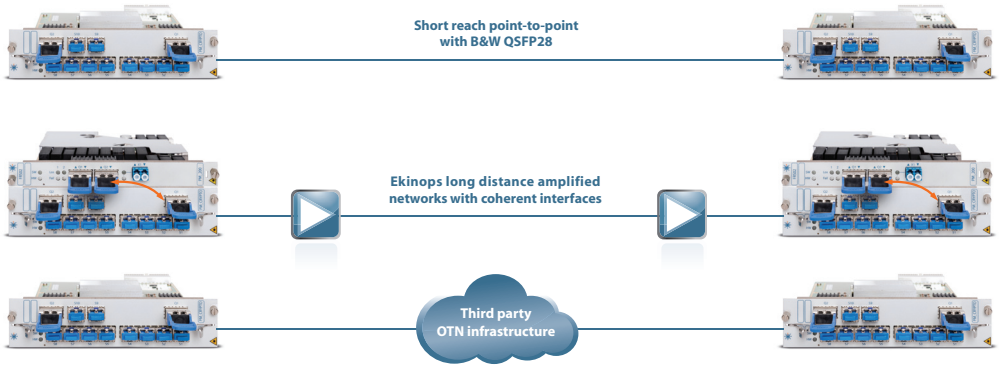

Figure 1: typical use cases

EKINOPS PM CRYPTO

Hardware Based Data Security Engine

MANAGEMENT

The PM CRYPTO module can be managed through SNMP or via the Ekinops standard element level management interfaces, which includes a CLI *(Command Line Interface)* and an Ekinops GUI *(Graphical User Interface)*. The CLI is accessible via SSH and Telnet remotely or via a local serial port on the Management board.

Complete performance monitoring and management is provided, including laser shut off and local and remote loopback which is useful for maintenance and fault isolation.

Digital Diagnostics Management *(DDM)* is supported for both QSFP28 and SFP+ interfaces. This includes link status, transmit *(TX)* and receive *(RX)* signal power monitoring and operational temperature, as well as manufacturer and transceiver model.

Complete performance monitoring and management are provided by Celestis**NMS**, the Ekinops advanced Network Management System, or through any SDN controller via NETCONF interface.

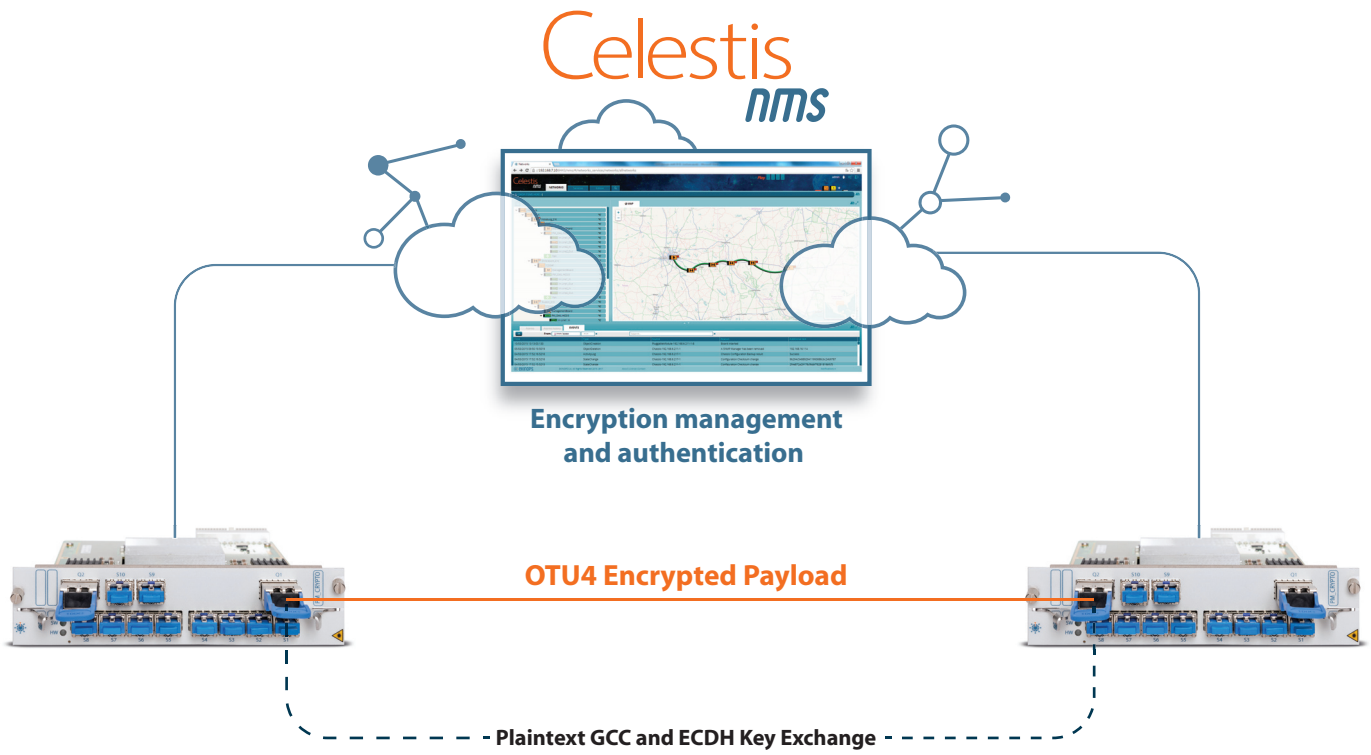

Figure 2: EKINOPS PM CRYPTO provides secure data transfer between locations

EKINOPS PM CRYPTO

Hardware Based Data Security Engine

SPECIFICATIONS

• CLIENT INTERFACE

Protocols	10GbE/40GbE/100GbE; OTU2/OTU2e; 8G/10G/16G Fibre Channel; OC-192/STM-64
Optical interface	SFP+ / QSFP28
Number of ports	10xSFP+; 1xQSFP28

• LINE INTERFACES

Protocol	OTU4
Optical interface	QSFP28
Number of ports	1

• MANAGEMENT

MIB	SNMP V2c private MIB
Remote management	10 Mb Ethernet DCC
Encryption management	Celestis NMS

• PHYSICAL SPECIFICATIONS

Module size	2 slots in C200HC
Operating temperature	0°C to +50°C / +32°F to +122°F -20°C
Storage temperature	to +85°C / -4°F to +185°F
Power (max.)	75W (PM_CRYPTO/PM_CRYPTO-E40) 100W (PM_CRYPTO-E100)

• INDICATORS

Status	HW ready, SW ready
Alarm	Port down *(clients and lines)*

• ENCRYPTION

Data Encryption	AES-GCM 256
Key Exchange Encryption	Elliptic Curve Diffie-Hellman
Encryption Engine Latency	0.2 us

• REFERENCE STANDARD

ITU-T Recommendation X.1035 ; ISO/IEC 18033-3

ORDERING INFORMATION

PLUGGABLE MODULE (PM)

EKINOPS CHASSIS

PRODUCT CODE	DESCRIPTION
PM_CRYPTO	Multi-rate encryption module. 10 multi-protocol clients ports *(SFP+)* to encrypted OTU4 *(QSFP28) (QSFP28 or SFP+ not included)*
PM_CRYPTO-E40	Encryption module, 2x10GbE & 2x40GbE client ports (*SFP+*) to encrypted OTU4 (*QSFP28*) (*QSFP28 or SFP+ not included*)
PM_CRYPTO-E100	Encryption module, 1x100GbE client ports (*QSFP28*) to encrypted OTU4 (*QSFP28*) (*QSFP28 not included*)
C200HC	High Capacity modular chassis 2RU
PM_MNGT4-2	Management card
400EEM	Ekinops Craft interface Software
NMS_License_initial	CELESTIS NMS initial License

CONTACT

www.ekinops.com

Ekinops EMEA
sales.eu@ekinops.com

Ekinops APAC
sales.asia@ekinops.com

Ekinops Americas
sales.us@ekinops.com