IP ENCRYPTION SYSTEM

CM2100IP is the new generation of high speed multipurpose and programmable IP encryption equipment developed for protecting IP high classified traffic to be exchanged over IPv4/IPv6 strategic and tactical networks. CM2100IP in combination with the KNMS2100IP allow the creation and management of “Secure Virtual Private Networks” (SVPN).

The CM2100IP is a ruggedized equipment with a multipurpose/programmable architecture allowing thus to be used in various operational situations at the strategic or tactical level for protecting National, NATO, UE and Coalition classified information up to maximum security levels.

Thanks to a Programmable Software architecture, the CM2100IP is upgradable (without hardware changes) to meet the upcoming NATO IPSec standard (NINE) or to implement new capabilities in terms of algorithms and networking/routing features.

Encryption devices: CM2100IP families

The CM2100IP has been specifically designed for increasing considerably the performances with respect of the legacy Crypto IP equipment (CM109IP and CM2000IP), as listed below:

▪ At least 60Mbps with National legacy algorithm and 90Mbps with NATO legacy Algorithm but maintaining the capability to operate with the legacy IP equipment
▪ At least 2.5Gbps (aggregate) by implementing the new generation of NATO and National algorithms for the NINE standard

A Crypto Ignition Key (CIK) is necessary to make CM2100IP equipment operational. The removal of the CIK also declassifies the device to “COMSEC Controlled Item” (CCI). Interconnected crypto devices form a “virtual private network” (VPN) able to protect the classified traffic, generated by “trusted” (or red) networks and conveyed over an “untrusted” (or black) IP network.
In order to guarantee the security of the exchanged data, the crypto devices use IPSEC protocol in Tunneling mode to encapsulate the IP packets.

**KNMS2100IP: Key and Network Management System**

KNMS2100IP is the HW/SW system for keys and network management. It allows an easy management of encryption device network (also including legacy CM109IP and CM2000IP family), and to electronically distribute traffic keys through the network.

KNMS consists of a standard PC with proprietary SW and an encryption device, of the same type of the ones used in the network, employed to encrypt the management traffic.

**CM2100IP CHARACTERISTICS**

**HW Features**
The CM2100IP is composed by two main units, the crypto unit and an AC/DC Converter used to feed the crypto unit with AC connections. If the AC/DC Converter is not present, the crypto unit can be feed only in DC.

The crypto unit has 3 internal sub modules, two embedded programmable routers separated by an high secure crypto core which includes a secure memory module (removable and tamper proof) capable of storing up to 4 algorithms (statically).

Only one algorithm at a time can be executed within the crypto core after a pre-selection made manually with the rotary switch on the front panel. On the frontal panel it is also possible to configure the encryption device by using the keypad, to read the status information on the display, to erase the encryption keys quickly, to extract and to substitute the back-up battery, to fill keys.

The DTE and DCE interfaces to interconnect red and black networks through crypto core and the power connector are located on the rear panel. Both on trusted and untrusted sides, two interfaces compliant to IEEE802.3 standard are available:
- 100/1000 Base-TX (100Mbps/1Gbps)
- Multimode fiber optic 1000BASE-SX
- Multimode fiber optic 10 Gbps-S

The red and the black interfaces may be configured independently. Strategic and tactical version is available.
**SW Features**
The CM2100IP are network devices supporting several routing features, compliant with IPv4/IPv6 standard. They allow the transmission of all TCP/IP suite protocols. Basic equipment configuration and monitoring are possible using display and keypad on the front panel or a Local Craft Terminal (KNMS like) running on a PC connected on DTE interface.

All CM2100IP devices support advanced features such as:
- BIT Functions
- Quality of Service (QoS)
- Multicast
- Access List
- Routing Table
- Gateway functionalities among different VPNs
- Subnet management
- Generic Routing Encapsulation (GRE) on DCE
- RIP on DTE/DCE
- OSPF on DTE/DCE
- BGP on DTE/DCE
- Virtual Router Redundancy Protocol (VRRP)
- RoHC
- TCP Accelerator
- TCP
- DHCP server for DTE networks
- Natting on DTE incoming traffic
- Remote download of IP Line interfaces SW
- Remote Update/Change of Traffic Keys

**Security Features**
The IP encryption devices create a VPN, encrypting the data exchanged among the sub-networks that they protect. The CM2100IP encryption devices must be installed at the access point of the sub-network to be protected and before the access router to the geographical network.

The access router is not required in case the available interface to the geographical network is compliant to the Ethernet standard. The IP packets to be transmitted from the trusted to the untrusted network are encapsulated in a new IP packet (IPSec encapsulation).

CM2100IP encryption devices guarantee the following security services:
- Data confidentiality
- Data integrity
- Authentication
- Trusted IP address protection
- Data Re-sending protection
- Secure remote management

In order to increase the device physical security, several mechanisms have been implemented:
- “Erase” switch
- Anti-tampering mechanisms
- CIK (Crypto Ignition Key) to enable/disable the device and to allow a rapid declassification to CCI
- Removable Crypto Memory Module
- Manual loading of the Unique Key for management link, through Fill Gun or Tape Reader

**Encryption Algorithms**
CM2100IP Encryption devices can be configured with the following encryption algorithms:
- NATO and National legacy algorithms (for backwards interoperability with CM109IP/CM2000IP legacy IP equipment)
- UE
- Coalition
- NATO/National algorithms to be used for the NINE standard

**KNMS2100IP CHARACTERISTICS**

KNMS2100 is the management system for networks of IP encryption devices. KNMS2100 has been developed to securely manage both network and security features of the CM2100IP encryption devices belonging to the same VPN.

KNMS comprises:
- A Client/Server Management Software, to be installed on standard PC.
- One CM2100IP, named Local CM, to distinguish it from other IP crypto devices belonging to the VPN network, referred to as Remote CM.
- A key loading device (Fill Gun, Tape Reader, DTD)

KNMS2100IP allows the remote administration of:
- Encryption links (creation, enabling, disabling)
- Traffic keys (change, uploading)
- Network configuration (IP address, Default gateway, etc.)
- Advanced functionality management (Subnets, QoS, Multicast, Default CM, Access List, etc.). These features can be configured only through KNMS system
All commands and information exchanged between KNMS2100IP and the network encryption devices are delivered through the Management SVPN.

The Management software uses a client/server architecture, so it is possible to install the two applications on different PCs. In particular, it is possible to install the client application on different terminals, to let different users perform network monitoring.

The management station where the server application is installed is used to store the database of all the Remote CM keys and network configurations. All the keys stored in the PC are encrypted.

FEATURES

General
▪ Supports dual stack IPv4/IPv6 protocols
▪ Supports IPSEC (RFC 2401)
▪ Supports ESP-Encapsulating Security Payload (RFC 2406) in tunneling mode

Network interfaces
▪ 100/1000 Base-TX
▪ Multimode fibre optic 1000BASE-SX
▪ multimode fibre optic 10 Gbps-S

Additional features
▪ Access List
▪ Multicast
▪ GoS
▪ VRRP
▪ Static and dynamic routing (OSPF, RIP and BGP)
▪ Tunnel GRE
▪ RoHC
▪ TCP Accelerator
▪ Natting
▪ DHCP Server
▪ Remote Software Download

Encryption keys
▪ Key loading: local (Fill Gun, Tape Reader) or remote (KNMS Management System)
▪ Key loading standard: DS101/DS102 protocol
▪ Key preservation in case of power outage

Security services
▪ Data confidentiality (encryption/decryption)
▪ Authentication
▪ Data integrity
▪ Traffic security (encryption of “red” IP addresses)
▪ Anti-Replay Attack (Data Re-sending protection)

Security
▪ NATO and National (Italy) approved up to NATO SECRET
▪ NATO, National and Customized or Proprietary algorithms
▪ Equipment enabling by CIK: declassified to CCI when CIK is removed
▪ Anti-Tampering mechanism
▪ Key zeroization in emergency
▪ Tempest compliant SDIP-27/1 Level A

Management
▪ Built in Test (BIT)
▪ System and Security Alarms
▪ Local Event Log
▪ Local control: display/keypad use on the front panel
▪ KNMS, via encrypted IP network (Management VPN)

Electrical features
▪ Supply: 115/220 Vac or 48 Vdc
▪ Power consumption: 100W max (strategic version) – 80 W (tactical version)

Physical data
▪ Dimensions (W x D x H): 90mm x 450mm x 500mm (strategic version) – 90mm x 290mm x 470mm (tactical without AC/DC converter)
▪ Weight: 17Kg (strategic version) – 11Kg (tactical version without AC/DC converter)

Environmental data (Strategic Version)
▪ Operative temperature: -32ºC/+40ºC
▪ Storage temperature: -33 ºC/+71 ºC
▪ Relative humidity: form 20% to 80%
▪ Storage altitude: 10,000m

Environmental data (Tactical Version)
▪ Operative temperature: -32ºC/+55ºC
▪ Storage temperature: -33 ºC/+71 ºC
▪ Relative humidity: 93% ± 5% @ 30ºC
▪ Storage altitude: 10,000m
▪ Operative altitude: 2,000m