Defence Communications Systems

ELECTRONIC KEY MANAGEMENT SYSTEM

Electronic Key Management System (EKMS) is an integrated and automatic system specifically designed for enhancing the distribution process of cryptographic material. It reduces time, resources and cost when compared to commonly used manual procedures.

It provides greater intrinsic assurance of key distribution process and facilitates interoperability among military agencies involved in the distribution of cryptographic material.

EKMS performs ordering, distribution and accounting to implement the management and distribution processes of electronic COMSEC material for ECUs.

It is:

- Modular, for easy distribution of skills with respect to roles and regulations
- Scalable, to allow easy adjustment in the event of changes in the organisation
- Dynamic system configuration for temporary needs, such as distribution of cryptographic material in an operation area

KEY BENEFITS

- Management of crypto keys in all phases of the lifecycle: planning, ordering, storage, distribution and destruction
- Preserve confidentiality and integrity of crypto material
- Technological enhancements represented by electronic data stored and transmitted over IP secure networks, replacing physical keys and related complex procedural management processes
- Near instantaneous distribution of cryptographic material
- Effective rationalization of key planning and orders, which allows strong reduction of keys to be provided in advance
- Improved inherent threat protection by decreasing human treatment of keys during their lifetime
- Immediate traceability of key position and status through mechanisms of accounting system
- Common Criteria EAL3 security certification (LMD and KNMS applications)
- Strong reduction of human resources necessary to manage and deliver cryptographic material: cost saving and secure solution.

EKMS

EKMS allows the distribution of single cryptographic keys and multiple or complex files of keys. The transmission network is IP-based - protection is provided by approved crypto equipment with the creation of dedicated VPNs (Virtual Private Networks).

Classified information is stored encrypted within System components, data exchange between them is always properly protected with approved encryption algorithms across the entire workflow.

The supply of cryptographic material (by external key generation systems) to EKMS is via AirGap mode. Key loading and key export from single workstations to EndPoint Cryptographic Units (ECU) is via a Fill-Device, supporting standard DS-101 and DS-102 (EKMS-308) protocols. The system can be customized to support non-standard key types and non-National Customers.

The user interface is clear, intuitive and process-oriented, while the system makes use of commercial computers and software with appropriate security configurations.

Accessibility to resources and system data is based on the operators specific role, in accordance with the principles of need to know and least privilege.

3-TIER SYSTEM ARCHITECTURE

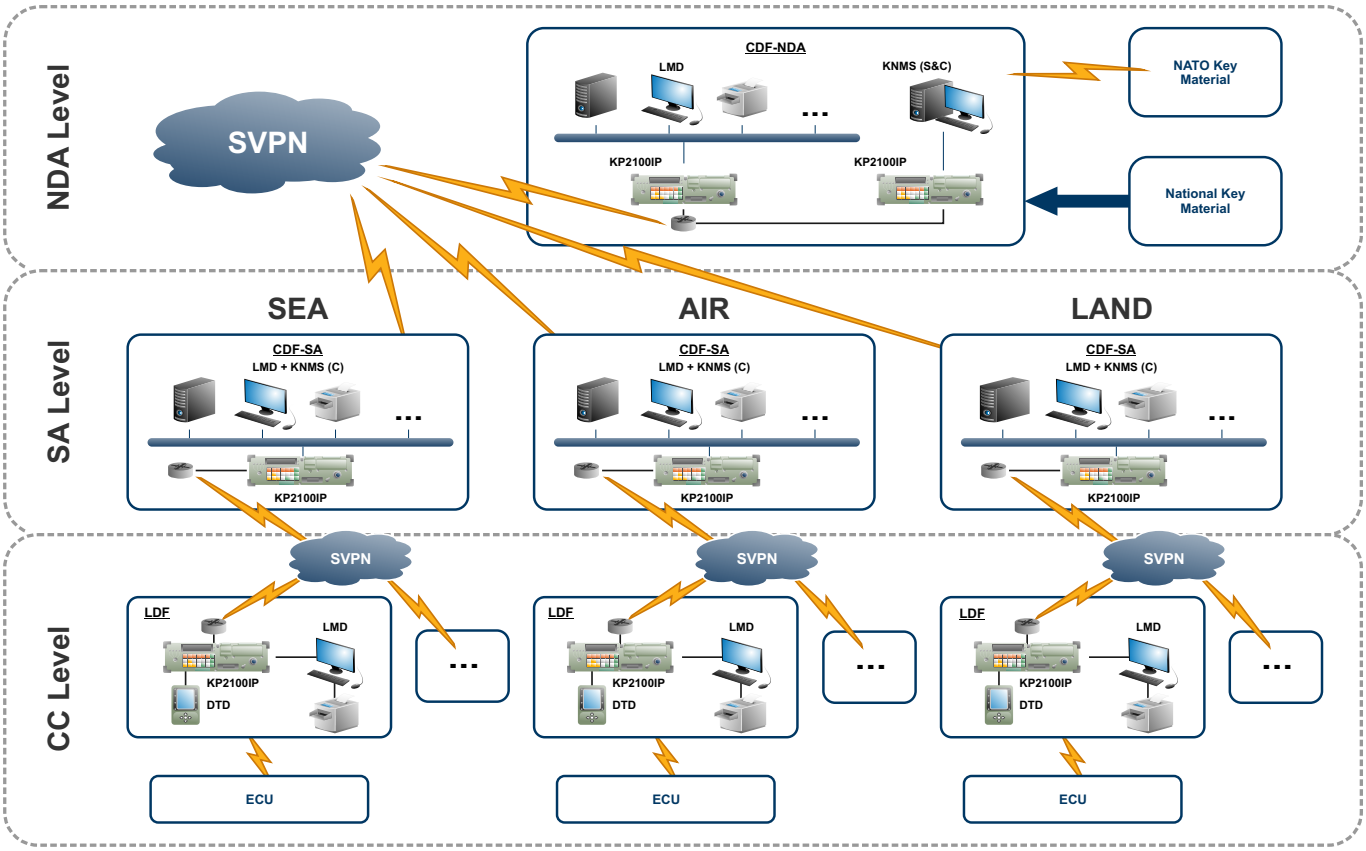
CDF-NDA (Central Distribution Facility - National Distribution Authority) (Tier-0)
This is the entry point of all cryptographic material to be distributed and performs:
Management of planned orders of cryptographic material from lower levels, forwarded via air-gap to external systems responsible for the generation of cryptographic material
Delivery of generated cryptographic material to the stations on the lower level CDF-SA
Receiving and management of the reporting of cryptographic material distributed on the network

CDF-SA (Central Distribution Facility - SubAgency) (Tier-1)
This represents the Sub Distribution Agency and performs:

- Key ordering to NDA based on needs received from LDF
- Distribution of cryptographic material received from NDA to dependent LDF
- Exchange of logging and accounting information with NDA and dependent LDFs

LDF (Local Distribution Facility) (Tier-2)
This represents the receiving Agency final collection station of cryptographic material and performs:

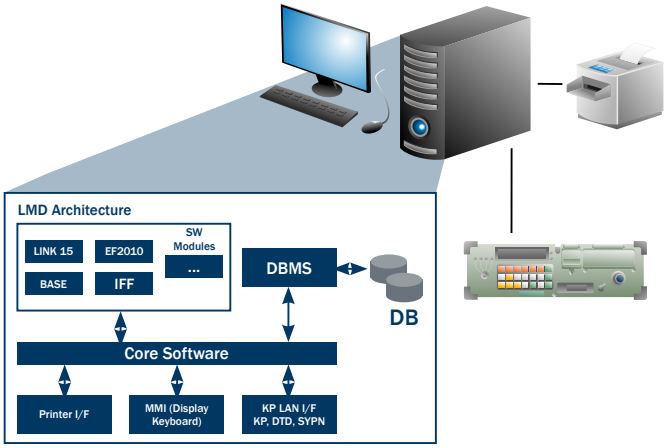
- Key management - receiving and loading keys on ECU
- Planning of key needs and delivery to SA
- Key loading on EndPoint Cryptographic Unit (ECU) through “fill device” IT-DTD



SYSTEM COMPONENTS

Local Management Device – LMD

- Used at CDF-NDA, CDF-SA and LDF levels
- Running on a COTS PC with appropriate software applications
- Equipped with distributed DataBase with its management software and applications required to manage the cryptographic material
- Exchanging data with local key processor: commands and status information
- Role and hierarchical location dependent: management of cryptographic material, orders and records events about EKMS infrastructure



Key Processor – KP

- COMSEC and TEMPEST (SDIP-27/1 Level A) equipment, approved for classified information handling ; it is a part of all EKMS network nodes
- Cryptographic material encryption and decryption functions
- VPN establishment, connecting EKMS network workstations

Key and Network Management System – KNMS

- Management system for Key Processors
- Based on a hardware/software client-server architecture
- KP configuration and monitoring (alarms and status) and provisioning/monitoring of secure connections (VPNs)
- Management of all EKMS KP network (from NDA) or monitor of dependent KP network (from SA)

Data Transfer Device – IT-DTD

- Handheld computer used for key loading on EndPoint Cryptographic Units (ECUs)
- EKMS-308 protocols
- Storing and decryption of keys during key loading on ECUs
- COMSEC and TEMPEST (SDIP-27/1 Level A) device, approved for processing classified information

EKMS

TECHNICAL SPECIFICATION

SYSTEM	
NATO and National Keys electronic distribution	
Multi-layer system, with modules at	NDA level Sub-Agency level (CDF) Crypto Custodian level (LDF)
Modular system, Composed of as many CDFs and LDFs as needed	

LOCAL MANAGEMENT DEVICE	
PC with Certified Operating System (Windows family)	
Specialized software	NDA/Management Station NDA/Server Station CDF/Management Station CDF/Server Station LDF/Operator Station

KEY PROCESSOR
IP based encryption device
10/100Base-TX DTE and DCE interfaces
Offline and online encryption algorithm on-board

SECURITY
NATO and National (Italy) approved algorithms
Anti-Tampering mechanism
TEMPEST tested (SDIP 27/1 Level A)

MANAGEMENT	
Local control	Display/keypad use on the front panel
Dedicated "Key and Network Management SW" (KNMS) to control KP network, via encrypted IP network (Management VPN)	

ELECTRICAL FEATURES	
Supply	115/220 Vac ± 15% @ 45-63Hz or 48V ±15% Vdc
Power consumption	180W max

PHYSICAL DATA	
Dimensions (w x d x h)	387mm x 479mm x 95mm (19" rack mountable using an optional kit)
Weight	14Kg

ENVIRONMENTAL DATA	
Operating temperature	-20°C / +44°C
Storage temperature	-33°C / +71°C
Altitude for trasnportation	15,000m

DATA TRANSFER DEVICE	
Capable of storing key material in encrypted form	Application Key Traffic Encryption Key (TEK) Key Encryption Key (KEK) Transfer Key Encryption Key (TrKEK) Certificates Mission Management Information
Can receive data from TR101 Tape Reader	
Can send/receive keys to/from FG101 Fill Gun	
Can transfer keys to/from devices supporting DS101 and DS102 protocols (now described in "EKMS 308 Rev F" standard)	
Can interpret key tagging information as defined in EKMS 308	
Maintains accounting information on keying activity i.a.w. SDIP 293 and AC/322-D(2006)0069, together with a log on any user activity and alarms.	

SECURITY
Capable of encrypting and decrypting key with NATO and National (Italy) approved algorithms
Anti-Tampering mechanism
TEMPEST tested i.a.w. SDIP-27/1 Level A
Access to stored keys and classified accounting information is protected by a physical token (Crypto Ignition Key, CIK) to control unauthorized access to classified data.
Emergency erasure of classified keying material and classified accounting data.

ELECTRICAL FEATURES	
Power supply	Rechargeable battery, with supplied AC-DC converter (100 – 240V AC, 47Hz – 63Hz)
Operating time	>8 hours when fully charged
Storage time	>32 days when fully charged

PHYSICAL DATA	
Dimensions (w x d x h)	< 60mm x150mm x 200mm
Weight	1.3Kg

ENVIRONMENTAL DATA	
Operating temperature	20°C to +50°C
Storage temperature	-40°C to +65°C
Relative humidity	90% @ 40°C
Storage altitude	10,000m
Operating altitude	4000m

LEONARDO
LAND & NAVAL DEFENCE ELECTRONICS

For more information please email infomarketing@leonardocompany.com
Leonardo - Finmeccanica S.p.A.
Via Laurentina, 760 - 00143 Rome - Italy - Tel: +39 06 50271 - Fax: +39 06 5051140