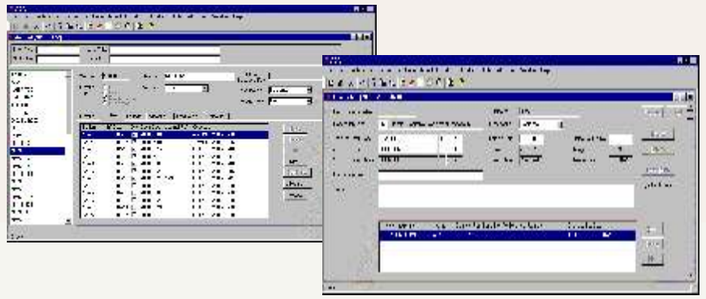
EKMS User Interface

The EKMS Accounting and Distribution Application (ADA) provides complete control of all cryptographic material. ADA is present at the NDA, SubDA and LDA level and has the main user interface in the system.

Through a standard user friendly Windows Interface the local operator defines material, plans and accounts. The planning involves production and stockpiling of key material at different locations. Electronic production plans are forwarded to the production system and electronic keys are returned to the database for secure storage. Keys are further distributed to SubDA and LDA for reproduction or transfer to crypto equipment. Double book-keeping based on approved transactions provides up-to-date accounting of all material at any time.

The main available functions:

- Planning of production and distribution
- Production and reproduction of keys
- Complete accounting for all crypto material
- Distribution of electronic keys and accounting data
- Request handling and report generation
- Management of users and audit logs



EKMS
Security Features

No cryptographic systems can be better than the way you manage your keys. EKMS provides optimal key protection during the complete key life-cycle. The security features of EKMS ensure that keys are protected from unauthorised access or modification during storage and distribution.

Cryptographic protection

Electronic keys are produced in a physically secured production system and encrypted in the TCE 121 (KPE) during transfer to the accounting and distribution system. The KPE will add integrity protection based on Message Authentication Codes. Additional network encryption will protect key material and accounting data during distribution to sub-ordinate nodes.

Physical protection

The red production system is connected to the rest of the system through the KPE. The KPE will not allow that information can pass from black to red side. Orders to the production system are transferred manually. Key material is passed to secure Data Transfer Devices or via reproduction equipment for transfer to cryptographic equipment. Encryption and the secure Military Message Handling System (MMHS) is used for safe distribution of information between EKMS nodes.

Secure management

Role based access control to EKMS applications ensures that critical functions are restricted to authorised personnel.

NATO approval

The EKMS system has been evaluated and is approved by NATO.

THALES

THALES Communications
P.O. Box 22 Økern ~ 0508 Oslo ~ Norway ~ Phone: +47 22 63 83 00 ~ Telefax: +47 22 63 79 44
www.thales-communications.no ~ info@thalesgroup.no

THALES COMMUNICATIONS

EKMS

Electronic Key Management System

...a new solution to an old problem!

EKMS
THE ELECTRONIC KEY MANAGEMENT SYSTEM
FOR SECURE HANDLING AND ACCOUNTING OF CRYPTO MATERIAL

A complete system for handling of crypto material

EKMS is an effective tool for management of crypto keys in all phases of the lifecycle; planning, production, storage, distribution and destruction. EKMS also supports management of physical crypto material by utilising the planning and the accounting facilities.

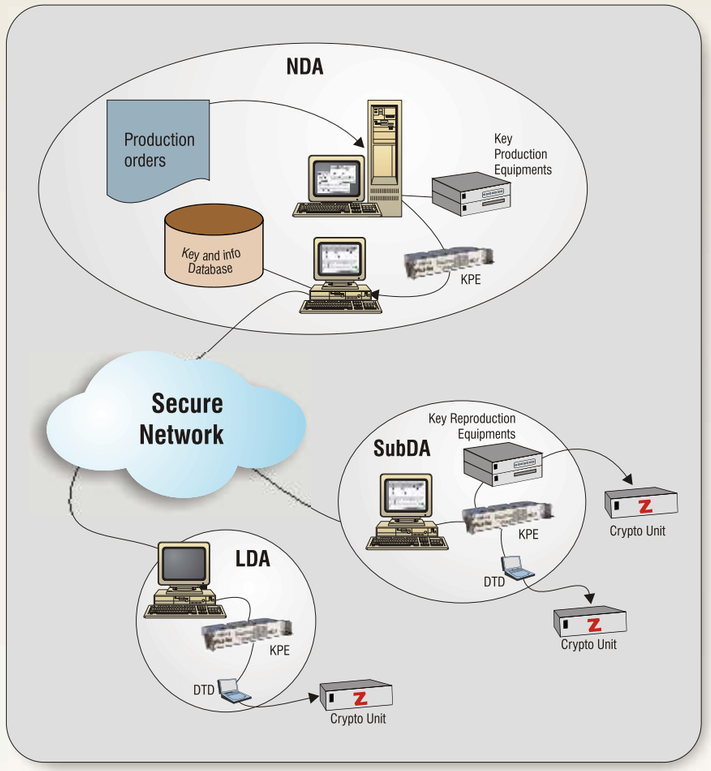
Crypto Key Management a challenging topic

The keys are critical in a crypto system. To maintain the intended security level, it is essential to preserve the confidentiality and integrity of the keys. Crypto keys must be produced and distributed according to predefined plans and accurately accounted for and traceable all the time.

Traditional key management based on manual couriers has a considerable risk for loss and compromising, and is time consuming and expensive.

- electronic handling is the solution

EKMS offers a cost saving and secure solution to all aspects of key management. Secure electronic storage and distribution of crypto keys will reduce the volume of storage and distribution of physical keys. Reduced manual handling will not only reduce cost, but most important reduce distribution time and increase the security.



Legends:

NDA: National Distribution Authority
SubDA: Subordinate Distribution Agency, can be one or more SubDAs within EKMS
LDA: Local Distribution Agency, the nodes from where keys are transported to crypto units
KPE: Key Processor and Encryptor (TCE 121), performs encryption of all keys handled by EKMS
DTD: Data Transfer Device

Management of physical crypto material

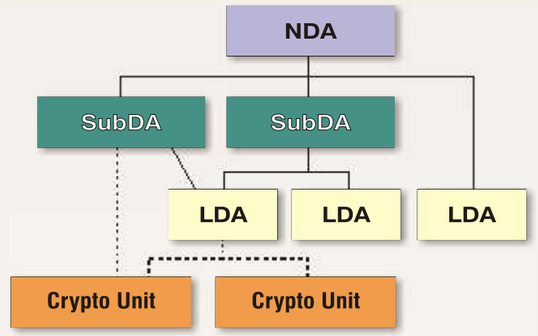
Most physical crypto material (e.g. equipment and publications) must be handled according to similar rules as crypto keys, and EKMS provides functionality for efficient accounting of such material. Transactions of the material are accompanied by electronic messages which updates the accounts of the material holders within EKMS. Receipts are returned upon reception of the material, and all the involved accounts are automatically updated.

Functionality supported by EKMS

- **Initial planning**: Define all accounts (holders) and corresponding material allocation. Define cryptographic network interconnections. Specify the key material for each supported crypto unit in terms of type, edition, effective date and destruction date. Specify and make key and other crypto material allocations to different accounts.
- **Production**: Produce the key variables in due time before use.
- **Storage**: Store the keys in encrypted form until distribution to user location.
- **Distribution**: Distribute keys electronically through EKMS from NDA to SubDA or LDA in encrypted form.
- **Transfer**: Transfer electronic keys to Data Transfer Device or to reproduction equipment.
- **Reproduction:** Convert electronic keys to physical medium, e.g. to tape, diskette or to smartcard.
- **Destruction**: Issue destruction reports when needed and register destruction of keys and material.
- **Accounting:** Keep track of possessions and responsibility through all phases of the lifetime of keys and material. All transfers are subject to registrations and accounting.

Arrangement of EKMS nodes

- An EKMS network is typically configured as a hierarchical system.
- At the NDA level, system definition, planning, key production and accounting are accomplished for the complete system.
- A SubDA is an intermediate level where accounting is performed for the subordinate nodes and requests for new keys from subordinate nodes are approved.
- The LDA performs local accounting, and key requests can also be initiated from this level.
- At each level, crypto keys can be transferred to Fill Devices or reprod-uced to physical media for transfer to crypto equipment.



EKMS benefits

- Minimal manual handling of crypto keys
- Reduced risks
- Easy configuration of crypto networks
- Cost savings

Electronic Key Management System - Building Blocks

Production/Reproduction Subsystem
Produces key variables from true random source and makes correct key formats. During reproduc-tion are keys transformed from electronic to physical medium or loaded to an electronic transfer medium.

Accounting and Distribution Application
Handles the accounting and planning functionality including information about the supported crypto equipments and networks. Makes production, reprod-uction and distribution orders, and contains the main operator interface of EKMS.

Crypto Subsystem
Takes care of the confi-dentiality and integrity of the key material within EKMS. All encryption functions are performed in hardware by the KPE.

Communication Subsystem
Communication between EKMS nodes is using an X.400 Military Message Handling system inter-connected by means of a secure IP or X.25 network.