

DEFENDING WORLD SECURITY



SECURE KEY Management Solution

Secure Key Management Solution (SKMS) from AIRBUS is a complete solution for cryptographic key generation, management and distribution. This has been developed on proven technology and capability to meet the evolving needs to maintain and provide secure communications systems.

The move towards an integrated and informed battle-space has led to an increased number of communications systems and associated cryptographic devices for maritime, land and airborne systems. Fast, secure and reliable transfer of cryptographic key material is essential to maintain an effective communications network in high tempo operations.

SKMS improves mission responsiveness, and brings the opportunity to realise major through-life cost savings. SKMS also supports the investment in legacy crypto systems while allowing the transformation of National Key Infrastructures to new business models.

AIRBUS

The network centric environment, in which modern military installations operate, requires multiple communications systems. The high demands for security necessitates numerous cryptographic protection devices, each of which have different requirements for key variables and fill devices. Key generation, transmission and management has traditionally been a time consuming and labour intensive task, often requiring staff to manually transport key material in paper-tape format across long distances to support short-notice requirements. Against a backdrop of budget challenges, reducing staff numbers and the need to reduce response times, there is a requirement for efficient key distribution and management without compromising security. SKMS brings together AIRBUS's portfolio of Key Management products to meet the demands for a highly responsive, secure and flexible SKMS solution. Secure management of electronic key material improves flexibility for out-of-area operations and eases the burden of manual transfer and loading of key material by COMSEC custodial staff.

Benefits

SKMS brings together 4 elements of AIRBUS's Key Management portfolio in a single solution for the management of key material including:

Key Generation

SKMS enables the generation of electronic key variables for national use, removing the reliance on third-parties for the production and management of key material. Self generation of electronic key material can support training, trials and operational activities.

Secure Key Conversion

The system provides the facility to convert different formats of key material provision into a generic secure electronic format providing the facility to support legacy crypto using modern electronic fill devices and distribution chains. This also allows business transformation to continue maintaining legacy system capability yet underpinning and enabling future distribution strategies.

Platform Key Management

SKMS eliminates the need for expensive and time-consuming manual crypto key distribution systems through the use of an integrated key management system flexible enough to be tailored to specific user requirements.

Key Transmission Encryption

(ECTOCRYPT® Blue and Crypto Converter) SKMS also provides highly secure key distribution utilising IP and file encryption based upon UK Government High Grade specifications. It is designed to be transparent to the user community, whilst also providing Confidentiality, Integrity and Availability services, and enables the transfer of key material securely over unprotected networks.

Significant Through Life Cost Savings

SKMS enhances operational effectiveness by improving the speed and integrity of the distribution of key material, and also offers

improved flexibility in responding to short-notice key changes. As a result, large throughlife cost savings can be realised. SKMS provides the complete solution and is a major enhancement in support of secure communication networks.

Technical Specifications

Key Management

- Complete Secure Key Management Solution to meet the demands for highly secure data management
- Key transmission over insecure networks through the use of high assurance IP and file encryption devices
- Flexible key management over a distributed architecture
- Fully customisable to meet specific customer requirements
- Distributed architecture that allows hierarchical management of key accounts
- Full accounting and user management
- Push and Pull delivery of key material

Interfaces/Protocols

- DS-101 – Intelligent Fill Interface
- DS-102 – Common Fill Interface
- EKMS 319

Electronic Key Generation

- Self generation of dedicated electronic key material to meet national requirements

Key Conversion

- DS101/DS102 interfaces
- Variable configuration to meet specific user needs for input and/or output
- Translation of physical key to secure electronic format

Key Transmission Security

- High assurance IP and file encryption
- 10Mb-1Gb full duplex throughput
- High Grade Algorithms, others available e.g. AES 256

Certification Features

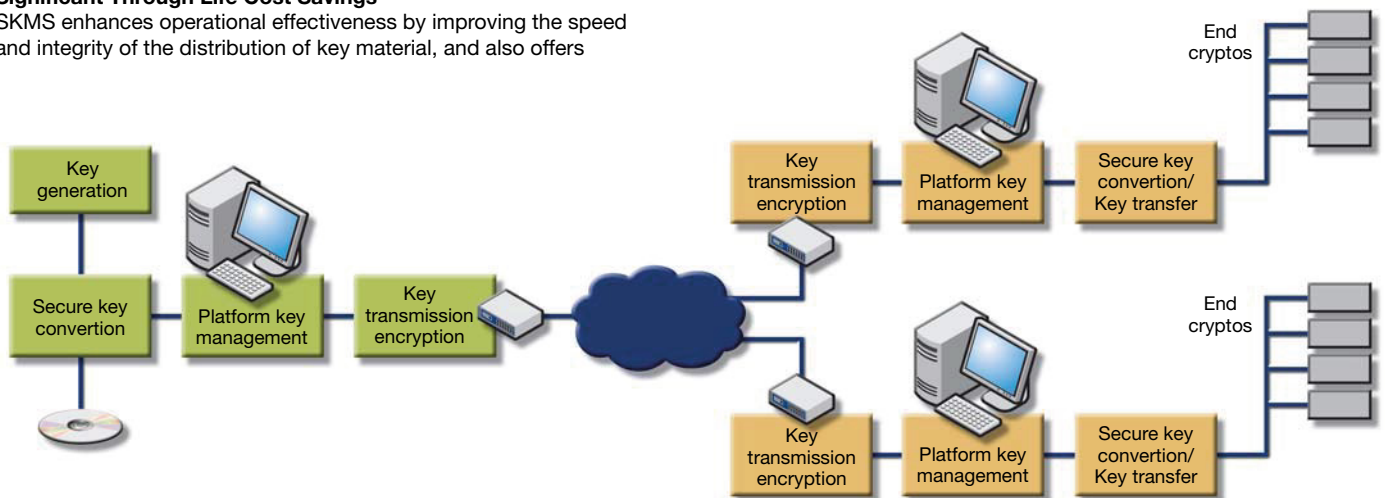
- High assurance COMSEC approved devices
- Tempest Approved
- CE Approved

Security Features

- Tamper Proof
- Tempest Certified

Safety

- Compliant with relevant EEC Directives



Airbus
MetaPole
1, Boulevard Jean Moulin
CS 40001
78996 Elancourt Cedex - France

Airbus
Landshuter Str. 26
85716 Unterschleissheim
Germany

Airbus
Quadrant House - Celtic Springs
Coedkernew
South Wales - NP10 8FZ
UK
Phone +44 (0) 1633 713000
Fax +44 (0) 1633 713333
Email: ukinfo@airbus.com

AIRBUS