![L3HARRIS® FAST. FORWARD.]

RF-KMS-001

Key generation capability for L3Harris high-assurance radios

The key management system (KMS) is a key generation capability that allows users of high-assurance radios to generate sovereign national authenticated pre-placed keys (APPK). It removes the need to obtain key material from a third-party key production agency when supporting national CONOPS.

The KMS uses the proven CATAPAN global key management system which is an off-the-shelf solution for full sovereign key generation and management. Leveraging over a decade of experience in government grade encryption and a catalog of award-winning products, the key management system provides users a high level of confidence in the system and the generated key material.

The KMS comprises a bespoke hardware security module (HSM) that incorporates dual high-assurance entropy sources with an intuitive PC-based management environment incorporating COTS database technology.

The KMS generates authenticated pre-placed keys (APPK) for onward loading into a suitable fill device such as the L3Harris KIK-11 Tactical Key Loader (TKL). The TKL is field-proven and provides key fill capability into L3Harris radios.

Each APPK is unique to a customer and is verified by a Trust Anchor that is specific to the customer. This approach assures, to the highest level, the integrity and authenticity of the key material.

The KMS provides control over the design, generation and management of the cryptographic keys for the L3Harris high-assurance radios.

All generated key material is backed up in a high-security data vault using a COTS database structure. This ensures a robust and resilient backup is readily and easily implemented. In addition, the security process is easily auditable.

PROVIDES SECURE SUITE B COMMUNICATIONS TRAFFIC USING AUTHENTICATED PRE-PLACED KEYS

KEY BENEFITS

> Allows for sovereign operations by high-assurance radio users
> Increases operational agility
> Improves mission effectiveness
> Mitigates dependency on a third-party key management system
> Brings the resilience, versatility and capabilities of the Falcon Net Ecosystem™ to the cockpit
> User has control over key generation and management
> Produces authenticated pre-placed keys for use with Suite B traffic encryption radios
> Supports import and generation of key trust anchor and signing key

L3Harris.com

Key Management Utility, PC Hosted

Key Management System

KIK-11 TKL

Scenarios
> System set up
> Generation/loading of key material
> Loading of key material into secure radios

Deployment

High-Assurance Radios

Scenarios
> Maintenance
> Loading of key materials into secure radios

TECHNICAL SPECIFICATIONS

Interoperability	The CATAPAN Global KMS produces customer-specific authenticated pre-placed keys (APPK) for loading into a suitable electronic fill device
Cryptographic Specification	Database protection algorithm: AES 256 Key Wrap
Keys Generated	TSVCIS Suite B Key, NATO NINE APPK

PHYSICAL

Max Ethernet Rate	Greater than 300 Mbps
Dimensions	1.57 H x 7.44 x 5.28 in 4.0 H x 18.9 W x 13.4 D cm
Weight	~ 1 kg
Power Consumption	~10 watts
Interfaces	**Management port:** 10/100 BASE-T wired 802.3 Ethernet USB to RS232 Datakey SPI token

MANAGEMENT

Local management	Standards based using SNMPv3, supplied with bespoke management application, incorporating graphical user interface (GUI)
Compatibility	AN/PRC-117G, AN/PRC-152A, AN/PRC-158, AN/PRC-163, AN/PRC-167

ENVIRONMENTAL

Operating range	32°F to 122°F (0°C to 50°C)
EMC	Electromagnetic Compatibility Directive 2004/108/EC

L3Harris can provide security consultancy on the concepts, design, implementation and management processes for the KMS. In addition, we can work with customers to integrate the KMS into their existing key management processes.

L3HARRIS®

1025 W. NASA Boulevard
Melbourne, FL 32919

L3Harris.com