SAFECOM®

Federal Partnership for Interoperable Communications (FPIC)

NCSWIC®

Encryption Key Management Fact Sheet

What is encryption key management?

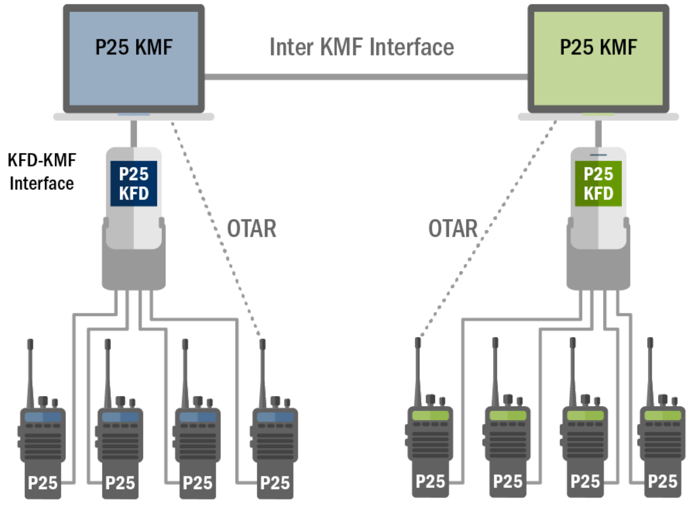
Encryption key management is the administration of policies and procedures for protecting, storing, organizing, and distributing encryption keys. Encryption keys (also called cryptographic keys) are the strings of bits generated to encode and decode data and voice transmissions. Effective encryption key management is crucial to the security of land mobile radio (LMR) communications and the sensitive information those communications contain. In addition to ensuring security, key management also ensures that encryption does not impede the interoperability of LMR systems and radios within and among agencies.

Why should I encrypt radio transmissions?

There are several reasons to encrypt LMR transmissions, the foremost reason being operational integrity. Scanners and smartphone applications enable almost anyone to monitor public safety radio traffic and eavesdrop on everything from tactical law enforcement communications (potentially endangering law enforcement personnel) to emergency medical communications containing sensitive patient information. Encryption can keep such transmissions private within the public safety sphere. This does not mean all channels need to be encrypted; each agency should determine which information and channels require encryption.

How are encryption keys managed?

Encryption keys are managed using key management facilities (KMFs) and key fill devices (KFDs). KMFs are secure devices that generate encryption keys, maintain secure databases of keys and securely transmit keys to KFDs. Keys are distributed to subscriber units (individual LMRs) either by direct connection to a KFD or via over-the-air-rekeying (OTAR) from a KMF.



Why is key management important?

The secrecy and security of encryption keys are the foundation of effective encryption. Key management maintains secrecy and security by controlling the distribution of keys and reacting immediately if an encrypted radio is lost or stolen. A lost or stolen radio that falls into the hands of an unauthorized user can compromise the security of the entire LMR system. Key management requires that such a radio be disabled remotely and new encryption keys be issued to all subscriber units.

Does key management affect interoperability?

Key management maintains the interoperability of LMR systems and radios by ensuring that all radios within the system have the same encryption algorithm and keys, enabling them to talk to one another. Just as important, good key management policies ensure that encryption keys are shared with partner agencies to maintain fully interoperable communications in mutual aid situations. Balancing security and interoperability is one of the core objectives of key management.

What encryption algorithm should I use?

Several encryption algorithms are available; however, they are not equal and do not offer the same level of security. Advanced Encryption Standard (AES) 256 is the only recommended algorithm by the U.S. Department of Commerce's

National Institute of Standards and Technology (NIST). Less secure algorithms, such as the Data Encryption Standard (DES) and various manufacturer-proprietary algorithms, are not recommended for use in Project 25 (P25) systems.[1]

Under SAFECOM Grant Guidance, if a radio is purchased with any form of encryption or manufacturer-proprietary algorithms, it must include AES 256 to be eligible for grant funding.

How often should encryption keys be changed?

Encryption keys should be changed regularly to minimize the risk to LMR communications. How often the keys are changed should be determined by agency policy. The use of static keys— keys used more than once over a long period of time without being changed—is strongly discouraged.

Interoperability with Federal Partners

Although commonly used in public safety radio systems, DES 56-bit encryption is far less secure than the recommended AES 256-bit algorithm. DES, developed in 1977, was cracked by the Electronic Frontier Foundation in 1997 in 84 days. It was cracked again in 1998 and twice in 1999, each time in fewer and fewer days. In 2017, claims surfaced that the DES algorithm was cracked in 25 seconds. NIST withdrew its approval of DES as an encryption standard in 2005, and since then AES has been the federal encryption standard. Federal Information Processing Standard 140-2 requires all federal agencies to use AES encryption and, as mandated by the Cybersecurity Enhancement Act of 2014, any state or local agency wishing to interoperate on a federal LMR system must also have AES encryption on their subscriber units.

What is the National Law Enforcement Communications Center?

The National Law Enforcement Communications Center (NLECC), part of U.S. Customs and Border Protection (CBP), provides encryption key services nationwide to federal, state, and local agencies. It generates and distributes national interoperability keys and can generate specific keys for an agency's use. The center has specific requirements for its services, and agencies are strongly encouraged to contact the center for further information. For more information about the NLECC, please send an email to nlecc-wsoc@cbp.dhs.gov.

For More Information

For more information, please send an email to FPIC@cisa.dhs.gov.

[1] This document focuses on encryption protocols for voice services. Other algorithms are available for purposes such as data and authentication.