Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems

September 2016

SAFECOM

Federal Partnership for Interoperable Communications

NCSWIC

Contents

Preface

As the public safety user community has continued to recognize the importance of protecting sensitive information, the interest in encrypted communications has steadily increased. This document specifically addresses the complex issues of key management and the importance of common procedures. As was the case for two previously published documents addressing encrypted communications noted in the *Introduction*, the incentive for this document came from a request from the state and local public safety community, particularly the non-federal members of the Federal Partnership for Interoperable Communications (FPIC) Security Working Group (SWG) to provide guidelines and best practices to be considered when implementing encrypted communications. It is essential that the design and operation of mission critical radio systems enable voice and data communications that are protected from unauthorized reception as well as provide communications interoperability as required.

There were a significant number of public safety officials and systems administrators that recognized the importance of encryption and the need to address common key management methods. This document begins to outline how key management can be approached in a standard way so that the coordination of key parameters can help to enhance encrypted interoperability at all levels of government. In addition, a *Fact Sheet* has been developed to accompany this document that provides a high-level summary of the key facts, issues, and recommendations for the encryption of public safety radio systems at all levels of government.

This report is a result of an extended effort by the Federal Partnership for Interoperable Communications (FPIC) Security Working Group[1] and other contributing individuals, agencies, and organizations outlined in Appendix C. In addition, the FPIC wishes to acknowledge the valuable input of the following groups and organizations: Department of Homeland Security OneDHS[2], SAFECOM EC[3], NCSWIC EC,[4] SAFECOM-NCSWIC Technology Policy Committee, and the DHS Southwest Border Communications Working Group[5]. It is important to note that there are significant governance, policy, and training implications that must be considered with the use of encryption.

[1] The FPIC is recognized as a technical advisory group to SAFECOM and the ECPC.
[2] OneDHS worked to coordinate and integrate communications activity within DHS.
[3] SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters
[4] NCSWIC assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices to ensure the highest level of interoperable communications across the nation.
[5] SWBCWG serves as a forum for F/S/L/T agencies in Arizona, California, New Mexico, and Texas to share information on common communications issues; collaborate on existing and planned activities; and, facilitate federal involvement in multi-agency projects within the Southwest Border Region.

1. Executive Summary

The encryption of public safety land mobile radio systems is a decision that many public safety agencies are contemplating or have made in recent years. It is a primary method of mitigating threats from the potential compromise of personal or sensitive data and can enhance operational security as well as improve interoperability. Protecting land mobile radio systems and the information they transmit from unauthorized interception and use is increasingly important to maintaining effective public safety communications.

Successful encrypted interoperability depends largely upon improved coordination between agencies that need to interoperate. It is also enhanced when all agencies understand how the use and coordination of key management parameters can affect their ability to interoperate. It is vital that agencies implement encryption and key management in a consistent manner and in collaboration with other public safety agencies.

The *Best Practices* discussed in this document provide an understanding of how basic key management parameters are related in Project 25 land mobile radio (P25 LMR)[6] systems. In addition, the document addresses improved coordination of these elements, and the use of standards-based encryption can enhance encrypted interoperability while minimizing the risk of compromising sensitive information. Examples of these *Best Practices* are listed below.

- **Key Management Organization** – Develop an effective key management structure.
- **Key Generation and Distribution** – Adopt P25 standard key parameters for enhanced interoperability.
- **National SLN Assignment Plan** – Adopt a standardized Storage Location Number (SLN) plan to minimize conflicts.
- **Standards-based Encryption** – Use P25 standard AES-256[7] security solution to protect against compromise.
- **Crypto Period Considerations** – Use defined crypto periods to mitigate risk.
- **Communications Planning** – Develop Communications Plans that incorporate encryption requirements.
- **Education and Training** – Develop appropriate training for system personnel to improve effectiveness.
- **Exercise and Testing** - Develop and execute regular communications exercises and testing to maintain effectiveness.
- **Outreach** – Collaborate with experts to ensure effective encryption implementation.

[6] Project 25 was previously referred to as APCO Project 25, now simply P25.
[7] FIPS 197, *Advanced Encryption Standard*, Nov 2001

Although these best practices are considered important in developing an environment where encrypted interoperability is realizable, significant additional planning and coordination must be accomplished to enable progress on a national scale. Leadership in developing more detailed encryption guidelines and support for further education and outreach is also needed. These best practices are governed by the same guiding principles of the Interoperability Continuum[8] in that they are based on the goal of interoperability by effective leadership, planning, and collaboration among public safety agencies.

2. Introduction and Background

Reliable, secure encryption techniques applied to public safety radio systems can provide the safeguard needed to ensure the protection of sensitive information from unauthorized use. Once that decision is made, the encryption equipment has been installed, and the system administrator is ready to employ encryption on parts or all of the radio system, key management becomes the primary task. What comes next is the realization that radio encryption, when properly used, requires a degree of maintenance in setting up the initial encryption scheme, programming radios, providing the initial encryption key(s) to the system and radios, and developing a key management protocol to ensure that security is maintained.

This document supplements two other documents addressing encryption in public safety land mobile radio systems. In February 2016, SAFECOM, NCSWIC and FPIC jointly published *Guidelines for Encryption in Land Mobile Radio Systems*, which outlined and discussed the encryption methods that can be used to protect sensitive information for public safety radio systems. Previously, in November 2014, the FPIC developed *Considerations for Encryption in Public Safety Radio Systems*, which provided real-world examples of why encryption is needed and discussed issues involved in making that decision, and is pending publication as a joint SAFECOM/NCSWIC/FPIC document[9]. Together, these documents provide public safety agencies with some important information for deploying encryption in land mobile radio systems. Hopefully, these reports will allow agencies to develop strategies for justifying the additional cost and complexity that encryption adds to system planning, architecture, and operation.

As state, local, and tribal public safety agencies began to implement encryption systems throughout the Nation, the users began to realize that additional guidance and education would be beneficial to ensure that encryption was applied in a reliable manner and that common key management methodologies are available to provide consistent practices among Federal, state, local, and tribal public safety agencies. Although the emerging Project 25 Digital Standards provide enhanced capabilities and interoperability, the basic methods and protocols for encryption have been developed and tested by Federal agencies over the past several decades and have proved reliable and secure.

[8] http://www.dhs.gov/publication/commonly-accessed-documents-safecom
[9] www.dhs.gov/technology

Based on the knowledge gained through years of use and applied throughout the Federal Government on a daily basis, the FPIC[10] Security Working Group (SWG) has been developing strategies for key management that can be applied at all levels of government to assure compliance with the standards[11] that govern how encryption in public safety grade Project 25 (P25) land mobile radio systems works. Additionally, as encrypted interoperability becomes more common among first responders, common procedures will be needed to ensure that systems from different jurisdictions and different manufacturers remain protected and interoperable.

3. Purpose

The purpose of this document is to highlight those elements and best practices of key management that are needed to allow encrypted operability as well as interoperability. The importance and relationship of the elements of key management will be addressed. Fundamentally, the intent of this document is to simplify the complex process of encryption and key management so that *only the essential elements or parameters that are needed for operability and interoperability* are described. The primary goal is to identify Best Practices[12] for the basic aspects of key management, so that encrypted interoperability is possible and manageable among public safety agencies at all levels of government.

The details of how encryption works in a P25 system is contained in the ANSI/TIA 102 Series of Standards[13], and key management guidance is provided in by the National Institute of Standards and Technology (NIST) SP 800-57 series of publications.[14] The standards describe how encryption enables these systems to maintain a robust security profile that protects sensitive information from compromise. This document will address how and why certain encryption parameters are crucial to maintaining a well-functioning encryption system that will assure security and enable interoperability in the encrypted mode.

4. Key Management Overview

In general, key management is the process for the creation (generation), distribution, use, archiving, and destruction of cryptographic keys in a P25 land mobile radio system. It is a vital

[10] The FPIC serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community. The FPIC serves as an interface between the federal, state, tribal, and local agencies. It includes more than 200 federal, state, local, and tribal public safety representatives from over 45 Federal agencies, as well as representatives from State, tribal and local entities.

[11] TIA standards and NIST standards listed in Appendix C

[12] A *Best Practice* is commonly defined as a methodology developed through investigation and experience that has proven reliable and effective.

[13] The published American National Standards Institute/Telecommunications Industry Association ANSI/TIA-102 Standards are available at https://Global.ihs.com.

[14] NIST SP-800-57, *Recommendation for Key Management, Parts 1-3*

part of maintaining a secure operating environment for any public safety radio system. This document will not include a detailed discussion or description of this relationship or details of all the components of key management. Instead, a description of how certain parameters of key management affect interoperability and the importance of maintaining good key management procedures will be included. Without proper and consistently applied key management techniques and protocols, system administrators at different agencies and various levels of government may find it difficult to assure security throughout their system. If common protocols and best practices are applied across all levels of government, encrypted interoperability becomes less onerous.

The P25 Security Services Overview document [15] addresses the need for agencies to develop a key management procedure or doctrine within each organization. The P25 standards do not provide a key management standard. The only elements of key management specifically addressed by the standard are key distribution, entry and use within system elements. NIST provides specific guidelines for establishing a key management program for the proper management of cryptographic keys, including *best practices, general organization and management requirements, and implementation specific key management guidance.* Additionally, the resources listed in Appendix B can provide further guidance in developing key management processes and implementing encryption systems, as they represent a significant source of knowledge and experience in the subject.

Each of the aspects of key management plays an important role in maintaining an effective key management process within an agency. Although simplified in this document, cryptography in P25 land mobile radio systems and key management are complex processes that must be well understood and coordinated to be effective.

Key Generation

The two basic types of keys referred to in this document are the Traffic Encryption Key (TEK)[16] and the Key Encryption Key (KEK). The TEK is the primary key that encrypts voice and data transmissions. The KEK encrypts one or more TEKs (or other KEKs) and is used to identify/authenticate a group of TEKs. Another type of key is the Unique Key Encryption Key (UKEK), a unique KEK that is common to only an individual subscriber unit (SU) or Key Fill Device (KFD) and the Key Management Facility (KMF) and is used to create a secure link during initialization with an individual unit within the KMF's management. These keys can be generated by various key generators, both manually and automatically. The generation of keys is normally accomplished within the agency that manages the encrypted radio system with one of various key generation methods. Once generated, keys can be loaded or distributed through various methods discussed below. The importance to encrypted interoperability is that keys need to be coordinated and shared with other agencies if interoperability is to be realized.

[15] TIA-102.AAAB-A, *Project 25 Digital Land Mobile Radio – Security Services Overview*, Jan 2005

[16] The TEK is a unique hexadecimal key used to encrypt and decrypt voice and data traffic. The length of the TEK depends on the algorithm used.

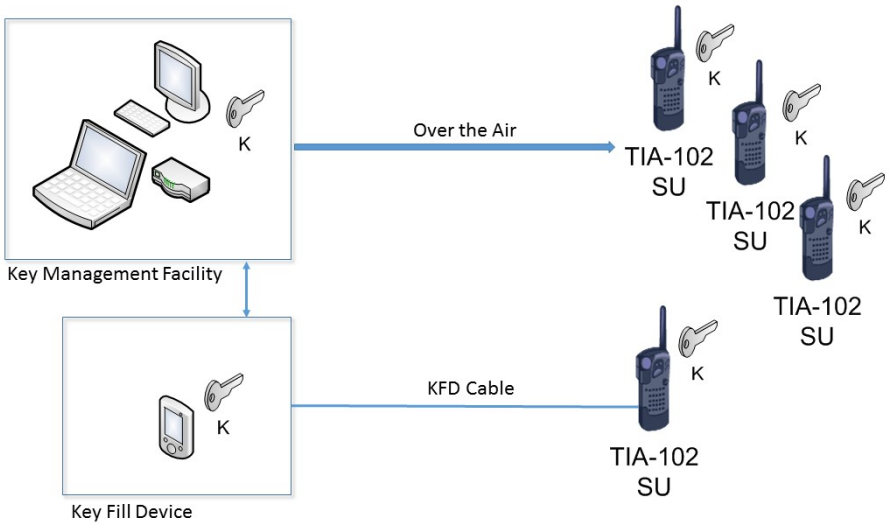
Obviously, without the proper key (and other important parameters identified in Section 5), transmissions cannot be decrypted.

Key Distribution and Use

This is where encrypted interoperability is proven. The only way for jurisdictions to interoperate in the encrypted mode is to share common keys and coordinate the distribution of those keys. The preparation for ensuring encrypted interoperability within an agency, among agencies of neighboring jurisdictions, and on a national level requires a significant amount of planning and cooperation.

The distribution of keys for P25 radios can be accomplished using a KFD for loading keys into subscriber units manually or a KMF for loading keys into subscriber units using OTAR (Over-the-Air-Rekeying). These devices also provide for the management of the key system. Figure 1 below shows that relationship. KFDs can also be programmed or managed by KMFs so that field personnel can load keys in remote areas or in special circumstances. A KMF provides for centralized key management and can include a web-based interface for IP connectivity. A KMF allows for remote inhibit/permit of radios, where a KFD must "touch" each radio for loading keys. The parameter *K* in Figure 1 (and wherever it appears) represents the key variable, hereafter referred to as the TEK, which is used to encrypt the transmission.

Figure 1: KMF, KFD, and Subscriber Unit Interfaces



Key Archiving and Destruction

If keys or keying material needs to be recoverable, for whatever reason, then it needs to be archived and maintained by a trusted party. When it is no longer needed, all copies of the keying material should be destroyed with a method that removes all traces of the keying

material to ensure it cannot be recovered by either physical or electronic means[17]. In general, these elements must be addressed when developing common key management policy and procedures for interoperability among multiple agencies.

5. Importance of Coordinated Key Management

As stated, key management is the process for the administration of cryptographic keys in a LMR system. It consists of a complex set of relationships between the P25 Common Air Interface (CAI), the Encryption Protocol, and the Key Management Protocols described in the P25 TIA-102 Security Services series of standards and elaborated upon in the NIST SP-800-57 publications. It is important to note that a key management policy in a department or agency should address the key management process that is appropriate for each user organization.

Since the practice of encryption and key management varies significantly between public safety agencies, it is essential that these policies/procedures be managed in a consistent way among agencies implementing encryption. In addition, close coordination of these policies and practices among users, especially among joint task forces and neighboring jurisdictions, is essential so that interoperability can be achieved in the encrypted mode at incidents or joint operations. Without a coordinated approach, where agencies have established common encryption groups with shared keys, encrypted interoperability among agencies would experience significant challenges.

Elements of Encrypted Interoperability

There are many complex elements of key management that must be addressed to ensure an effective and secure encrypted radio system. Encrypted interoperability, however, depends on how well jurisdictions that need to interoperate coordinate their protocols and methods for key management. To ensure dependable results, agencies should ensure those policies are consistent with National Guidelines/Best Practices being developed within the FPIC SWG.

Fundamentally, LMR encryption works between two or more radio units or consoles. Voice or data enters one radio, is encrypted through a process that involves a number of parameters, including the appropriate encryption algorithm and TEK. All elements in this process must be synchronized and aligned (common) for the encryption/decryption process to work properly. If the receiving radio contains the proper parameters or identifiers, then the received traffic is decrypted. The alignment of these parameters should be a given for an agency that operates encrypted radios only within its own radio system. The agencies control each of the parameters, which are assigned when programming the subscriber units within a system. It becomes complicated when an agency must coordinate these parameters with other agencies or among a number of agencies, such as a task force.

These critical parameters or identifiers include:

- **The Key ID (KID**) - Provides a unique address to identify a Traffic Encryption Key. The KID is a 16-bit identifier that has a reserve value of hexadecimal $0000 for unencrypted traffic and can be used for single key radios. The P25 Block Encryption Protocol, TIA-102.AAAD-B, specifies hexadecimal[18] $0000 as a reserve value and is used as a default KID for equipment that is not capable of multi-key operation. It is strongly recommended that this reserve value not be used in single key radios, as this will cause the radio to ignore any messages originated from multi-key devices that use non-default key values.

- **Traffic Encryption Key (TEK)** - The Key Variable, a unique hexadecimal key used to encrypt and decrypt voice and data traffic.

- **The Storage Location Number (SLN),** a common term to refer to an encryption key slot in a subscriber unit (also referred to as the CKR[19]). In cases when the key is strapped to a specific talk group, the SLN can be used to designate the encrypted talk group.

- **The Algorithm ID (ALGID)** - an indicator of the type of encryption used. The ALGID is a static hexadecimal value established based on what type of encryption is present. Unencrypted has a reserved value of $80, DES is $81, AES128 is $85, and AES256 is $84.

One or more Keys are categorized by a KID and the appropriate ALGID that identifies the encryption algorithm used, and are stored in the SLN in the radio. The SLN is used to designate a collection of keys (multiple encryption keys within a radio) that may be used for an encrypted operation or target, and can be used to designate a cryptographic talk group. The combination of the Key ID and the Algorithm ID uniquely identifies a key within the KMF/KFD or subscriber unit. The KID and the TEK must match for the process to work properly and for the receiving radios to decrypt transmissions. Multiple encryption keys can be stored in radio equipment conforming to the standard. In order to identify the keys, they are stored with an associated label, the KID.

[18] The "$" is an indicator that the value is hexadecimal and is not programmed in the software.
[19] CKR or Common Key Reference is a term used in Motorola programming software.

Figure 2: Essential Indicators for Encrypted Interoperability

	Keyset 1	Keyset 2
SLN xx	TEK, KID, ALGID	TEK, KID, ALGID
SLN yy	TEK, KID, ALGID	TEK, KID, ALGID
SLN zz	TEK, KID, ALGID	TEK, KID, ALGID
SLN …	TEK, KID, ALGID	TEK, KID, ALGID

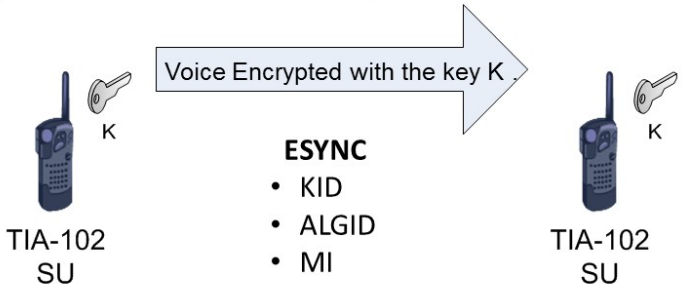


Figure 2 above illustrates, in basic terms, the relationship of the parameters or indicators needed for this process to work effectively. Encryption synchronization (ESYNC) represents the elements required for the transmitter (TX) and receiver (RX) to synchronize transmission, including the Message Indicator (MI) that provides the basic synchronization information, but does not affect the actual encryption process. The SLN is a location programmed in the radio that contains the position of the keyset(s). The KID, the ALGID and the TEK allow the RX to decrypt the transmission. The table within the figure shows what is stored in the subscriber unit for encryption purposes. Each SLN (0 through 4095) contains the key indicators that are needed for encryption to work: the key, the KID, and the ALGID. This illustration shows a multi-key configuration where the current keyset and the future keyset are stored in a particular SLN.

In simplified terms, encrypted interoperability hinges on the coordination of all of these parameters among those agencies needing to interoperate. Encrypted interoperability depends not only on the coordination of these parameters, but on how well jurisdictions who need to interoperate coordinate their protocols and methods for key management. These agencies should ensure that plans and policies are developed to include their own encryption requirements as well as those necessary to operate with other jurisdictions.

The Current Environment

In general, key management is left to the agency that manages the land mobile radio system. It is normally accomplished at a local agency level but is sometimes coordinated on a broader level, such as county, region, or state. However, many public safety agencies who have implemented encryption have limited experience in key management and could benefit greatly from learning about how their current key management policies may adversely affect the

vulnerability of the information they transmit. As an example, they may use the same SLN for all radios, when a more organized use of the SLN is to treat it as a type of encrypted talk group to segment user groups for certain purposes, such as Task Force, Incident Response, SWAT[20], or investigations. As discussed below, some SLNs can be reserved on a National basis for use in creating regional and National response groups for encrypted communications.

In addition, some agencies use static keys and crypto periods for sensitive operations, meaning the TEK is *never* changed. If the key is compromised in whatever manner, any information on the encrypted channel is potentially compromised. Currently, there is a mix of agencies who are well informed on key management and those who are new to the game and need help in understanding its complexities.

Federal agencies differ from state and local agencies in that they have national missions and must deal with managing encryption and key management in a more centralized way and on a broader scale. Much of federal land mobile radio assets are encrypted, and many federal departments and agencies provide for their own key management. A major force in the management of federal land mobile radio systems and provider of key management services to many federal as well as state and local public safety agencies is the National Law Enforcement Communications Center (NLECC) in Orlando, Florida. The NLECC is a Department of Homeland Security/Customs and Border Protection facility whose primary mission is to manage all aspects of DHS/CBP land mobile communications, but has gained expertise in providing key management services to many other agencies at all levels of government. The use of the NLECC to generate and assign Keysets (KID, Key, ALGID) for agencies at all levels of government assures that these parameters are unique and will not conflict with other systems that also use NLECC services. Using a national coordination entity helps to ensure a more uniform approach to key management.

For state and local agencies, the Statewide Interoperability Coordinator (SWIC)[21] can provide the basic point of contact within each state and territory for information on encryption and how to best coordinate encrypted interoperability with partner agencies. They have the knowledge regarding the local environment and know the local encryption experts. They also are members of the National Council of Statewide Interoperability Coordinators (NCSWIC)[22] and can act as a coordinator for coordinating key management with other state and local agencies in the region and assistance from the NLECC as well as with other national organizations and federal agencies.

In general, public safety agencies have varying requirements for encryption and deploy a number of different techniques for managing their encryption. They range from *no encryption*

[20] SWAT (Special Weapons and Tactics) – specialized law enforcement units that use specialized equipment and tactics.

[21] The SWIC is the primary coordinator in each State and territory for the operation of the state's interoperability efforts.

[22] NCSWIC (composed of SWICs) assists state and territory interoperability coordinators with promoting the critical importance of interoperable communications.

to fully-compliant P25 *AES encryption.* Many state and local agencies limit the use of encryption to SWAT, Investigations, or other operations that require protection of sensitive transmissions. Others may use non-standard privacy techniques such as RC4[23], which will not provide the degree of protection that P25 AES provides, is not recommended for transmission of sensitive or mission critical information, and is not approved for federal government use.

For those agencies who do employ P25 standard encryption (DES [24]or AES), key management is usually accomplished in one of two primary ways:

- Use of a Key Fill Device (KFD) which is programmed with the KID and the TEK and is manually loaded into each radio. The key management is accomplished locally, and key changes must be accomplished manually.
- Use of a Key Management Facility (KMF) that provides Over-the-Air-Rekeying capability. The KMF also can be used to manage the configuration of Key Fill Devices.

Those systems that do not have an OTAR capability must use a Key Fill Device or other method for key management. This mix of methods for loading keys into radios can cause conflicts in that all keys are not generated by the same source and may not be coordinated or shared with other jurisdictions.

In addition, the use of the SLN is sometimes random and can cause conflicts when SLNs are duplicated in the same or neighboring jurisdiction. The coordination of SLN assignments is one of the key factors to achieve encrypted interoperability and avoid conflicts. Ideally, the coordination of SLN assignments on a National or regional basis can be effective in avoiding conflicts when attempting to interoperate with other jurisdictions.

How can we achieve Encrypted Interoperability?

As difficult as regular interoperability has been to achieve, it seems achieving encrypted interoperability is beyond reason to some. In fact, encrypted interoperability presents the same roadblocks as unencrypted interoperability: dissimilar frequency bands, technology differences, policy and procedural/coordination issues, and many other factors. In addition, encryption brings further complexities to the table. The coordination of parameters, such as SLN and encryption keys, the methods and policies for general key management, the crypto period, and common naming conventions, can all contribute to the lack of interoperability.

Encrypted interoperability requires a number of factors to be coordinated among agencies that require interoperability. Primarily, the desire to interoperate and to coordinate with one another on a National or Regional level is a key driver. The Interoperability Continuum relies on

[23] RC4 is a stream cipher. It is initialized with a variable length key, typically between 40 and 256 bits, using the *keyscheduling* algorithm (KSA). The key stream of bits is generated using a pseudo-random generation algorithm (PRGA).

[24] Although DES is no longer approved for federal agency use, it remains a part of some installations, awaiting replacement.

Governance and Standard Operating Procedures to form the basis of interoperability. Encrypted interoperability also relies on these basic principles and suggests that the adoption of common key management policies and procedures can form the basis for improved encrypted interoperability.

Essentially, this type of interoperability requires the desire to interoperate; the knowledge and understanding of key management; coordination, planning, implementation, and cooperation between agencies; and a standards-based key management system. In addition to the training received by the vendor, there is a network of telecommunications managers and technicians who have years of experience in the details of key management and can be relied upon to help implement an effective encrypted P25 land mobile radio system. Those resources are listed in Appendix B. They include the National Law Enforcement Communications Center (NLECC), the NCSWIC, and the FPIC Security Working Group.

Encrypted interoperability depends not only on cooperation, but also on coordination of the parameters discussed above; the SLN, the KID, the ALGID, and the TEK. Since there are so many combinations of these parameters that must align before encrypted transmissions can be decrypted, prior coordination among all agencies that need to communicate is essential. Ideally, a common set of SLNs designated for specific purposes (general interoperability, tactical, law enforcement, Fire, etc.) must be defined and recognized on a National basis, so that they can be pre-programmed into radio systems prior to events in order to avoid unnecessary conflicts. As a start to realizing encrypted interoperability on a broader scale, the FPIC has developed Appendix A, *National Reserved SLN Table* in much the same way the FCC and NTIA have identified National I/O channels[25]. These SLNs (1-20) are designated based on encryption type, purpose, and recommended crypto period, and should be avoided in the assignment of local SLNs during programming.

6. Recommended Best Practices for Encrypted Interoperability

An effective way to enhance interoperability is to develop a common set of *best practices* that will encourage public safety agencies to work toward a common goal of encrypted operations and interoperability. If public safety agencies subscribe to these *best practices*, the goal can be realized and will not interfere with an individual agency's ability to configure their encryption system to meet their own unique needs while also supporting common encrypted interoperable channels in their area of operations.

The FPIC Security Working Group has collaborated with LMR security experts at the federal, state, and local government level to examine the methods and procedures that lead to effective

[25] FCC Public Safety and Homeland Security Bureau at http://transition.fcc.gov/pshs/techtopics/techtopics12.html and NTIA Rules at 4.3.16

encrypted interoperability. Primary Best Practices that lead to effective use of encryption include:

Key Management Organization

Ensure the proper organization, implementation planning, and testing of the key management process prior to final implementation. This includes organizational key structure for various disciplinary needs (LE, Fire, EMS, SWAT, etc.) and assignment of the SLN to accommodate those needs. As a start, establish an effective, interoperable key management procedure within your agency. Effective key management includes day-to-day operation as well as planning for contingencies. Planning should include shared keys for events, emergency response, and contingencies. Think of who you will need to interoperate with before the event. The P25 TIA-102.AAAB-A Security Services Overview Standard governs how various aspects of security requirements and key management are specified for P25 LMR systems.

Key Generation and Distribution

Adopt the standard generation and distribution of SLN, KID, Keys, and other parameters that is defined in the P25 TIA series of standards listed in Appendix D. The P25 TIA-102.BAKA KMF-to-KMF Interface Standard presents a generalized concept of operations for managing interoperability keys. A standard for the KMF-to-KFD Interface is under development consistent with current standards addressing the KMF-to-KMF Interface and the KFD Interface Protocol. In that concept, the interoperability of key sharing, both inside and outside an agency, is determined by local agency policy, and ideally should be coordinated among neighboring jurisdictions. The NLECC has helped many agencies at all levels of government in providing keys for both P25 AES and P25 DES systems, and the SWIC is an ideal coordinator for developing key sharing plans.

National SLN Assignment Plan

Promote the use of the Storage Location Number in a common configuration to enhance National encrypted interoperability. The FPIC has developed a plan to reserve SLNs 1-20 to be used for National Interoperability. The Plan, shown in Appendix A, lists reserved values of the SLN and designates them for National, regional, local, task force, and incident response for various public safety disciplines. By adopting this plan, public safety agencies at all levels can begin to coordinate encrypted interoperability plans while minimizing SLN and Key conflicts with neighboring jurisdictions or within Task Force situations.

Standards-Based Encryption

Encourage the use of the P25 security solution using the Advanced Encryption Standard (AES-256). The P25 standard also defines processes and procedures for key management. If interoperability is required with federal agencies, an AES capable radio system is strongly recommended. Although DES is still in use, support for DES will eventually be concluded. The use of multi-key radios is highly recommended to enable the deployment of OTAR for current or future use. The use of non-standard encryption is inconsistent with NIST recommendations and cannot provide protection from compromise. A claim that a particular non-standard

encryption method is capable of providing adequate security is arguable. Algorithms such as RC4 and other ciphers are *not* P25 standards and should not be used.[26]

Crypto Period Considerations

Encourage the use of a key with a defined crypto period to mitigate the risk of compromise (see NIST SP 800-57). Many agencies use a monthly crypto period and can change keys immediately if a key has been compromised. Static crypto periods should be avoided as much as possible. Although not discussed in this document, the understanding of how the crypto period affects the effectiveness of the key management process is as equally important as other elements of key management.

Communications Planning

Ensure that communications plans incorporate encryption requirements. Make encryption part of the Incident Radio Communications Plan (ICS 205) as well as multi-jurisdictional, and multi-discipline plans.

Education and Training

Promote the development and dissemination of accurate information regarding effective key management so that all public safety agencies can develop policies that allow for interoperability at regional, state, and national levels. Train LMR managers, technicians, Communications Unit Leader (COML), and Communications Unit (COMU) personnel in encryption interoperability methods and key management.

Exercise and Testing

Develop and execute regular exercises and testing to maintain effectiveness in encrypted operations. Testing and analysis of encryption and key management procedures and equipment is vital to maintaining the technology and ensuring availability when needed. Exercises within an agency and among jurisdictions that need to interoperate help to resolve common problems and guarantee encrypted communications interoperability during joint operations or incident response.

Outreach

Collaborate with the experts. Most importantly, talk to someone who has done this before. Learn from others' mistakes. Benefit from the knowledge of others with years of experience. If you have any questions regarding how to best implement encryption in your P25 LMR system, do not hesitate to ***Ask for Help!***

[26] SAFECOM/NCSWIC/FPIC, *Guidelines for Encryption in Land Mobile Radio Systems*, February 8, 2016. www.dhs.gov/technology

Appendix A: National Reserved SLN Table (6/19/15)

SLN	Algorithm	Use	SLN Name	Crypto Period (Annual key changes are completed on the first working Monday of October)
1	DES	Public Safety Interoperable	ALL IO D	Annual
2	DES	Federal Interoperable	FED IO D	Annual
3	AES	Public Safety Interoperable	ALL IO A	Annual
4	AES	Federal Interoperable	FED IO A	Annual
5	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static
7	AES	US – Canadian Fed Law Enforcement Interoperability	FED CAN	Static
8	AES	US – Canadian PS Interoperability	USCAN PS	Static
9	DES	National Tactical Event	NTAC D	Single Event Use – Not to exceed 30 Days
10	AES	National Tactical Event	NTAC A	Single Event Use – Not to exceed 30 Days
11	DES	Multiple Public Safety Disciplines	PS IO D	Static
12	AES	Multiple Public Safety Disciplines	PS IO A	Static
13	DES	National Fire/EMS/Rescue	NFER D	Static
14	AES	National Fire/EMS/Rescue	NFER A	Static
15	DES	National Task Force Operations	FED TF D	One time use as needed for Special OPS
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS
17	DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for Special OPS
18	AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for Special OPS
19	AES	Federal – International Law Enforcement Interoperability	FED INTL	When needed by operational requirement
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement

Appendix B: Points of Contact

For additional information regarding the implementation and management of P25 land mobile radio encryption systems, the following points of contact are provided:

1. The National Law Enforcement Communications Center (NLECC):
   Email: nlecc-wsoc@cbp.dhs.gov

2. Statewide Interoperability Coordinator (SWIC) for each of the 56 states and territories:
   see http://www.dhs.gov/safecom/contact-information

3. The Federal Partnership for Interoperable Communications Security Working Group:
   Email: FPIC@hq.dhs.gov

Appendix C: Report Contributors

The following federal, State, and local public safety Departments and Agencies contributed to the creation and completion of this document. These contributions represent the combined opinions of recognized subject matter experts in the field of encryption and key management.

- Connecticut Department of Emergency Services and Public Protection, Division of Statewide Emergency Telecommunications
- Fairfax County (Virginia) Department of Information Technology, Radio Services Division
- Federal Bureau of Investigation, Operational Technology Division, Technical Programs Section, Radio Systems Development Unit
- Montana Department of Justice, Highway Patrol Division
- Orange County (California) Sheriff's Department
- Phoenix (Arizona) Police Department
- State of South Carolina, Office of the CIO
- Texas Department of Public Safety
- Treasury Inspector General for Tax Administration, Technical and Firearms Support Division
- U.S. Coast Guard Headquarters
- U.S. Department of Homeland Security, Customs and Border Protection, National Law Enforcement Communications Center
- U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations
- U.S. Marine Corps, MCAS Yuma, Communications Data Electronics Department
- Wyoming Public Safety Communications Commission

Appendix D: References [27]

- FIPS 197, Federal Information Processing Standards Publication 197, *Specification for the Advanced Encryption Standard*, November 2001

- FIPS 140-2, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, December 2002

- NIST SP-800-57, National Institute of Standards and Technology Special Publication SP-800-57, *Recommendation for Key Management, Parts 1-3*

- NIST SP 800-152, National Institute of Standards and Technology Special Publication SP-800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*

- TIA-102.AAAB-A, *Project 25 Security Services Overview*, January 2005

- TIA-102.AAAB-A-1, *Project 25 Security Services Overview Addendum 1 – Key Management Architecture,* September 2014

- TIA-102.AACA-A, *Project 25 Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures*, September 2014

- TIA-102.AACE-A, *Project 25 Digital Land Mobile Radio Link Layer Authentication*, April 2011

- TIA-102.BAKA, *Project 25 KMF to KMF Interface*, April 2012

- TIA-102.AAAD-B, *Project 25 Block Encryption Protocol*, December 2015

- TIA/EIA-102.AACA-A, *Project 25 Digital Radio Over-The-Air Rekeying (OTAR) Protocol*, September 2014

- TIA-102.AACD-A, *Project 25 Digital Land Mobile Radio-Key Fill Device (KFD) Interface Protocol*, September 2014

[27] To access the latest versions of the information listed, check the reference sources at http://www.NIST.GOV and http://www.GLOBAL.IHS.COM