DHS Office of Emergency Communications

Guidelines for Encryption in Land Mobile Radio Systems

September 2013

PREFACE

The incentive to develop this document originated as a compelling request from the State and local public safety community for guidelines that would provide clear and factual information regarding the use of encryption, what it can provide to protect mission critical communications from compromise, and how to best implement it to maintain interoperability among agencies at all levels of government. The importance of this request was elevated when non-standard and "weak" encryption solutions were introduced to a number of public safety agencies as they implemented Project 25 digital communications technology to support their mission critical voice and data communications needs. Although most felt these non-standard encryption protocols could not ensure the level of security necessary, the cost of these solutions was attractive and many were not aware of the actual lack of protection and the potential impact on communications interoperability.

Although the federal agencies have been required to protect Sensitive but Unclassified (SBU) Information for several years, most public safety agencies felt the cost of implementing encryption could not be justified. However, as the importance of protecting sensitive information became evident, coupled with the introduction and implementation of digital technology, such as Project 25, the interest in encryption and protection of information steadily increased.

There were a significant number of public safety officials and system administrators that recognized the need for encryption in specific applications. This group also recognized there was significant confusion and competing information regarding voice and data encryption in the Land Mobile Radio (LMR) environment. A significant number of the public safety communications officials and system managers, including representatives from federal agencies, strongly felt a guideline needed to be developed that provided factual information and a guideline that provided consistent information.

The initial request for such a document was introduced to the Federal Partnership for Interoperable Communications (FPIC). The FPIC Security Working Group agreed to develop a document to satisfy the demand to encourage consistency in deploying a standardized encryption methodology across Federal, State, and local public safety communications platforms. In further developing this document, a wide range of public safety security and encryption experts at all levels of government provided valuable input. Their specific contributions ensured consistent content and efficacy. Although many individuals and organizations took part in the development of this document, the organizations listed in the Appendix were especially helpful in assuring the content is both timely and accurate.

Although this document was developed as a result of a joint, cooperative effort of public safety agency representatives and a specific author is not recognized, the group agreed to identify the Office of Emergency Communications as the common coordinating entity. The contributing representatives anticipate acceptance and release of this document by the appropriate authority within the Department of Homeland Security as an information guide that can be disseminated to all public safety user agencies and organizations as appropriate. This document is not intended to be a policy directive or procedure.

1. EXECUTIVE SUMMARY

As a result of a number of security risk and vulnerability assessments, the public safety community has recognized the increasing effort to protect sensitive information transmitted over their wireless communications systems. Additionally, as the users continue to implement digital land mobile radio (LMR) technology, such as Project 25, they have realized the relative cost of protecting this information has decreased with digital technology. Most public-safety system administrators and managers want to minimize the possibility of sensitive information being monitored with low-cost scanners, but are concerned with the costs associated with the costs of standards compliant encryption. The purpose of this document is to provide information that should be considered when evaluating encryption solutions.

The key to protecting sensitive operational or safety of life radio transmissions is to deploy an encryption system with an algorithm that provides the assurance that information is adequately protected from eavesdropping. A number of encryption algorithms exist that include encryption key lengths from 56 bits to 256 bits. These techniques are being used in land mobile systems throughout the U.S. and the World, but all do not provide the protection needed to ensure operational security.

Standards compliant algorithms, such as the Advanced Encryption Standard (AES), offer the greatest opportunity for achieving maximum interoperability while providing a high level of protection. The AES algorithm is specified in NIST FIPS PUB-197. Unlike proprietary or non-standard algorithms, AES is freely available to any manufacturer who wishes to use it. There are no intellectual property restrictions or royalty payments involved in its use. While key lengths of 128-bit and 192-bit are authorized for use, it is strongly recommended that the 256-bit key is utilized in public safety wireless systems in accordance with the published standard for Project 25 Block Encryption Protocol (TIA-102.AAAD-A).

The National Institute of Standards and Technology (NIST) has concluded that a cryptographically strong algorithm with a key length of 128 bits or longer is the most effective way to protect sensitive information from compromise and has mandated the use of the NIST certified Advanced Encryption Standard (AES) as the only encryption technique for federal land mobile systems. Federal Departments and Agencies require NIST-approved encryption for Sensitive but Unclassified (SBU) Information and do not allow the use of proprietary encryption algorithms. The P25 Standard relies on AES 256-bit to ensure the best level of protection and interoperability.

2. BACKGROUND

As the public safety user community continues to implement digital technology to support the mission- critical voice communications, they have recognized an increasing need to protect sensitive information that is transmitted over the air and within the network. As these users realize that cost delta for encryption is significantly reduced when implemented in a digital wireless communications network, such as Project 25.

While any electronic communications system is vulnerable to exploitation by interception (eavesdropping), a radio communication system is one of the most vulnerable. Interception can

occur anywhere in the radio coverage area, is difficult to detect (since no physical interconnection is required) and can be accomplished with equipment that is readily available, or easily acquired.

The purpose of this document is to discuss methods that may be used to ensure the confidentiality of sensitive public safety land mobile radio communications. These methods mainly involve the use of encryption. However, the use of encryption can adversely affect interoperability with other agencies if due consideration is not given. For example, ensuring that all agencies support the same cryptographic algorithms is the first step in protecting sensitive communications while still allowing for interoperability.

3. ENCRYPTION

Cryptography[1] can be used to provide several security services including: Confidentiality (the protection of message contents from disclosure); Authentication (the verification of the identity of message sender); and to ensure message Integrity (the message contents have not been modified). Encryption is commonly used to mitigate the threat of interception by providing the Confidentiality service.

Encryption, in simple terms, is the conversion of data into a form called cipher text that cannot be understood by unauthorized entities. Decryption is the process of converting encrypted data (cipher text) back into its original form.

Encryption (and subsequent decryption) requires the selection and use of a common cryptographic algorithm. Examples of encryption algorithms include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest, Shamir, and Adelman (RSA) and various other algorithms. Encryption requires not only the use of an algorithm, but also an encryption key chosen by the message originator and a decryption key known to the message receiver. Algorithms that use the same key for encryption and decryption are known as symmetric key algorithms, and it is this type of algorithm that is used for the encryption of voice and data in land mobile-radio applications. The aforementioned DES and AES are symmetric key algorithms. When a symmetric key algorithm is used, the key used for both encryption and decryption must be protected from unauthorized disclosure.

A “cryptographically strong” encryption algorithm is one that is highly resistant to unauthorized decryption and cryptanalysis. For a cryptographically strong encryption algorithm, the “cryptographic strength” of an algorithm directly corresponds to its key length, or number of possible keys.[2] Roughly, this means that the plaintext that corresponds to encrypted data (cipher text) can only be determined by an adversary by trying each possible key until he finds the key used to encrypt the data (a process known as exhaustive key search), and the amount of time it takes to do this is significantly longer than the useful lifetime of the information transmitted by the plaintext.

[1] Although Cryptography is the proper term in most government environments, the term encryption is also commonly used by many users and manufacturers.

[2] An analogy to this is the size of passwords, where a 12-character password is inherently stronger than an 8-character password.

For cryptographic algorithms, key length is typically specified in terms of the number of bits used. The encryption algorithm formerly used by the U.S. Government, DES, has a key length of 56-bits, which allows 2^{56} or approximately 10^{17} (100,000,000,000,000,000) unique keys. AES has a minimum key length of 128-bits and can use additional key lengths of 192-bits and 256-bits. This gives 3.4×10^{38} possible 128-bit keys; 6.2×10^{57} possible 192-bit keys; and 1.1×10^{77} possible 256-bit keys.

While the DES key length of 56-bits seems to allow an enormous number of keys, it has been shown to be subject to exhaustive key search using modern computer systems. More sophisticated cryptanalysis can further reduce the work factor of recovering a DES key to significantly less than 2^{56} operations. Most knowledgeable cryptographic experts currently recommend a ***minimum cryptographic strength*** of 112 to 128-bits for use in new systems. In fact, DES has already been withdrawn (de-certified) for use in U.S. Government applications. It should be noted that as key size is reduced below the recommended values, the vulnerability to exhaustive key search increases, especially as advances in computing speed and power occur. This is true regardless of the cryptographic algorithm used.

An example of an encryption algorithm commonly accepted as "strong" is the NIST Advanced Encryption Standard.[3] It is a publically specified algorithm that was selected in 2001 for use by the U.S. Government, after a multi-year international competition. It has been subjected to the scrutiny of leading cryptographers and security organizations from around the world, and few weaknesses have been identified. Weaknesses, when referring to cryptographic algorithms, allow mathematical shortcuts that can be used to circumvent an exhaustive key search. NIST adopted AES as an approved standard for the protection of U.S. Government sensitive information. In addition, the National Security Agency (NSA) allows its use for the protection for certain levels of classified information.[4]

One might contrast this open public process with a proprietary developed algorithm. In most cases, these proprietary algorithms have not been published and have not been subject to public scrutiny prior to deployment. One must take the word of the developer that a particular algorithm is "strong" and is capable of providing real security. An example of a security implementation that was not subjected to thorough public review is Wired Equivalent Privacy (WEP) that was used for 802.11 Wi-Fi networks. WEP is the implementation of a communication protocol that uses an encryption algorithm RC4[5] as part of the protocol. It was developed using an open-standard process in the IEEE. However, once subjected to a thorough public review, a number of significant weaknesses were identified in the algorithm and its implementation that allowed it to be broken with little effort.

Lastly, while data encryption algorithms may be safe and secure to prevent unauthorized disclosure of potentially sensitive information, the handling of the cryptographic material, or mishandling thereof, can lead to a possible disclosure or unauthorized access. The official

[3] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[4] http://www.cnss.gov/Assets/pdf/CNSSP_No%2015_minorUpdate1_Oct12012.pdf
[5] RC4 is a stream cipher. It is initialized with a variable length key, typically between 40 and 256 bits, using the *key-scheduling* algorithm (KSA). The key stream of bits is generated using a pseudo-random generation algorithm (PRGA).

procedures for handling the cryptographic material need to be carefully crafted to minimize any unauthorized access from occurring. The overall strength of an encryption method is negated by the misuse or mishandling of these keys, therefore the proper handling of the cryptographic material is of the utmost importance and can be as important as the encryption method itself.

4. ALGORITHM CHOICE

Cryptographic algorithms are often contained in products with "type" designations that differentiate the conditions under which they are certified for use by public safety agencies at all levels of government; who approved the algorithm, or whether the algorithm is vendor proprietary. In general, there are four "type" designations for land-mobile radios. They include: Type I, Type II, Type III, and Type IV. Type III is the predominant type designation for public safety land-mobile radio and is approved by NIST for the protection of sensitive but unclassified (SBU) information.

There are a number of choices for encryption algorithms for use in public safety land mobile radios. These would include the AES, Triple-DES, DES and proprietary algorithms. AES is approved by NIST for protecting sensitive, but unclassified (SBU), information. Some advantages and disadvantages of each are given below;

AES – The AES was selected for use by the U.S. Government in 2001 after an open selection process, as noted above. It was subjected to several years of study prior to its being selected as a standard. It provides key lengths of 128, 192 or 256-bits which are capable of providing protection from exhaustive key search for the foreseeable (20 – 30 year) future. Although agencies may choose to use any of the three key lengths, AES (with 256-bit key length) has been specified in the Project 25 Statement of Requirements and published standards as the encryption algorithm for use in new Project 25 systems. It is the clear choice for new systems requiring robust security. Consequently, the U.S. government recommends that agencies implement the Project 25 compliant 256-bit key length. Agencies with existing or potential government interoperability requirements should adopt AES with 256-bit key length as their standard algorithm in order to ensure interoperability, while providing the long term protection that the more robust algorithm offers.

DES – This algorithm was developed in the mid-1970s to protect U.S. Government communications. Due to its small (56-bit) key size it no longer provides real protection, given the advances in computing speed and power that have occurred in the last 30 years. An exhaustive key search using dedicated equipment in 1998 was able to determine the key in 56 hours. Since then this time has been reduced. The DES should not be used in new systems and should only be used when backwards interoperability with systems that do not support newer algorithms is required. As noted above, DES is no longer certified for use with U.S. Government systems.

While it is recommended that all new systems be procured with the AES encryption algorithm, system administrators should exercise caution and identify those systems which are not capable of supporting these new algorithms. Those systems, which are only protected by the DES algorithm, must also be considered when surrounding systems are being upgraded or replaced.

Triple-DES (3 DES) – This algorithm basically encrypts data three times using the DES "engine". Two-key Triple DES has been assessed at a security strength of 80 bits, whereas three-key Triple DES is assessed at a security strength of 112 bits.. The algorithm uses DES encryption and decryption engine to encrypt, decrypt, and then encrypt again. It can use two DES keys with the first and last encryption using the same key (two key triple DES) or three DES keys (three key triple DES). It was mainly used as an interim algorithm while the AES was being developed. While currently capable of providing adequate security, its use is not recommended for new applications. Triple-DES also suffers from some performance issues since it must encrypt data three times. To date, Triple-DES is not offered in any current public-safety land mobile radios.

Proprietary/Unapproved algorithms – These algorithms may or may not provide adequate protection regardless of advertised key length. The risk one takes is that the user has to accept the developer's assurance that the algorithm and the resulting hardware or software implementation is cryptographically strong. Proprietary solutions can also adversely affect interoperability because an agency that uses proprietary encryption can only interoperate in an encrypted mode with agencies that use the same proprietary encryption algorithm. Specifically, NIST recommends proprietary/unapproved algorithms not be used with U.S. Government systems. In fact, Federal Departments and Agencies require the use of NIST approved encryption algorithms for protection of sensitive but unclassified information. Most departments and agencies have mandated the use of AES 256 bit encryption in their LMR Systems. None have authorized the use of proprietary algorithms**.** Generally, radio subscriber units do not provide users the ability to easily switch between different encryption systems. Generally, only qualified maintenance personnel can configure radio subscriber units capable of operating in multiple systems to operate with either a proprietary/unapproved algorithm or AES (or other NIST Approved Algorithm).

Table 1 – Algorithm Reference Matrix

Algorithm	Key Length (bits)	Recommended Use
AES	128, 196, 256	Unclassified but sensitive, all secure communications
Triple DES	112, 168	Not currently offered in LMR radios supporting public-safety communications
DES	56	Legacy secure communications, interoperability mode only
Non-standard	Varies	Not recommended for secure communications

5. CRYPTOGRAPHIC MODULE

The cryptographic algorithm is stored and executed in a cryptographic module. In particular, the module stores and uses the key to allow for encryption and decryption of voice and data communications. A crypto module supporting secure voice and data communications within a LMR system must be significantly enhanced to protect the keying material housed within that crypto module. Since protecting the key is vital to protecting the information, care

must be taken to ensure the module is designed properly. NIST has developed the FIPS140-2 standard to test and report the integrity of the module. Any radio that does not implement the algorithm on a FIPS 140-2 module is risking the integrity of the key for all users of that key. Therefore, it is recommended that all interoperating in secure mode have encryption modules certified to FIPS 140-2.

6. INTEROPERABILITY ISSUES

Standard algorithms, such as the AES, offer the greatest opportunity for achieving maximum interoperability. The AES algorithm is specified in NIST FIPS PUB-197. Unlike proprietary algorithms, AES is freely available to any manufacturer who wishes to use it. There are no intellectual property restrictions or royalty payments involved in its use. This is typically not the case with proprietary technology. While key lengths of 128-bit and 192-bit are authorized for use, it is strongly recommended that the 256-bit key is utilized in public safety wireless systems in accordance with the published standard for Project 25 Block Encryption Protocol.

Understanding that Federal Government users may not have the resources to evaluate encryption-based products, NIST offers a way for manufacturers to validate their AES offerings to assure that the encryption has been implemented correctly.

In addition, AES is the algorithm to which all of the Federal Government public-safety community is transitioning. Therefore, agencies with a need to interoperate with Federal entities in a secure manner will be required to use AES.

It should be pointed out that there is a host of other issues, besides the algorithm choice that need to be addressed in order to achieve secure interoperability. (A discussion of these complex issues is beyond the scope of this basic document.) This fact gives additional reasons to choose a standards-based solution to encryption because many of these issues are addressed for the user in the standards. This is particularly the case with the security standards developed for Project 25 interoperability.

7. SUMMARY

Some users will choose to adopt non-standard/proprietary security technology, but when they make this choice they should be fully aware of the possible security risks and interoperability issues involved in using non-standards-based solutions.

It is highly recommended that the AES-based security solutions specified in Project 25 be adopted by users who require robust security, or need to interoperate with Federal users and other agencies that have adopted the open Project 25 security standards. It is also recommended that agencies ensure that the cryptographic modules incorporated in any equipment be modules that have been validated by NIST under their cryptographic module validation program. The use of NIST-validated modules ensures that the AES and associated cryptographic functions have been implemented correctly. A list of NIST validated modules is available at: http://csrc.nist.gov/groups/STM/cmvp/validation.html.

References:

FIPS 140-2, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, May 2001 as annexed

FIPS 197, *Specification for the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, Nov 2001

TIA-102.AAAD-A, *Project 25 Digital Land Mobile Radio Block Encryption Protocol*, Telecommunications Industry Association, August 2009

APPENDIX – 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 wireless encryption operations and technology.

- U.S. Department of Justice, Wireless Management Office
- Federal Bureau of Investigation, Operational Technology Division, Technical Programs Section, Radio Systems Development Unit
- U.S. Drug Enforcement Administration, Office of Investigative Technology
- National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division
- Wyoming Public Safety Communications Commission
- Connecticut Department of Emergency Services and Public Protection, Division of State Police
- Missouri Department of Public Safety, Missouri Interoperability Center
- 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
- Treasury Inspector General for Tax Administration, Technical and Firearms Division
- Fairfax County (Virginia) Office of Information Technology, Radio Services Division
- Orange County (California) Sheriff's Department, Radio-Microwave Unit
- U.S. Marine Corps, MCAS Yuma, Communications Data Electronics Department
- Loudon County (Virginia) Department of Information Technology, Public Safety Division
- Metropolitan Washington Airports Authority, Wireless and Radio Systems Department
- Montgomery County (Maryland) Police Department

- Montana Department of Administration, Public Safety Services Bureau
- Montana Department of Justice, Highway Patrol Division
- U.S. Coast Guard