PUBLIC SAFETY

PSWN PROGRAM

WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Introduction to Encryption Key Management for Public Safety Radio Systems

FINAL

October 2001

TABLE OF CONTENTS

1. INTRODUCTION 1
2. IMPORTANCE OF ENCRYPTION KEY MANAGEMENT 3
3. ENCRYPTION KEY MANAGEMENT 5
   3.1 Key Generation 5
   3.2 Key Distribution 5
   3.3 Key Storage 6
   3.4 Key Destruction 7
   3.5 Key Maintenance 7
4. SECURITY ISSUES AND CONCERNS ON ENCRYPTION KEY MANAGEMENT 9
   4.1 Manual Rekeying Method 9
   4.2 Interoperability 9
   4.3 Insecure Storage of Encryption Keys 10
   4.4 Lack of Training Materials 10
   4.5 Lost or Stolen Radios with Encryption 11
   4.6 Unspecified Policy and Guidelines 11
   4.7 Comprehensive Key Management Procedures 11
   4.8 Improper Physical Security Controls 11
5. RECOMMENDATIONS 12
   5.1 Establishment of Key Management Policy 12
   5.2 Detailed Encryption Key Management Guidelines 13
   5.3 Establishment of Security Training Program 14
   5.4 OTAR Technology 15
   5.5 Use of Better Secure Algorithms 17
6. CONCLUSIONS 19

APPENDIX A—LIST OF ACRONYMS A-1
APPENDIX B—GLOSSARY B-1
APPENDIX C—REFERENCES C-1

LIST OF FIGURES

Figure 1. Basic Encryption Concept……... 1
Figure 2. Secret Key Algorithms……..….. 3
Figure 3. Key Management Facility……... 6
Figure 4. TIA 102 OTAR Architecture…….. 16
Figure 5. Multikey Operation…….…… 16
Figure 6. Recent Coordinated DES Attack…….18

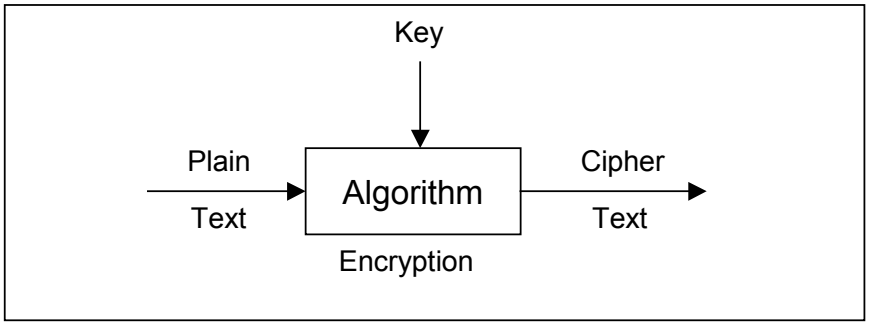
1. INTRODUCTION

Public safety radio communications often contain sensitive and vital information concerning law enforcement activities. Preserving the private nature of this information is essential to the protection of life and property, as well as satisfaction of law enforcement mission requirements. Disclosure or modification of this information could severely impact public safety operations and pose a threat to the safety of public safety officials and citizens. Because of the serious implications for operational effectiveness and personnel safety, the public safety community recognizes the need for encrypted radio transmissions when broadcasting sensitive law enforcement information over the air. Although some clear-channel broadcasting related to public safety activities is necessary, certain public safety communications should be protected from compromise. The most typical and cost effective method to accomplish this is through encryption. Encryption provides voice privacy allowing only the intended radio users to decipher the information transmitted. In a digital land mobile radio (LMR) system, the application of encryption does not affect the audio quality and geographic range, as was the case with the encrypted analog systems.

Because the latest technology has improved the quality of encrypted voice radio communications, use of encryption by public safety agencies has increased, and radio users have been encouraged to use the encryption capability. However, the use of encryption raises other issues—namely, how to effectively manage the encryption keys to ensure that they are safeguarded throughout their life cycle and are protected from unauthorized disclosure and modification. Encryption keys are a sequence of symbols used with a cryptographic algorithm, which enables encryption and decryption. It is imperative that an efficient key management program be established and facilitated throughout public safety agencies. Key management ensures that critical and sensitive radio transmissions are protected with proper encryption methods and that encryption keys are controlled and securely stored during their life cycle.

For purposes of this report, encryption is defined as the process of transforming plain text into unintelligible form by using a cryptographic system. The cryptosystem is hardware and software providing the means to encrypt and decrypt transmissions. Figure 1 presents a basic encryption concept.

Figure 1. Basic Encryption Concept



The fundamental elements of encryption include the algorithm (i.e., a means of changing information), the key (i.e., a secret starting point for the algorithm), and the key control (i.e., key management). The key is typically a binary number used with a cryptographic algorithm to enable the encryption and decryption of data. The key controls the algorithmic transformation applied to voice or data transmission during encryption and must be predictable so that a matching decryption algorithm can reverse the process using an appropriate key. With encryption, analog or digital electronic signals are altered to form an encrypted digital signal or vice versa.

Because encryption and key management are important subjects to the public safety community, the Public Safety Wireless Network (PSWN) Program has prepared this report to serve three purposes[1]:

- Address security issues and concerns regarding encryption key management
- Raise security awareness of decision makers on the importance of a key management program
- Provide recommendations for establishing proper key management.

1 *Note that this report does not focus on the technical issues of key management processes, but on the administrative and operational security issues.*

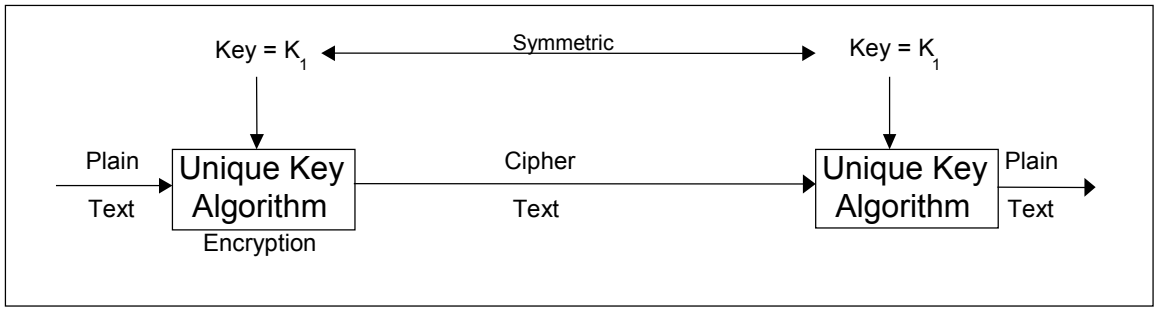
2. IMPORTANCE OF ENCRYPTION KEY MANAGEMENT

Increasingly, public safety agencies recognize the need for enhanced security as the use of encryption increases and as technological evolution allows various radio user groups to communicate and share sensitive information. In particular, the importance of thorough, consistent key management processes among public safety agencies with interoperable functions cannot be overemphasized. Secure distribution, loading, storing, and destroying of keys are essential to make encryption implementations effective.

There are inherent risks if proper key management procedures are not followed because of the complexity of distributing keys to all radio units in a synchronized fashion. The loss, theft, or compromise of encryption keys could seriously affect the integrity, confidentiality, and availability of radio communications. Without proper handling of keys during their life cycle, keys could be disclosed, modified, or substituted by unauthorized personnel who could then intercept sensitive radio communications. This risk can be significantly mitigated through adequate key controls and proper education on encryption key management.

Telecommunications Industry Association / Electronics Industry Alliance (TIA/EIA) 102 (Project 25) specifies that Type 3 encryption, Data Encryption Standard (DES) is the standard algorithm to be used for public safety radio communications. DES is a unique/protected-key, symmetric cryptosystem. This well-known form of private key encryption transforms 64-bit data blocks under a 56-bit unique/protected key. In private key encryption, the same 56-bit key is used for both encryption and decryption. Figure 2 depicts unique/protected key algorithms.

Figure 2. Unique/Protected Key Algorithms



Because the same key is used for encryption and decryption, the key should be changed frequently to prevent misuse.

TIA/EIA 102 will adopt Triple DES in Phase 2, which provides better security than standard DES. Three-key 168-bit Triple DES is considered very strong. Triple DES is a form of encryption that allows sensitive information to be transmitted over unprotected networks. The National Institute of Standards and Technology (NIST) has adopted Advanced Encryption

Standard (AES) to replace DES as the official U.S. Government encryption standard. AES will be secured with 256-bit keys. A large key results in strong, unbreakable encryption.

To protect keys or keying materials during their life cycle, guidelines providing detailed instructions or planned security measures must be available and followed. In particular, the current evolution of technology and interoperability in radio communications make the encryption system more vulnerable to compromise. Since most encryption algorithms are published and well known, the security of data being transmitted is dependent upon the protection of the key. The destruction or loss of the key is equivalent to the loss or destruction of the data itself. If disgruntled employees or unauthorized users know that encryption keys are not changed regularly, more opportunities exist for encrypted communications to be monitored and broken over time. This increases the need for guidance or standards that can be used and easily adopted throughout the public safety community. Such guidance is the basic foundation of proper key management.

3. ENCRYPTION KEY MANAGEMENT

This section provides a basic primer on key management. Key management is the overall process of generating and distributing cryptographic keys to authorized recipients in a protected manner.[2] The key management life cycle consists of the following five major steps, which are described in the subsequent subsections:

- Key generation
- Key distribution
- Key storage
- Key destruction
- Key maintenance.

Key management should be tied to the operational key mapping of the agency. This will determine number of keys to be generated, the classification level of keys (e.g., Type 3), and the cryptoperiod of each key (i.e., frequency of key changes).

3.1 Key Generation

Key generation is one of the most sensitive cryptographic functions. Keys can be generated using true random number generators (RNG) and/or pseudorandom number generators (PRNG). Keys must be generated using an approved key generation method specified by the organization-specific key management program in a protected environment. Only crypto-custodians who have the necessary security authorizations and have received proper training should perform key generation functions. Currently, public safety agencies generate their own keys (automatically or manually) or use National Security Agency (NSA) generated keys.

An effective key management program should document several crucial elements. It should document an approved means to generate encryption keys and state the responsibilities and secure functions for crypto-custodians who perform key generation. Additionally, protected environments where keys can be generated should be provided.

3.2 Key Distribution

Keys should be changed regularly (e.g., monthly or weekly) depending on the nature of the critical operations they protect. Key distribution can be performed using three methods: manual method, automated method, and a combination of automated and manual methods. In general, key distribution to public safety radios is performed by the manual method, although more agencies are implementing over-the-air-rekeying (OTAR). The encryption key is inserted ("filled") into each radio with the key variable loader (KVL) which must be physically connected to each subscriber unit.

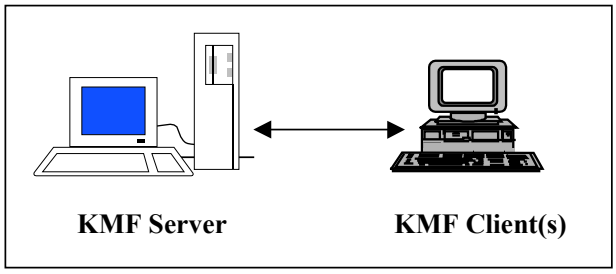
---

2 *ICSA Guide to Cryptography,* p. 745, Randall K. Nichols, 1999

Some in the public safety community are exploring OTAR technology, which enables automatic key distribution. OTAR provides efficient updating of encryption keys for field radios. When using the OTAR, the initial loading of each key into the subscriber unit is done manually. The central facility, called a key management facility (KMF) distributes keys by first encrypting the key and then transmitting it over the air to subscriber units in the system. Subscribers decrypt the key and store it for use among themselves. The KMF can fill a KVL with encryption keys using a direct cable connection or a telephone circuit and modems to a remote KVL.[3]

A KMF is a digital device (e.g., a desktop computer) and consists of a KMF server and a KMF client or clients. A KMF server maintains keying materials in databases; encrypts and decrypts all key management messages; and provides access point for KVL upload and download. A KMF client provides operator interface to OTAR, key management services (local and remote), and KMF administrator access. Figure 3 depicts a typical KMF.

Figure 3. Key Management Facility



To facilitate radio transmissions and updating of keys to radios, a key management program should document the key cryptoperiod and protected ways to distribute keys for either the manual or the automated method.

3.3 Key Storage

Unique/protected and private keys, which have a longer life than session keys, must be stored in a protected area. If keys are delivered via magnetic media, they are loaded into the key management controller (KMC) or KMF from the media. The KMC/KMF centrally manages all of the encryption keys. The KMC or KMF generates keys, stores keys, used or unused, and provides key functions. KMCs are used with analog LMR networks. KMFs are used with digital LMR networks based on TIA/EIA 102 standards. After keys are inserted into radio units, the original keys can be stored on a diskette or other media, or can be disabled.

When magnetic media are used to store keys, the media must be stored in a locked safe, vault, or a protected area whose access is restricted to a limited number of authorized personnel. The area should be authorized by the agency's security officer.

---

[3] *Multikey Over-the-Air Rekeying System, Test Report,* prepared by the VHF-UHF Subworking Group of the Communications Interoperability Working Group, December 28, 1990

When keys are stored in the database of the KMC/KMF, proper authentication mechanisms (e.g., password, biometrics identification, or tokens) must be used to restrict root access to the computer to only authorized personnel.

A key management program should document locations where keys are stored; protected ways to store magnetic media; proper authentication methods to prevent unauthorized access to computer and encryption software; and responsibilities of authorized personnel.

3.4 Key Destruction

When the key is no longer needed (i.e., after the key is loaded into KVLs) and when its life has ended, it must be destroyed. Procedures should be in place to properly destroy the key to ensure that no unauthorized party gains access to the key. In particular, there must be a reliable way of destroying or disabling the key if a mobile vehicle (e.g., police cruiser, ambulance, or fire vehicle) is disabled and must be abandoned. If a criminal were to obtain access to the radio, he or she could use it to send misleading messages to other public safety officers.

Keys can be manually or automatically destroyed. For manual deletion, keys on magnetic media can be erased, and the magnetic media can also be destroyed to ensure no data residue can be recovered. A KMC or KMF can automatically destroy old keys when more than a specified number of versions (e.g., five old versions) are stored in the KMC/KMF. Encryption software used to generate or delete keys can produce audit reports (i.e., event logs) with information on time/date, type of actions, and user identification.

A key management program should document protected ways to destroy or disable keys to protect keys from unauthorized disclosure and should document detailed instructions on how to review event logs.

3.5 Key Maintenance

The key storage devices (e.g., vault, safe, etc.) and KMCs/KMFs should be protected with adequate physical security controls (e.g., badge access, keypad, or keys) so that the keys are not disclosed, modified, or replaced without the approval of the key manager. Only authorized personnel must perform regular maintenance of equipment hardware and software. A detailed maintenance record should be documented whenever regular or emergency maintenance is performed.

A key management program should document physical access controls implemented for the KVLs, electronic devices, and rooms housing key-related equipment. In addition, it should document routine operations and personnel responsible for equipment maintenance.

Before an operational key is manually inserted into radios, a test key is generated to ensure that the key works properly. Once the test is complete, the test key can be deleted or it is used as a maintenance key. A maintenance key can be different from the test key; however, in general the same key is used for testing and maintenance purpose. The test key should not be used as an operational key. If the test key is used as a maintenance key, the key must be

protected from unauthorized disclosure or modification. The test/maintenance key is stored in key punch tapes or electronic media. These storage devices must be protected from unauthorized access.

A key management program should document how to develop test and maintenance keys and functions of the test and maintenance keys. Additionally, responsibilities of personnel who handle and operate test and maintenance keys should be addressed.

4. SECURITY ISSUES AND CONCERNS ON ENCRYPTION KEY MANAGEMENT

Although encryption provides voice privacy and data protection, without effective key management, a number of security risks associated with the integrity and confidentiality of encryption keys are introduced. Because encryption technology is somewhat new to public safety personnel, the majority of public safety agencies have not established any form of key management processes. The following describes security issues and concerns raised as a result of the increased use of encryption among radio users and the operational difficulties of implementing proper key management.

4.1 Manual Rekeying Method

In the multiuser environment of the public safety community, it is difficult to distribute encryption keys efficiently and effectively. The results of risk assessments performed recently for design-stage and operational LMR systems provide anecdotal evidence that state and local public safety agencies use the manual rekeying method. In cases where encryption is used, to permit their subscriber units to be manually rekeyed, radio users must bring the radios to a designated location for a physical connection to the key loader. This method is very cumbersome and manpower intensive. As a result, keys are not changed regularly or in some cases not used. Therefore, procedural and security problems inherent in the manual rekeying method occur. Discussions with federal radio managers indicate the same reliance on, and issues with, manual rekeying. Federal agencies manage these issues often by bringing key loaders to radio users (e.g., at command centers) to facilitate rekeying.

A key used to encrypt radio communications has a lifetime. Each time a key is used, it generates a ciphertext. Using the same key for a long period allows an attacker to have many ciphertexts available, which can make the key easier to break. Radio communications encrypted with keys that have not been changed for long periods of time are vulnerable to the threat of unauthorized interception using the technical advances in decoding technology.

4.2 Interoperability

Digital technology and the development of technical standards specified in TIA/EIA 102 (Project 25) enhance interconnectivity among local, state, federal and tribal public safety agencies. While interoperability provides greater benefits among public safety officials, it also raises new security issues related to the value of the shared information, level of encryption type, and responsibilities for security. Each public safety agency has its own specific operational requirements and environment. Therefore, key management procedures that may be suitable to one environment may not be appropriate for other agencies' environments.

Most public safety agencies have established mutual-aid agreements with other agencies. If the other agencies do not have compatible radio systems and the same type of encryption, sharing encrypted radio transmissions might not be feasible. When different types of voice

privacy encryption are used on radio transmissions, dual transition will prevent efficient interoperable mutual-aid operations.

Protected interoperability is possible when public safety officers from different agencies use a common key to perform different functions. However, this method has weaknesses on two fronts: keying material is not changed frequently, and not all radios support multi encryption keys. For these reasons, protected mutual-aid operations are difficult without some participants rekeying their radios.[4] To provide effective protected interoperable communications, better key management processes that address these two matters must be considered and established.

4.3 Insecure Storage of Encryption Keys

In general, encryption keys are stored on electronic media (e.g., diskettes or tapes) before or after key loading into KVLs. These media must be protected from unauthorized access with a proper key storage device (e.g., vault, safe, etc.) in a protected environment, and the keys should be stored in an encrypted form on the media. In particular, used keys should be stored in KMCs/KMFs during their cryptoperiod until they are deleted automatically or manually.

Stringent access controls must be in place through user identification and authentication methods (e.g., passwords, biometrics, or tokens) and proper privilege assignment. However, few public safety agencies have developed comprehensive computer security-related policies. Therefore, no requirements have been established for using stringent password constraints even though the systems used as KMCs/KMFs provide security features that can be configured to enforce these constraints. Unless stringent access controls are used, no assurance can be provided that keys cannot be compromised by internal and external threats. Once unauthorized personnel pass through the physical barriers, any key-related information stored in electronic media and computers could be easily compromised.

4.4 Lack of Training Materials

As public safety agencies begin to adapt to the new environment of using encryption more often, roles and responsibilities of encryption operators (i.e., crypto-custodians) who handle and maintain keys should be defined. Without roles and responsibilities being defined and assigned officially, the custodians can not be fully aware of the scope of their roles and can not have the positional authority necessary to perform these roles sufficiently well. Additionally, training programs for radio users should be established throughout public safety agencies. Custodians without specific training for handling keying materials (or keys) could mishandle keys or keying materials. Specific procedures should also be available to radio users to follow in emergency situations or for handling radios with encryption capability while unattended.

---

[4] *Multikey Over-the-Air Rekeying System, Test Report,* prepared by the VHF-UHF Subworking Group of the Communications Interoperability Working Group, December 28, 1990

4.5 Lost or Stolen Radios with Encryption

In manual rekeying systems no mechanisms are available to disable keys remotely (i.e., over-the-air) if radios with encryption are lost or stolen. Key revocation must be timely and reliable; otherwise, unauthorized people could compromise radios and confuse officers. The key fill devices should have physical security mechanisms to protect the contents of the cryptographic module from unauthorized physical access (e.g., by employing tamper-evident mechanisms). If the key fill devices (specifically, the removable covers) are accessed, all encryption keys contained in the cryptographic module should be erased. This process is known as "zeroizing" the key.

4.6 Unspecified Policy and Guidelines

The security issues addressed above all stem from unspecified guidelines on encryption key management. Because public safety officers focus on obtaining efficient and effective operational functions, adding on security or developing administrative guidelines are often afterthoughts. Many public safety agencies have not documented the information necessary to compile a complete set of specifications and requirements on key generation, storage, entry, key destruction, key changes, physical security mechanisms, and operating system security. Therefore, there is no assurance that encryption used for radio communications is compliant with Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*.

4.7 Comprehensive Key Management Procedures

The complexity of key management, which documents detailed instructions, methods, and network connectivity, discourages agencies from establishing comprehensive key management procedures. Thus, cost-effective solutions should be examined that can then be used by agencies with either a small network or a large network to efficiently manage encryption keys without endangering key security.

4.8 Improper Physical Security Controls

The lack of physical security controls for areas where keying materials are housed (e.g., rooms, communications centers, and maintenance facilities) seriously affects key security. Adequate physical security controls are the first protection for keying materials. Although radio managers are aware of the importance of physical security controls, resources (e.g., funding and personnel) are required to implement and enhance physical security controls suitable to their particular environments.

5. RECOMMENDATIONS

Various security issues and concerns regarding encryption key management were addressed in Section 4. This section discusses recommendations for establishing an encryption key management program that is, in general, applicable to public safety environments.

5.1 Establishment of Key Management Policy

As the first step, public safety agencies should establish key management policy that enforces the protection of keying materials (or keys) during their life cycle. The policy should ensure the confidentiality and integrity of keys and the encryption system and include, but not be limited to, the following elements:

- Private or encrypted communications shall be provided using proper encryption (e.g., Type 3) that meets the Federal Information Processing Standard (FIPS) 140-2 requirements.

- Encryption algorithms shall be as defined in the Federal Information Processing Standards (FIPS) Publication 140-2 and Publication 46-3, *Data Encryption Standard.*

- Integrity of keying material shall be ensured during all phases of its life, including its generation, distribution, storage, entry, use, and destruction.

- Keying material shall be controlled during its lifetime to prevent unauthorized disclosure, modification, or substitution.

- Keying material shall be distributed in a protected way to prevent unauthorized disclosure, modification, or destruction.

- Keying material shall be destroyed in a protected way to prevent unauthorized disclosure.

- Key access requirements shall be reviewed and endorsed by appropriate management personnel on a periodic basis.

- Keys received via electronic media shall be entered into the database on the KMC/KMF immediately upon receipt.

- Key generation equipment and storage devices shall be protected from unauthorized access through physical access controls.

- A copy of the Key Management Plan shall be stored in a protected environment and at an off-site facility to ensure the availability of information on keys and key components for backup.

5.2 Detailed Encryption Key Management Guidelines

Based on the established key management policy, key management guidelines (i.e., procedures) should be developed that provide detailed instructions on how to handle keys and keying materials properly. The key management guidelines should be designed to protect data encryption keys and associated keying materials from unauthorized disclosure, substitution, insertion, deletion, and recording. The guidelines should be reviewed regularly and updated to include changes made to the encryption system and its environment.

The guidelines should include, but not be limited to, the following:

- A strategy for implementing both encrypted voice and data communications to protect against threats
- The type of encryption to be used (e.g., DES, Triple DES, and AES)
- Source of key generation (e.g., self-generated and NSA-generated)
- Type of key generation (e.g., automatically, manually programmed with a key)
- Key changing method (e.g., manual, OTAR, or combination)
- Frequencies of changing keys (e.g., 7 days cryptoperiod)
- Procedures for protected storage of key materials and key loaders
- Destruction method (e.g., burning, pulverizing, chopping, shredding, and disintegrating)
- Location for KMCs/KMFs
- Primary functions of KMCs/KMFs
- Inventory controls for key-related equipment and devices
- Agencies or personnel responsible for managing KMCs/KMFs
- Points of contact for all keying materials
- Criteria for designating personnel who will access key materials (e.g., personnel on whom a background investigation has been conducted)
- Roles of crypto-custodians in performing a set of cryptographic operations

- Type of security training the custodians should take
- Number of people accessing key materials to generate, distribute, and destroy them
- Type of access controls for database (applications) storing information on keying materials (e.g., strong authentication, smart card, biometrics, or tokens)
- Type of physical access controls (e.g., key pad, combination locks, or badge access) for the room housing keys, key variable loaders, and key-related equipment
- Distribution of keys to the key storage room and vault to a limited number of authorized personnel
- Maintenance of key equipment and personnel responsible for performing regular and emergency maintenance
- Procedures for logging and reviewing all security-related activities related to keying materials
- Emergency response procedures.
- Proper generation of test and maintenance keys
- Procedures for handling and storing test and maintenance keys

5.3 Establishment of Security Training Program

Security training materials should be developed for crypto-custodians and radio users. Access to cryptographic software should be restricted to crypto-custodians who are trained properly to perform crypto functions and who have security knowledge related to encryption key functions. The training materials for crypto-custodian should address the following elements:

- Specific administrative functions to manage and change keys
- Installation of all cryptographic software only as executable code to prevent unauthorized modifications by users
- Loading and executing of cryptographic processes to prevent accidental modification
- Detailed security functions provided by encryption devices
- Responsibilities relevant to protected operations of keying material

- Computer-controlled security functions (authentication methods to access cryptographic software)

- Physical security controls

- Incident report procedures

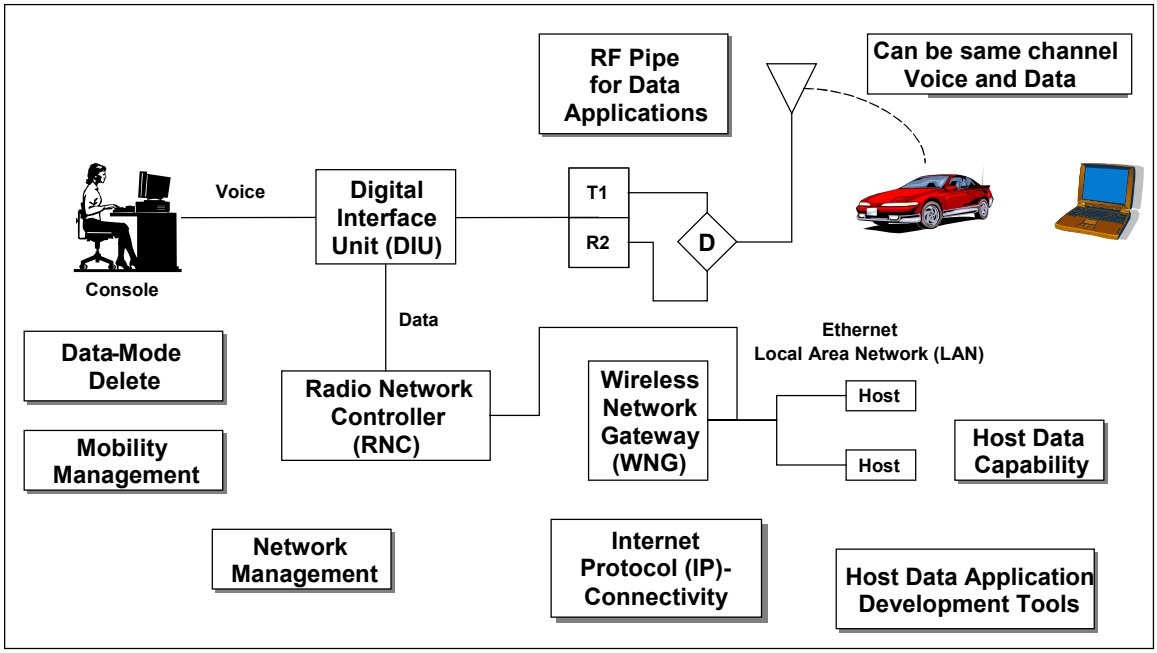
- Configuration of audit mechanisms of the encryption device to record—
  - Start-up and shutdown of the audit functions
  - Any attempt to modify or delete the audit trail
  - Attempts to provide invalid input for crypto-custodian functions
  - Addition or deletion of crypto-custodian role.

Training materials for radio users should include information on the importance of encryption usage and on how to use the encryption. In addition, basic operations of radios with multikeys should be included in the training.

5.4 Over-The-Air-Rekeying Technology

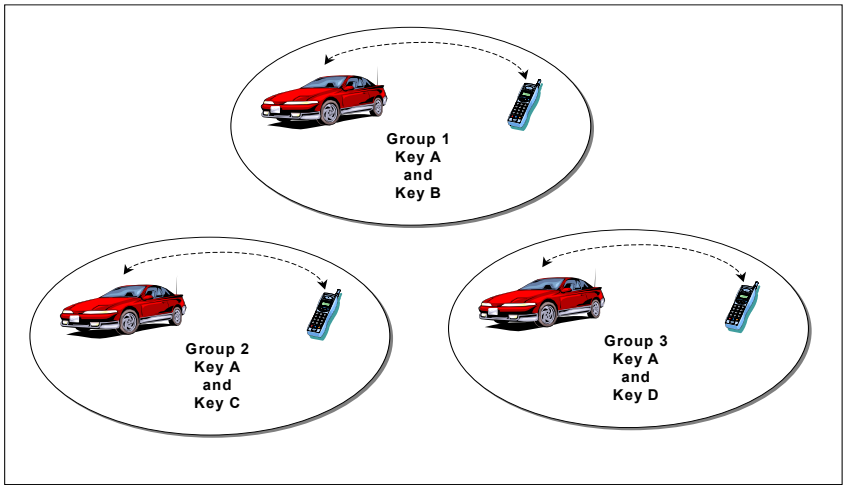
A centralized control over encryption keys can reduce procedural, operational, and security problems and cost, assuring the integrity of keys at a high level. An Over The Air Rekeying (OTAR) capability has been examined by law enforcement agencies to solve the problems associated with manual rekeying and to ensure encrypted communications among agencies. With the OTAR technology, it takes users only a few seconds to rekey their radios over the air from a remote location—allowing for easier and more regular rekeying, and resulting in timesavings. The OTAR channel can also be used for digital voice in the encrypted mode for emergency interoperability. Figure 4 in the following page depicts the TIA 102 OTAR architecture.

Figure 4. TIA 102 OTAR Architecture



The multikey radios capable of using the OTAR method allow for transmitting new and updated encryption codes to large numbers of radios over an existing radio network and simplify the changing of encryption keys when users roam.[5] Multikey provides the capability of equipping a radio with multiple encryption keys using the same algorithm, group partitioning, and interoperability. Typically, multiple keys are simultaneously distributed to all radios within a group. Figure 5 presents an example of multikey operation.

Figure 5. Multikey Operation



5 Multikey Over-the-Air Rekeying System, Test Report, prepared by the VHF-UHF Subworking Group of the Communications Interoperability Working Group, December 28, 1999

However, the OTAR method raises new issues. Implementing the OTAR technology requires additional infrastructure that supports OTAR related activities. As a result, the initial capital investment will be higher. It also raises concerns regarding how to properly manage the OTAR network and the OTAR KMFs that provide OTAR cryptographic capabilities. In particular, interoperability of critical public safety radio communications requires that each agency meet OTAR requirements and agreements made among public safety agencies to control their own or shared keys. Therefore, an encryption key management program must identify OTAR security requirements and responsibilities of public safety agencies using the centralized OTAR KMFs, as well as operational requirements.

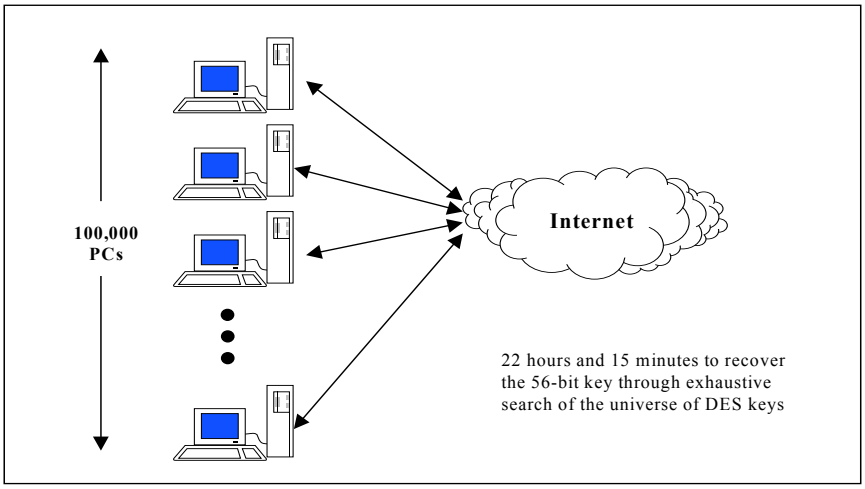
Currently, U.S. Treasury Bureaus and Department of Justice have taken the lead in the use of the OTAR capability, and more agencies are planning to participate in using the capability for their existing and new systems. To make it more effective, the OTAR technology should provide the following capabilities:

- Provide end-to-end protected communications from the communications center to the radio user in the field
- Provide a KMF that provides OTAR functions, storage of keying material, logging, and inventory control
- Allow an operator to rekey either individual radios or groups of radios
- Allow efficient key change in a compromised situation
- Allow over-the-air key zeroization and manual key zeroization to prevent a lost or stolen radio from being used to compromise public safety radio communications
- Document how to transmit a key to the registered radios
- Document interagency operating procedures for using OTAR networks.

5.5 Use of Better Secure Algorithms

DES is being replaced in various communities, including the financial community. To enhance DES security, keys must be frequently changed and known plaintext must be avoided. As discussed previously, when encryption keys are not changed frequently, they can be broken by key search attacks (e.g., SKIPJACK, EFF DES Cracker) over time. Figure 6 depicts the recent coordinated DES attack.

Figure 6. Recent Coordinated DES Attack



An alternative for DES is Triple DES that has been adopted by TIA/EIA 102. Within Triple DES, the plaintext can be encrypted with three keys using a different key each time.

6. CONCLUSIONS

Proper encryption key management is the overall process of generating and distributing cryptographic keys to authorized recipients in a protected manner. It ensures the integrity and confidentiality of keys and keying materials during their life cycle. Without established key management processes, encryption keys or keying materials can be compromised by internal threats (e.g., disgruntled employees) or external attacks.

To provide key management that offers cost-effectiveness and interoperability, central control over all key management functions is needed within an agency or among agencies sharing radio communications. The key management procedures established should allow each agency to manage its own security control objectives on either a geographical or a functional basis, but still work with the central control to maintain interoperability standards and avoid conflicts in device control and areas of jurisdiction.[6]

First, encryption used for radios should meet the current standards (e.g., FIPS 140-2) to provide the same voice privacy on all radio frequency (RF) transmissions. OTAR technology can provide benefits for interoperability in joint operations and enhance encrypted communications. It also enhances key security through frequent key changes and the ability to disable keys over the air when required.

It is important that each public safety agency examines the sensitivity of its operations and the information it transmits and develops agency-specific key management policy and guidelines. Senior-level management (i.e., decision makers) of public safety agencies must establish a key management policy and define requirements for encryption keys and keying materials within their associated operating environments. This policy should be the basis on which guidelines are developed. These guidelines should define the procedures for controlling and handling of keying materials. The guidelines should be reviewed regularly to ensure that any new technology to be employed is included in the guidelines.

Finally, public safety management must make an informed decision regarding the adequacy of security training for crypto-custodians and radio users and remedy any shortfalls through additional training.

---

6 U.S. Department of the Treasury, Treasury Directive Publication 71-10, *Security Manual,* 1993

APPENDIX A—LIST OF ACRONYMS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DIU	Digital Interface Unit
FIPS	Federal Information Processing Standards
IP	Internet Protocol
KMC	Key Management Controller
KMF	Key Management Facility
KVL	Key Variable Loader
LAN	Local Area Network
NSA	National Security Agency
NIST	National Institute of Standards and Technology
OTAR	Over-the-Air-Rekeying
PRNG	Pseudorandom Number Generator
RF	Radio Frequency
RNC	Radio Network Controller
RNG	Random Number Generator
TIA/EIA	Telecommunications Industry Association/Electronics Industry Alliance
WNG	Wireless Network Gateway
LMR	Land Mobile Radio
PSWN	Public Safety Wireless Network

APPENDIX B—GLOSSARY

Access Control. A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs or to obtain data from, or place data onto, a storage device.

Algorithm. A set of mathematical rules (logic) used in the processes of encryption and decryption.

Audit Record. A chronological record of system activities that is sufficient to reconstruct and review the sequence of events surrounding or leading up to all transactions and actions performed on or by the system.

Authentication. The process of verifying the identity of a user, terminal, or application program to prevent fraud, abuse, and misuse of services.

Availability. The accessibility and usability of service on demand by an authorized entity.

Confidentiality. The protection ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Crypto. A marking or designation identifying keying material used to secure sensitive information.

Crypto-custodian. The person designated in writing by proper authority to be responsible for the generating, storing, safeguarding, and destruction of keying materials.

Cryptography. Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Encryption. The process of transforming plain text into unintelligible form by using a cryptographic system.

Identification. A code, user name, card, or token that identifies an individual.

Integrity. The protection that ensures that data has not been altered (i.e., modified, inserted, or deleted), repeated, or destroyed in an unauthorized manner, either accidentally or deliberately.

Interoperability. The condition achieved among communications-electronics systems or equipment when information can be exchanged directly between them and their users.

Key. A series of characters used by an encryption algorithm to transform plain text data into encrypted (cipher text) data and vice versa.

Key Management. The process, policies, procedures, and administration encompassing every stage in the life cycle of a cryptographic key, including generation, distribution, entry, use, storage, destruction, and archiving.

Key Management Controller. An electronic device (desktop computer) that is used with analog LMR network and uses proprietary data signaling for key encryption.

Key Management Facility. An electronic device (desktop computer) that is used with digital LMR network and uses standards based signaling for key encryption.

Key Variable Loader. A hand-held device used to load encryption keys into a radio

Keying Material. Key, code, or authentication information in physical or magnetic form.

Over-the-Air Rekeying. OTAR refers to the distribution of cryptographic keys by transmitting the information over a radio system.

Password. A protected word, phrase, or a string of characters used to authenticate the identity of a user.

Risk. A measure of the potential degree of loss; the degree of loss expressed as the likelihood of a threat occurring multiplied by the expected loss incurred.

Unique/Protected Key. A crypto key that is used in a secret key algorithm.

Server. Computer devices or processes that provide service to clients in a client/server architecture.

Session Key. The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key or set of session keys is used for each communication session.

Symmetric key. Same key used to encrypt and decrypt data.

Threat(s). Person, thing, event, or idea that poses some danger to an asset. The occurrence of a threat might compromise the confidentiality, integrity, or availability of an asset by exploiting vulnerabilities.

Vulnerability. A weakness in a system's design or procedure that could be exploited by a threat to gain unauthorized access to a system or degrade the system's availability.

APPENDIX C—REFERENCES

Harold Abelson, et.al., *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption,* www.cdt.org/crypto/risks98.

American Bankers Association, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, ANSI TG-19, Washington, DC, 1999.

American Bankers Association, *American National Standard for Financial Institution Key Management (Wholesale)*, ANSI X9.17, Washington, DC, 1995.

Communications Interoperability Working Group*, Multikey Over-the-Air-Rekeying System Test Report*, December 28, 1990.

National Institute of Standards and Technology*, Specifications for Key Management Using ANSI X9.17*, FIPS Publication 171, April 27, 1992.

National Institute of Standards and Technology, *Data Encryption Standard*, FIPS Publication 46-3, October 25, 1999.

National Institute of Standards and Technology*, Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, January 11, 1994.

National Institute of Standards and Technology, *Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)*, Docket No. 970725180-7180-01.

National Institute of Standards and Technology Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.

Randall K. Nichols, *ICSA Guide to Cryptography*, McGraw-Hill, ISBN 0-07-913759-8, 1999.

U.S. Department of the Treasury, *Security Manual*, April 30, 1993.