SAFECOM
Federal Partnership for FPIC Interoperable Communications
NCSWIC

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

Developing Methods to Improve Encrypted Interoperability in Public Safety Communications

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 and response.

Successful encrypted interoperability depends largely upon improved coordination between agencies needing to interoperate. Encryption key management is also enhanced when all agencies understand how to use and coordinate key management. Improperly managed key parameters can affect radio users' ability to interoperate. If agencies choose to implement encryption, it is important that encryption and key management becomes an organizational priority implemented in a consistent manner across all public agencies with interoperability needs.

THE REPORT

The Federal Partnership for Interoperable Communications (FPIC), in coordination with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), developed this report in response to a growing need to improve encrypted interoperability at all levels of government. The *Best Practices* discussed in this document provide an overview of how basic key management parameters are related in Project 25 land mobile radio (P25 LMR)[1] systems. The document also addresses methods to improve cross-agency coordination, and emphasizes the use of standards-based encryption, to enhance secure interoperability minimizing the risk of compromising sensitive information. Primary *Best Practices* to improve encrypted interoperability include:

- **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.

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

May 2016

[1] Project 25 was previously referred to as APCO Project 25, now simply P25.

- **Standards-based Encryption –** Use P25 standard AES-256[2] security solution to protect against compromise.
- **Crypto Period Considerations –** Define and implement feasible crypto periods to mitigate risk.
- **Communications Planning –** Develop Communications Plans that incorporate encryption requirements.
- **Education and Training –** Develop appropriate training for both system personnel and field operational users to improve effectiveness.
- **Exercise and Testing -** Develop and execute regular communications exercises and testing to maintain effectiveness.
- **Outreach –** Collaborate with knowledgeable experts to ensure effective encryption implementation.

This document highlights best practices of key management necessary to allow encrypted operability and interoperability. Fundamentally, the intent of this document is to simplify the complex process of encryption and key management and discuss *the essential elements or parameters that are needed for operability and interoperability*. This document identifies *Best Practices* for basic aspects of encryption key management, making encrypted interoperability possible and manageable among public safety agencies at all levels of government.

ANSI/TIA 102 Series of Project 25 Standards explain how encryption works in a P25 system and how encryption protects sensitive information. The National Institute of Standards and Technology (NIST) SP 800-57 series of publications[3] describe methods of key management. This document provides details on how and why specific encryption parameters are crucial to maintaining system security and enable interoperability in the encrypted mode.

IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

These best practices are important in developing system security where encrypted interoperability is realizable. Additionally, significant planning and coordination must be undertaken to achieve encrypted interoperability on a national scale. Leadership in developing more detailed encryption guidelines and further education of the user community must occur. These best practices align with the guiding principles of the Interoperability Continuum.[4] The goals are based on increased interoperability by effective leadership, planning, and collaboration among public safety agencies. To that end, adherence to established *Best Practices* for encryption will provide

- **Cost efficient implementation**
- **Effective protection of sensitive information**
- **Credible standards-based policy development**
- **Successful encrypted interoperability during multi-agency emergency response**

The public safety community can achieve encrypted interoperability at the local, regional, state, and national level by collaborating with the other users and encryption experts. Effective planning, cooperation, governance, and a basic understanding of how key parameters are coordinated can lead to successful *Encrypted Interoperability*.

[2] NIST FIPS 197, *Advanced Encryption Standard*, Nov 2001
[3] NIST SP-800-57, *Recommendation for Key Management, Parts 1-3*
[4] http://www.dhs.gov/publication/commonly-accessed-documents-safecom