P25 Steering Committee Priorities: ISSI/CSSI Interoperability- Linking P25 Systems, KMF/KFD Encryption Key Interoperability, P25 Education and Outreach, P25 Testing

Jim Downes

James.Downes@cisa.dhs.gov

Cybersecurity and Infrastructure Security Agency (CISA)

Project 25 Steering Committee Chair

Presented by:
PTIG - The Project 25 Technology Interest Group

www.project25.org

Federal Partnership for Interoperable Communications (FPIC) and P25 Steering Committee Update

- Improve Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) interoperability
- Improve key management facility and key fill device interoperability capabilities
- Address encryption and key management vulnerabilities
- Increase P25 user input to the standards process
- Energize P25 education and outreach program
- Expand P25 test procedures
- Support P25 Land Mobile Radio/Long-Term Evolution interworking activities

The FPIC ISSI/CSSI Working Group developed guides for planning ISSI and CSSI implementation

Volume I includes pre-planning, partnerships, and governance

Pre-Planning
Conducting cost/benefit analysis, education, and training

Partnerships
Identifying partnering agencies, coordination

Governance
Determining governance structure, memorandum of understandings, and other agreements

Volume II was published in July 2020 and covers stakeholder engagement, policies, technology, and thinking ahead

Stakeholder Engagement
Radio personnel, network professionals, radio and consoled end users, and manufacturer personnel

Policies
Standard operating procedures, memoranda of understanding, and version control

Technology
Network connections, infrastructure, consoles, subscriber units, and features

Thinking Ahead
Maintenance plans or agreements and system upgrades

Both volumes are available at www.cisa.gov/safecom under Resources.

ISSI Fact Sheet

ISSI/CSSI Primer

- Provides a high-level overview of a broad range of introductory topic areas relevant to ISSI and CSSI
- Published in February 2019

FPIC Features and Functions Product Development Group focusing on education and outreach materials for:

- Emergency Alarm and Emergency Alarm Cancel
- Cross-Patching
- Radio Inhibit
- Unit Aliasing
- Automatic Roaming

Encrypted interoperability enables

- protection of sensitive information
- effective communication with neighboring jurisdictions, task forces, and other public safety responders

Public safety community realizing need for encryption services within public safety systems

FPIC membership recognizes issues with implementing encryption and continues to examine ways public safety community can utilize encryption services

Focused on:

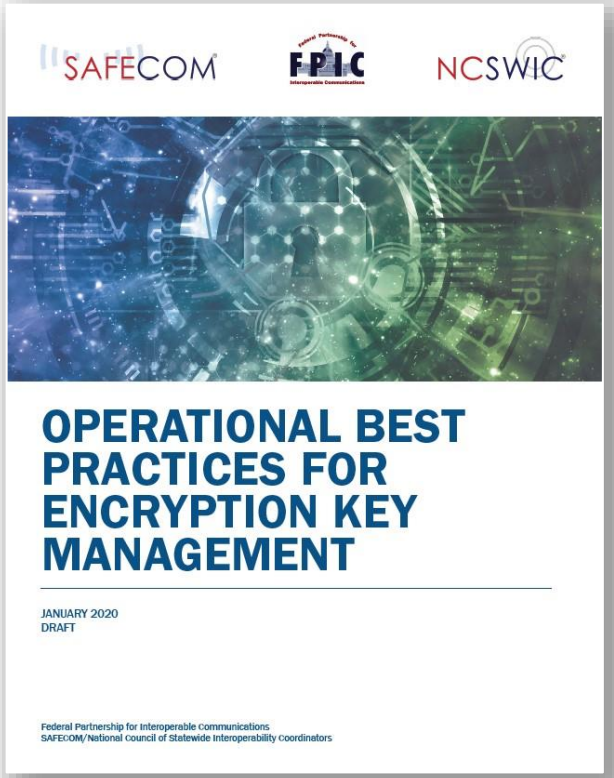
- Data Encryption Standard (DES) - outdated and ineffective
- Addressing key change periods
- Specific key management and key distribution vulnerabilities and best practices

Developed Operational Best Practices for Encryption Key Management and Encryption Fact Sheet documents

Continuing to work with National Institute of Standards and Technology and National Law Enforcement Communications Center

Operational Best Practices for Encryption Key Management document addresses:

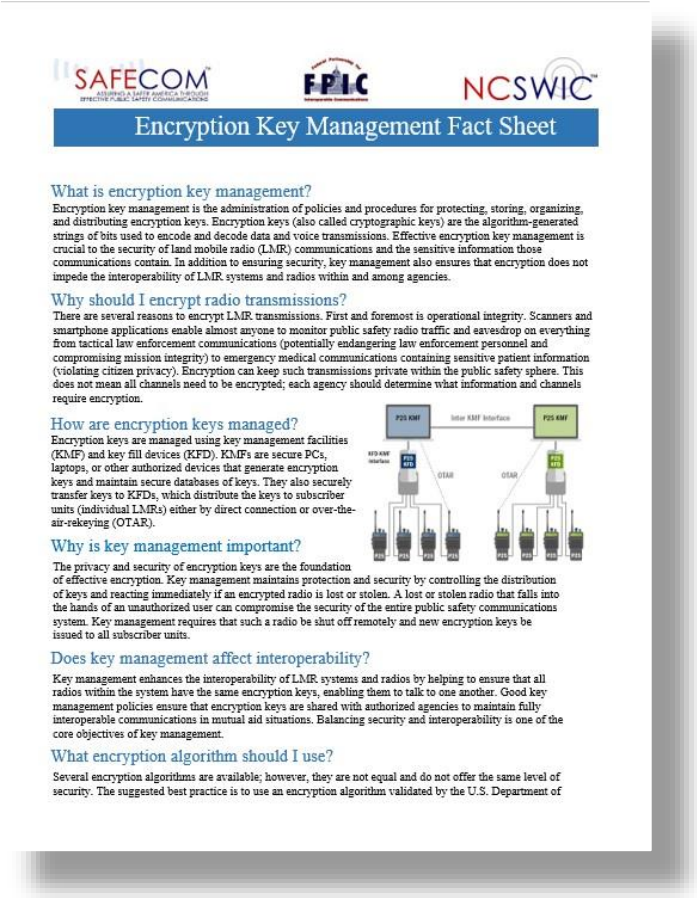
- Best practices for key management, distribution, and governance among partner agencies based on lessons learned
- Vulnerabilities with continued use of DES, including Triple DES and DES-XL and proprietary algorithms
- Risks associated with inconsistent



The Encryption Key Management Fact Sheet is intended for public safety agencies interested in implementing encryption

Provides high level overview of encryption and its importance

Stresses importance of proper key management and its impact on interoperability



SAFECOM FPIC NCSWIC

Encryption Key Management Fact Sheet

What is encryption key management?

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

Why should I encrypt radio transmissions?

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

How are encryption keys managed?

Encryption keys are managed using key management facilities (KMF) and key fill devices (KFD). KMFs are secure PCs, laptops, or other authorized devices that generate encryption keys and maintain secure databases of keys. They also securely transfer keys to KFDs, which distribute the keys to subscriber units (individual LMRs) either by direct connection or over-the-air-rekeying (OTAR).

Why is key management important?

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

Does key management affect interoperability?

Key management enhances the interoperability of LMR systems and radios by helping to ensure that all radios within the system have the same encryption keys, enabling them to talk to one another. Good key management policies ensure that encryption keys are shared with authorized agencies to maintain fully interoperable communications in mutual aid situations. Balancing security and interoperability is one of the core objectives of key management.

What encryption algorithm should I use?

Several encryption algorithms are available; however, they are not equal and do not offer the same level of security. The suggested best practice is to use an encryption algorithm validated by the U.S. Department of

ISSI/CSSI Conformance Test Tool (ICCTT) Validation Products Document

- High-level framework document available by email request
- Comment matrix
- Compliance Assessment Bulletin (CAB) in development

Newly Accredited Labs for ISSI/CSSI Testing

- Department of Interior – Conformance
- EF Johnson Technologies – Conformance, Interoperability
- Compliance Testing LLC – Interoperability

P25 Feature Gap Analysis

Next P25 CAP Open Meeting: Nov/Dec 2020

Program Updates & Upcoming Events

https://www.dhs.gov/science-and-technology/p25-cap
or email P25CAP@hq.dhs.gov

S&T Virtual Booth at IWCE

ISSI/CSSI Conformance Test Tool (ICCTT) Validation Products Document

- High-level framework document available by email request
- Comment matrix
- Compliance Assessment Bulletin (CAB) in development

Newly Accredited Labs for ISSI/CSSI Testing

- Department of Interior – Conformance
- EF Johnson Technologies – Conformance, Interoperability
- Compliance Testing LLC – Interoperability

P25 Feature Gap Analysis

Next P25 CAP Open Meeting: Nov/Dec 2020

Program Updates & Upcoming Events

https://www.dhs.gov/science-and-technology/p25-cap
or email P25CAP@hq.dhs.gov

S&T Virtual Booth at IWCE

Project 25 Steering Committee & FPIC Education & Outreach IWCE 2020

For More Information on Project 25 Go to:

www.project25.org

www.cisa.gov/safecom

Stephen Nichols, Project 25 Technology Interest Group Director: director@project25.org
Jim Downes, Cybersecurity and Infrastructure Security Agency (CISA), Project 25 Steering Committee Chair: James.Downes@cisa.dhs.gov