National Public Safety Telecommunications Council

Radio Interoperability Best Practices

Best Practice #11
Managing Encryption for Interoperability Resources

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

The use of voice encryption on designated interoperability and mutual aid channels can create obstacles to interoperability and is highly discouraged. In the event encryption is deemed necessary due to unique operational needs, it must follow existing FCC regulations and comply with an approved regional communications plan.

Scope of this Best Practice

For the purposes of this Best Practice, "interoperability Resources" is not limited to the FCC designated public safety interoperability channels, but includes any channel intended to be shared in the context of multi-agency or multi-jurisdictional responses.

This best practice does not intend to instruct an agency how to manage encryption, nor provide a technical description of how it works. The Related Documents section of this Best Practice contains links to several of the numerous publications available for referencing encryption technologies and management.

Statement of Importance

Interoperable communications are critical to the success of any response when multiple jurisdictions or disciplines are involved. There are standards for the public safety

interoperability channels[1] that include channel naming and CTCSS tones and NAC settings. Adding encryption to interoperability channels can create additional challenges and confusion. There are reported cases in After Action Reports where encryption was a factor in the inability to communicate.

The decision to use encrypted interoperable communications must be made with the understanding that encryption can add a significant level of complexity and should be considered only when the operational requirements of the incident outweigh the additional complications.

There are various encryption technologies in Land Mobile Radio (LMR). AES 256 is the current standard for all Federal LMR devices and is recommended as the standards based highly secure, encryption protocol. The Department of Homeland Security also issued rules in March 2017 that requires Project 25 (P25) radio equipment which incorporates encryption to include AES 256. If other non-standard encryption protocols are being used by interoperable agencies, the resultant barrier to communications must be addressed.

Access to the keys is an important element in encryption management. The Federal Partnership for Interoperable Communications (FPIC) Security Working Group has recommended all agencies that employ DES-OFB or AES encryption utilize keys generated by the National Law Enforcement Communications Center (NLECC) and the adoption of the SLN Database for national use. In addition, FPIC also recommends that a common Key ID database be developed and utilized to minimize the possibility of duplication of these keys.

Supporting Elements

The use of encryption has increased as technologies for monitoring public safety become more accessible. The options include scanners both digital and trunked, web based scanner services and smart phone apps and the use of those options can be detrimental to operations. Law enforcement needs secure communications and what was initially limited to SRT and SWAT operations have become options for daily use[2]. Fire and EMS agencies are also becoming interested in encryption as a means of protecting patient privacy and sensitive information in emergency incidents.

Encryption on some of the nationwide interoperability channels is governed by regulation. In 2016, the FCC issued Report and Order, PS Docket No. 13-209[3] and Report and Order, PS Docket No. 15-199 revising Section 90.20(I)[4]. In the first, the FCC confirmed that analog FM is

---

[1] APCO/NPSTC 1.104.2-2017 Standard Channel Nomenclature for Public Safety Interoperability Channels - http://www.npstc.org/download.jsp?tableId=37&column=217&id=17&file=CommonChannelNamingDocument_11042_2017_180221.pdf

[2] https://wiki.radioreference.com/index.php/Encrypted_Agencies

[3] Analog Voice Operations

[4] Railroad Police Eligibility

required for interoperability and modified its rules to require the use of analog FM as the common modulation scheme for mobiles and portables operating on the designated public safety nationwide interoperability channels in the VHF, UHF, and 800 MHz bands. The FCC decision is specific to the designated nationwide public safety interoperability Calling and Tactical channels. This FCC order does not mention encryption; however, the mandate for analog operations prevents the use of digital encryption. As the 700 MHz band is digital only, it was not addressed in this order.

The second Report and Order issued later that year authorizes railroad police departments to access nationwide interoperability channels. This order included an appendix of those channels and prohibits encryption on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz and 700MHz bands. However, it does not supersede the requirement for analog FM modulation noted above on the calling and tactical VHF, UHF and 800 MHz band nationwide interoperability channels.

As a combined result of these two releases:

- Encryption may not be used on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz, and 700 MHz bands.
    - VCALL10
    - UCALL40
    - 8CALL90
    - 7CALL50, 7CALL70
- Encryption may not be used on designated tactical channels in VHF, UHF and 800.
    - VTAC (VTAC11-14) & (VTAC33-38)
    - UTAC (UTAC41-43)
    - 8TAC (8TAC91-94)

The FCC Orders do not apply to certain channels, where encryption is not prohibited by regulations such as:

- Mutual Aid Channels
    - VFIRE, VMED, VLAW
    - UHF MED frequencies –
- 700 MHz Tactical Channels
    - 7LAW, 7FIRE, 7TAC, 7MED,
    - 700 MHz Air to Ground channels
- NTIA designated channels
    - IR and LE

- State, regional, and local interoperability channels and talkgroups if allowed by SIEC/Local Authority

Though the use of encryption is not prohibited on these channels, it is discouraged except when it is determined to be the only solution and requires a concerted commitment and effort to ensure interoperability. Even with prior planning and protocols that support encryption for first responders within a region, it is important to recognize that mutual aid units from outside the region may arrive without encryption capabilities. Encryption is basically a very complex alpha-numeric password referred to as a "key" This key is very difficult to hack without tremendous supercomputer capabilities. Even though the numbers of combinations are astronomical, keys must be updated periodically to avoid the possibility of key compromise.

When a voice (or text) transmission occurs, the key is used to encrypt the information so it cannot be captured in transmission. The receiving device or console has the same key that is able to decrypt the message and reassemble it exactly as before encryption. (See Figure 1)

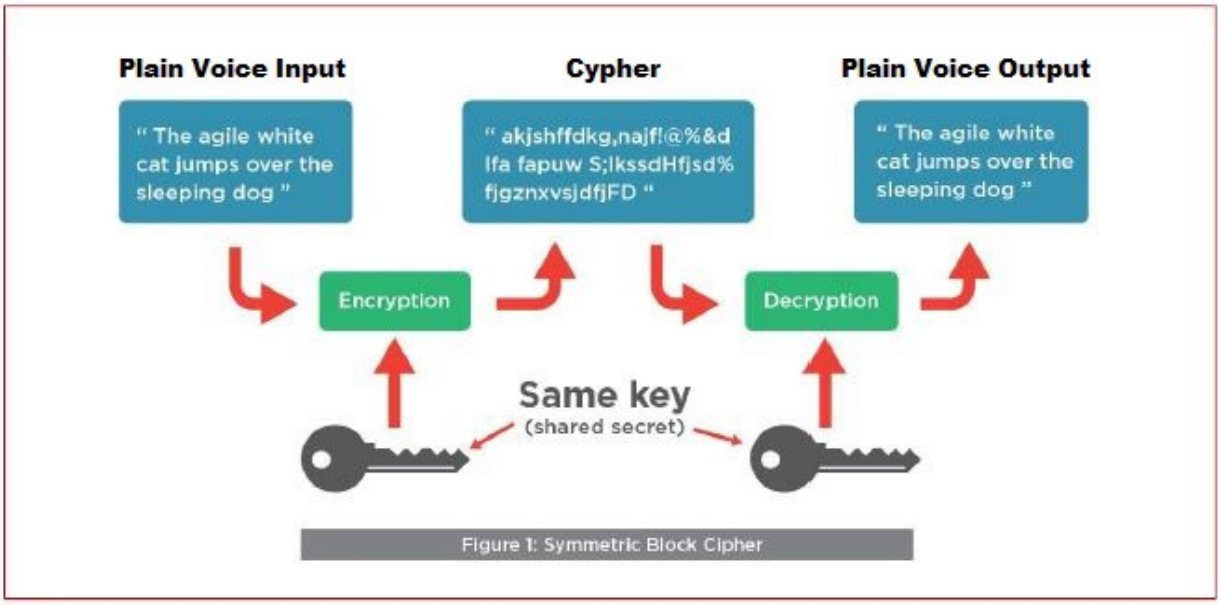

Figure 1: Symmetric Block Cipher

When the operational requirements outweigh the additional complexity of encryption, such as scene security, privacy, or other life safety issues, then encryption may be necessary, where authorized by FCC rules. The decision to encrypt interoperability channels must include all agencies that would have the channels in their devices and consoles.

The decisions that need consensus include:

- Which channels will be encrypted?
- Do all agencies operate with the same encryption technologies and algorithms?

- Do all agencies have the staffing and budget to support the planned key management profile?
- Who will control the keys?
- How and how often will the keys be updated?
- When will the keys be updated and what validation protocol will be employed?
- Are there channels "in the clear" available in the event interoperability is lost?
- Agreement and notification to all impacted agencies on the timeline and transition plan for implementing encryption
- Agreement on field user and PSAP training regarding the proper use of encryption, covering both governing policy and the technology involved.

SAFECOM Continuum

Managing Encryption for Interoperability Resources touches every lane of the Continuum which effectively demonstrates its importance in creating an interoperability solution.

Incident Use Case

The Stanford County Department of Health, Emergency Medical Services (EMS) Agency recently switched all paramedic-hospital contact to a P25, AES 256-bit encrypted, trunked radio system operated by the County. The decision to do so was based on incidents where celebrity residents were identified by address and patient information was at risk of public release.

The EMS Agency licenses 47 emergency medical Advanced Life Support (ALS) providers and 16 base hospitals for ALS radio contact. The providers include fire departments, private ambulance companies, Sheriff SWAT Teams, and aero-medical services. Adding to those user devices are the 16 base hospitals that interface with the field units.

The need to coordinate encryption keys was recognized early and key management was assigned to the Sheriff's Department. The Department determines which keys will be utilized, what month the re-keying will occur, and shares the information at the monthly EMS Agency/Stakeholder meetings. The date and time of Over-the-Air Re-keying (OTAR) is shared at least 2 months prior to give each stakeholder time to plan for updating. Those agencies that do not have radios capable of OTAR are in particular need to plan ahead. The time of day is chosen to maximize stakeholder's ability to assure OTAR is successful. This would likely be in the early morning hours and would be completed before the daily paramedic-hospital radio check.

Migration Path

Public safety agencies wishing to deploy encryption on their interoperability channels need to become educated on the regulations controlling encryption. They need to understand what other entities are likely to operate on those channels and what encryption technology they utilize. Disparate technologies must be reconciled before entering any agreement.

Agencies should understand the staffing and other budgetary elements that encryption might introduce.

Next, an agreement on encryption policy needs to be formalized between all stakeholders. They must agree to all the key management parameters, including who controls the keys, how do agencies access the keys, when are keys updated, and how are the keys updated. There should be a process for immediate troubleshooting should encryption hamper response efforts.

Responders and dispatchers need to be trained on the major points of encryption. They must know which channels are encrypted, how and when to disable encryption (if capable), and what events might cause inadvertent "in-the-clear" transmissions, such as patching.

Related Documents –

FCC PS Docket 15-100 – Amendment of Part 90 of the Commission's Rules to Enable Railroad Police Officers to Access Public Safety Interoperability and Mutual Aid Channels - https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-113A1.pdf

Report on the Use of Encryption on the Interoperability Channels - https://www.google.com/url?q=http://www.npstc.org/download.jsp%3FtableId%3D37%26column%3D217%26id%3D3854%26file%3DEncryption_on_Interoperablity_Channels_FINAL_20170131.pdf&sa=U&ved=0ahUKEwiDuovTx8nWAhVKw2MKHSBKA2QQFggFMAA&client=internal-uds-cse&usg=AFQjCNH9vlXOCnitJnmINw7cHdSxG_uSVg

Guidelines for Encryption in Land Mobile Radio Systems - https://www.dhs.gov/sites/default/files/publications/20160204_Guidelines%20for%20Encryption%20in%20Land%20Mobile%20Radio%20Systems_Final508c_0_0.pdf

Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems - https://www.dhs.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption_Final%20Draft508_0.pdf

Developing Methods to Improve Encrypted Interoperability in Public Safety Communications (Fact Sheet) - https://www.dhs.gov/sites/default/files/publications/20160830%20Fact%20Sheet%20Best%20Practices_Final%20Draft508_1.pdf

Considerations for Encryption in Public Safety Radio Systems - https://www.dhs.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf

Project 25 Compliance Assessment Program Encryption Requirements - http://www.npstc.org/download.jsp?tableId=37&column=217&id=3891&file=P25_CAP_Encryption_Requirements_March_2017.pdf

NPSTC Outreach Article, March 27, 2017 - http://www.npstc.org/article.jsp?id=1722

LMR Encryption – Navigating Recent FCC Rule Changes (slide deck) – NPSTC Presentation at the APCO Western Regional Conference - http://www.npstc.org/download.jsp?tableId=37&column=217&id=3910&file=APCO_WR_2017_Encryption_Final_20170413.pdf

Encryption on P25 CAP approved - https://www.dhs.gov/science-and-technology/news/2017/03/27/news-release-encryption-requirements-change-p25-cap-approved

Date Approved

January 9, 2018

Contributors

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.