Encryption Recommendations and Best Practices

Purpose:

Provide education and guidance to police, fire, emergency medical, emergency management, transportation, public works and critical infrastructure governmental agencies regarding the programming, keyloading and use of encryption features on 700/800 MHz radios.

Background:

The Michigan Public Safety Interoperable Communications Board (MIPSCIB) has been charged with the responsibility of coordinating interoperable public safety communications in Michigan. Numerous public safety agencies and governmental disciplines use 700/800 MHz trunked and conventional radios intended to provide interoperable communications between all public safety and governmental disciplines. Radios on the Michigan Public Safety Communications System (MPSCS) are programmed with a basic radio interoperability template that included statewide interoperable talkgroups as well as 700/800 MHz analog and digital channels that are part of the non-Federal national interoperability plan.

At the request of public safety members, and by the growing demand for a solution to provide more secure radio communications, the MPSCIB has drafted this document to provide education, give guidance, and set a path/process for users and the MPSCS Radio Programming Unit (RPU) to add encryption features to radio templates for use during day-today operations, or at significant events where transmission of sensitive information over non-encrypted radio channels may put the safety of personnel or the public at risk.

As a result, the MPSCIB has adopted these recommendations best practices to help promote the education and guidance for all users, while maintaining a high level of interoperability for mutual aid clear/open and encrypted/secured communications.

Types of Encryption Algorithms

- **ADP (Advanced Digital Privacy)/ARC4** Low security encryption. Usually loaded in template but can be loaded with keyloader.
- **DES-OFB (Digital Encryption Standard Output Feed Back)** Medium security encryption that is usually loaded with keyloader but can be loaded with software.
- **AES256 (Advanced Encryption Standard**) High security (Federal Grade) encryption that can be loaded with keyloader or software (in some radios).

Encryption Activation Settings

There are three different states for encryption: Clear, Selectable and Strapped (secure).

- **Clear** is used when there is no encryption on the talk-group and the encryption cannot be turned on.
- **Selectable** can be used to turn encryption on or off using a switch or button or other radio feature selectable setting.
- **Strapped** is used when the talk-group is always encrypted and cannot be turned off.
- **Infinite Key Retention:** Selected in the radio template/programming to retain the keys if power is removed from the radio. If unchecked the radio will lose all keys if power is removed and that talkgroup may lose the ability to transmit on encrypted talkgroups on the system.

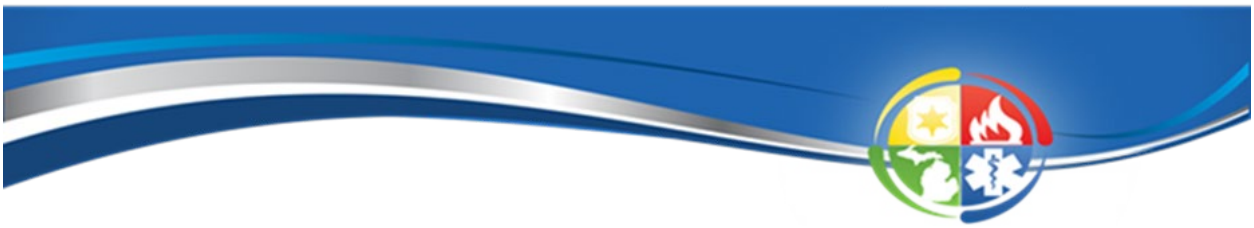
Encryption Feature Recommendations:

1. Use **strapped** when using talkgroups that are always going to be encrypted. (Examples = Drug Team, Tactical or Agency Specific “Proprietary” talkgroups).
2. Use **selectable** for Zone I and J Event talkgroups.
3. **Infinite Key Retention:** Recommended that it is checked in the programming to be selected to retain the keys.
4. **Encryption interoperability** Recommends that certain keys be shared between agencies to allow interoperability across different talkgroups.

Talkgroup Encryption

Talkgroups can have different levels of encryption depending on how they are used. Any talkgroups that are used for interoperability with different agencies or have the possibility of someone not having encryption should not use the encryption feature. This would include but not be limited to county main dispatch, common, special event and interop channels/talkgroups. If there is a need for encryption on county interop channels/talkgroups, you should split them over several channels with talkgroups that are designated with some being clear and some being strapped.

If the talkgroup needs to be both encrypted or clear depending on how it is used and who has access to encryption then it should be set to selectable. This should mainly be used for talkgroups that cover a large area and are in a large number of radios. The MPCSC Zone I and J event talkgroups use this selectable encryption feature and only use the MPSCS DES-OFB encryption key.



For talkgroups that are encrypted and everyone using them has encryption then they should be set as strapped. This gives the radio user the defined knowledge that the talkgroups will always be encrypted and not be set to clear by mistake.

Talkgroup Encryption Recommendations:

1. Do not encrypt talkgroups that are being used for interoperability.
2. Use strapped encryption on talkgroups that are always going to be encrypted to avoid accidental clear transmission.
3. Leave your dispatch/common shared talkgroups (P911, E911, F911, FE911, County COM1-83, and SPEV) free from encryption features for interoperability with your surrounding agencies. Other talkgroups can have encryption enabled to maintain secure communications.
4. If any agency/county/dispatch wishes to encrypt their P911s, or talkgroups corresponding to P911s whereby day-to-day law enforcement calls for service, etc. are transmitted/received, they use the standard MPSCS encryption key, whether it is ADP or DES.
5. If any agency/county/dispatch wishes to encrypt a P911 or other talkgroup, they should immediately notify MPSCS and local and surrounding stakeholders so plans can be made in advance to rewrite codeplugs to support the encryption, update Memorandums of Understanding (MOUs) if needed, purchase encryption boards if the radios are not capable of it, and determine pathways for unencrypted communications in the interim.
6. It is recommended that the MPSCS key be used for CKR1 which is used in the consoles during a multiselect usage.
7. It is recommended that the MPSCS key be used for the Private Call, Failsoft, and Dynamic Regrouping features in the radio programming.

MPSCS uses all three types of encryption algorithms, however both the ADP and DES-OFB algorithms are not P25 standard compliant. Because the lower security algorithms are still used in many radios across the State, it is recommended that all three different algorithms be loaded into a radio if using encryption to ensure interoperability with all other agencies.

Algorithm Type Recommendations:

1. Use the current P25 compliant algorithm (currently AES256) in your radios.
2. Use older, non P25 compliant algorithms, when communicating with other agencies using older standards. (Install all versions that are available to maintain interoperability including encryption security with other agencies.)

Multi key

Radios come with either a single key or multi key option in them.

- Single key allows only using a single key between multiple algorithms. This will limit interoperability between agencies.
- Multi key allows multiple encryption keys to be used in the radio.

Recommendations:

1. Purchase multi key option when using encryption in your radios.

Common Key Reference (CKR) Systemwide Reference Number

The CKR is used as a reference number between a keyloader and a radio when adding encryption to the radio. It is recommended that each agency have a unique CKR number to avoid confusion between different radios and agencies. An agency is not required to give their encryption key to the MPSCS Radio Programming Unit but it is required that they coordinate their encryption CKRs with them to avoid any confusion.

CKR Recommendations:

1. Work with the MPSCS to assign unique CKRs and to avoid duplicates.
2. Reference the CKR when requesting encryption for updates in the software.

Key ID (KID)

The key is a number that is specific to the encryption key and must be unique across the system or it can lead to conflict. Duplicate KIDs are not allowed in the software or keyloaders because of software limitations.

KID Recommendations:

1. Work with the MPSCS Radio Programming Unit to assign unique KIDs and to avoid duplicates.

Over the Air Rekeying (OTAR)

OTAR is the ability to rekey the radio over the system without the use of a keyloader. This provides the ability to issue a new key quickly and without the possibility of missing radios or having older keys that don't work. This should be used to eliminate the possibility of a lost or stolen key or if constant key updates are needed for secure communication.

OTAR Recommendations:

1. Use OTAR for constant key updates and to avoid the use of multiple keys per agency for key security.
2. Use one key that is changed on a regular basis instead of several keys that are never changed.

Key Sharing

To use or have access to another agency's talkgroup you must have a MOU stating that you can have it programmed in your radios. You must also obtain any encryption keys that are used for the talkgroup. The MPSCS does not share any DES-OFB or AES keys that are in possession of the State (State or Local keys) with another keyloader but they can be loaded into any radio or console that has encrypted talkgroups in them. MPSCS radio techs (through coordination with the MPSCS Radio Programming Unit) will load any State keys that are needed into a radio upon request to ensure secure communication in that radio.

The ADP software keys can be viewed in the software without a system key and can be shared in both radios and keyloaders.

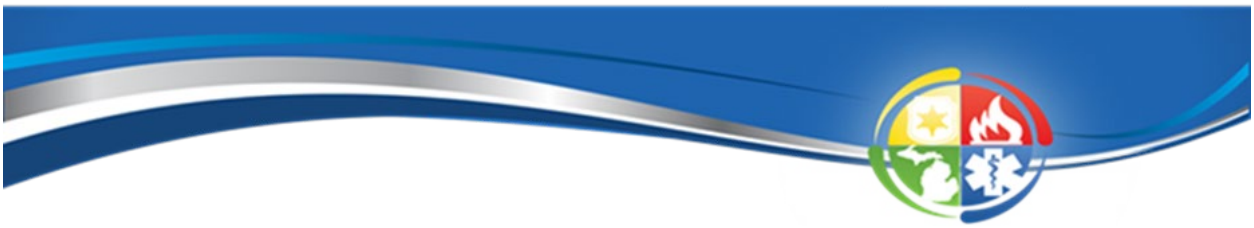
Reference the MPSCS policy that all radios being removed from the system have all keys erased before transferred to another agency or removed from the system.

Key Sharing Recommendations:

1. Load encryption keys in the radios of other agencies that are going to use your encrypted talkgroups so secure communications and interoperability can be maintained.
2. It is recommended that accurate records be kept by the authority having jurisdiction to maintain accountability and tracking of shared encryption keys, in coordination with radio inventory list.

Best Practices for Encryption Security

1. Keyloader security
    a. Password protection: keyloader must be password protected.
    b. Physical security: Must be stored in a secure location and maintaining a strict chain of custody.
    c. Accountability: Shared authorization of keyloader use and access from multiple consenting authorities.



   d. Sharing of keys between keyloaders: Keys should only be shared with a MOU agreement between authorized parties. Once that key is shared it cannot be recalled unless of a compromised security breech. Should be supervised by the owner of the key being shared.

2. Key rotation
   a. Use OTAR for key rotation in a large number of radios.
3. Compromised keys
   a. There should be timely notification when keys are compromised (within 24 hours).
   b. Develop a key replacement plan.
4. Compromised radios with loaded keys
   a. There should be timely notification when radios are lost or stolen (within 24 hours).
      i. Compromised radios can be used to monitor encrypted traffic.
   b. Radios removed form service, transferred or sold should have all keys erased.
      i. Keys must be erased manually or with keyloader separate from programming software.
5. Key documentation and security
   a. Document hard copy key strings and store in a secure location.
   b. Maintain a list of radios that have that key installed.