Integrated Public Safety Commission

Safety Acting for Everyone- Together (SAFE-T) Radio System

Encryption Programming Guidelines

Last Updated: December 5, 2023

Purpose:

Provide guidelines for participating public safety agencies regarding the programming, keyloading and use of encryption features on the 700/800 MHz SAFE-T radio system.

Background:

The Integrated Public Safety Commission (IPSC) has been statutorily charged with the responsibility of providing voice and data interoperable for public safety communications in Indiana. 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 IPSC P25 Trunked Radio System (SAFE-T) should be programmed with a basic radio interoperability template that includes statewide interoperable talkgroups as well as 700/800 MHz 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 and 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, the IPSC has adopted these policies and guidelines to help maintaining a *high leve*l of interoperability for mutual aid clear/open and encrypted/secured communications.

Types of Encryption Algorithms

- **AES256 (Advanced Encryption Standard**) High security (Federal Grade) encryption that can be loaded with keyloader or software (in some radios).
- **ADP (Advanced Digital Privacy)/ARC4 -** *Motorola proprietary algorithim.* Low security encryption. Usually loaded in template but can be loaded with keyloader.
- **Rivest Cipher 4 (RC4/ARC4)** - *Harris proprietary algorithim*. 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. <u>This algorithm is not recommended by NIST/CISA or IPSC.</u>

Encryption Activation Settings

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

- **Clear Strapped** 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.
- **Secure Strapped** is used when the talk-group is always encrypted and cannot be turned off.
- **Infinite Key Retention:** This is a feature in the radio template/programming. If selected the radio will retain the voice encryption keys if it is powered down. If unchecked the radio will lose all encryption keys if the radio is powered down. The radio may lose the ability to transmit on encrypted talkgroups on the system.
- **Storage Location Number (SLN):** The SLN is the identifier or alias for a designated location, or key slot, in the radio programming codeplug. The SLN is used to identify where a key is placed within a list of keys. Also known as Common Key Reference, or CKR.
- **Key Name:** The Key Name is the identifier or alias for the Key String.
- **Key ID:** The Key ID is a selectable, visible, portion of the key string. The key ID must be unique within the codeplug and most commonly matches the SLN that has been assigned.
- **Encryption String:** This is the actual voice encryption key which varies in length and complexity.

Encryption Feature Recommendations:

1. Use **secure strapped** when using talkgroups that are always going to be encrypted. (Examples: SWAT Teams, Drug Enforcement Team, Tactical, etc.).
2. For Zone 1 (North) and Zone 2 (South) Event talkgroups, IPSC recommends that the Event talkgroups are programmed and replicated two times (in two separate zones – one “clear strapped” and one “secure strapped”), as follows:
    - Clear strapped
    - Secure strapped using federal AES interop key SLN 12
3. **Infinite Key Retention:** IPSC recommends that it is checked in the programming to be selected to retain the keys.
4. **Encryption interoperability:** IPSC recommends that certain voice encryption keys be shared between agencies to allow interoperability across different talkgroups. National Law Enforcement Communications Center (NLECC) defines Storage Location Number 1 through 20 as interoperable keys. Some are defined as federal use only while others are accessible to State and Local agencies. A full list of available SLN’s can be obtained by contacting IPSC.

Talkgroup Encryption

Talkgroups may have different levels of encryption depending on how they are used. Statewide Interoperability Talkgroups (SW-CALL and SW-MA1 through SW-MA9 and Regional Mutual Aid talkgroups A-MA1 through O-MA4) should not use encryption to ensure interoperability.

IPSC also recommends not using encryption on talkgroups used for multiple agencies or if there is possibility of someone not having the encryption feature and/or the ability to use multiple encryption keys.

Examples of talkgroups that IPSC suggests not using encryption on include, but are not limited to:

- Main dispatch
- Common talkgroups
- Special event talkgroups
- Interop talkgroups

Encryption should not be used on these talkgroups without a statewide plan and consideration of all potential participants as well as their radio's encryption capabilities (ie: single key vs multikey).

If a talkgroup needs to be both encrypted or clear depending on how it is used and who has access to encryption, then it should be programmed into the radio twice, once as clear strapped and once as secure strapped.

For talkgroups that are encrypted, and all parties involved have the proper encryption key and radio hardware, talkgroups should be programmed as secure 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 (DISP, DSP, countywide, SW-MA and Regional MA) 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 Dispatch type talkgroups whereby day-to-day law enforcement calls for service, etc. are transmitted/received, they should:
    - Use the standard IPSC ADP encryption key.
    - Immediately notify IPSC and local and surrounding or supporting stakeholders. Plans can be made in advance to rewrite codeplugs to support the encryption, update Memorandums of Understanding (MOUs) if needed, purchase encryption options if the radios are not capable of it and determine pathways for unencrypted

communications in the interim.

5. It is recommended that the IPSC interop ADP key be used for SLN2026 which is used in the consoles during a multiselect usage.
6. It is recommended that the IPSC interop ADP key be used for the Failsoft, and Dynamic Regrouping features in the radio programming

Participating agencies use all three types of encryption algorithms, however both the ADP and DES-OFB algorithms are not P25 standard compliant. Furthermore, the DES-OFB algorithm has been sunset by NIST and CISA due to the encryption algorithm having been broken/cracked and not meeting the current FIPS 140-2 standard.

If you know a key has been compromised, or is using an unsupported algorithm, you should work to find an alternate method of communication that is secure.

Algorithm Type Recommendations:

1. Use the current P25 compliant algorithm (currently AES256) in your radios whenever possible.
2. Use ARC4 (ADP or compatible) when communicating with other agencies using older standards.
3. To maintain interoperability, ensure all proper encryption keys and algorithms are programmed into your radios.
4. IPSC does not support the use of DES-OFB for encryption (due to being unsupported by NIST/CISA due to security concerns)

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 and algorithms to be programmed in the radio, and is the **strongly recommended** configuration for all radios utilizing encryption on the SAFE-T system.

Storage Location Number (SLN) Systemwide Reference Number

The SLN 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 SLN number to avoid confusion between different radios and agencies. An agency is not required to give their encryption key to the IPSC, but it is required that they coordinate their encryption SLNs with them to enable the use of voice encryption while maintaining voice interoperability.

SLN Recommendations:

1. Work with IPSC to assign unique SLNs and to avoid duplicates.
2. Reference the SLN when requesting encryption for updates in the codeplug.

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. **The creation of the KID is the responsibility to administer by the participating agencies programmer or the radio shop.**

KID Recommendations:

1. Work with the IPSC to assist in creation of a unique KIDs and to avoid duplicates. The agency radio programming staff or vendor should contact IPSC Connections Center.
    - 317.234.1540
    - Icc@ipsc.in.gov

Over the Air Rekeying (OTAR)

OTAR is the ability to rekey the radio over the system without the use of a keyloader. The original radio keyloading must be completed with a key fill device or keyloader. The agency that wishes to use OTAR must provide IPSC the ability to key load the system with the encryption key from their key fill device. 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. To use OTAR, the agency must provide the encryption key via the key fill device to load into the system.
2. SLN's and KID's must be coordinated through IPSC to prevent duplication errors.
3. Use OTAR for constant key updates and to avoid the use of multiple keys per agency for key security.
4. 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.

IPSC will not share any 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. IPSC

radio techs (through coordination with the IPSC Field Services Unit) will load any State or National Interop keys that are needed into a radio upon request to ensure secure communication in that radio.

ADP software keys can be viewed in the software original codeplug without a system key and can be shared in both radios and keyloaders. Radios can't be read to reveal the ADP keys loaded through the programming software.

Reference the IPSC 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. Encryption keys should not be shared electronically, either by email or text message. Keys should be hand-written or read over the phone.
3. 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.

It is *vital* to coordinate encryption settings with IPSC and neighboring agencies to ensure seamless communication and interoperability.

Encryption is a critical component of the SAFE-T 700/800MHz public safety radio systems, ensuring the confidentiality, integrity, and security of sensitive communications.

By following these programming guidelines, public safety agencies can enhance their encryption strategies, maintain regulatory compliance, and effectively protect their communications during critical incidents. Balancing security measures with operational needs is key to ensuring the continued success of these vital systems.

REVISION HISTORY:

Date:	Responsible Party:	Change Summary:
December 12, 2023	Integrated Public Safety Commission (IPSC)	Initial Draft