Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

ISICS Standard: Encryption Key Storage Location Number and Key ID	**Standard #:**	2.12.5
	Date Adopted:	06/09/2022
	Date Reviewed:	
	Version:	

1. Purpose or Objective

To clarify the assignment and use of the storage location number (SLN) and key identification number (KID) in ISICS-connected radios. Proper assignment and use of the various SLNs and KIDs will ensure that encrypted traffic will be possible on the Iowa Statewide Interoperable Communications System (ISICS) along with preserving interoperable and other system capabilities among ISICS-connected subscriber units. Any reference in this standard to programming or encryption information is considered non-public information under Iowa Code 22.7(50) and is only eligible for disclosure specific individuals.

2. Technical Background

- **Capabilities**

  A traffic encryption key (TEK) is used to encode the radio transmission in a manner that prevents unauthorized radios from receiving or transmitting audio. Each TEK is stored within a hexadecimal KID that is associated with a decimal SLN. Some manufacturers may refer to a SLN as a common key reference (CKR).

  The ISICS core software has the ability to "strap" specified talkgroups as clear or encrypted. By strapping specific talkgroups as encrypted, it is also assigned a SLN/CKR[1].

  The use of encryption on the ISICS Platform allows for secure communication among public safety and public service personnel.

[1] Specific ASTRO system function definitions are available in the Motorola Secure Communications Feature Guide (MN004902A01-A) documentation.

- **Constraints**
  - Proper coordination of SLNs/CKRs and KIDs among ISICS users is necessary to ensure interoperability is not adversely affected. Each SLN/CKR can store two KIDs. Each SLN/CKR and KID combination is limited to one TEK. Subscriber equipment will not be able to decode transmissions if TEKs differ.
  - If a subscriber radio is not programmed properly for an encryption strapped talkgroup, it may display an error message upon affiliation or attempted transmission.
  - Under certain situations it may be necessary to patch encrypted talkgroups together. In this case, the system will resort to using a 'patch key' that is a unique SLN/CKR, KID and TEK grouping. This patch key needs to be in end user subscriber radios in order for the patch to be successful.
  - In addition, expectations of functionality need to be established among the ISICS System Administrator (SA) and Local Subsystem Administrators (LSAs) to define roles and establish processes for encryption key management. See ISICS Standard 2.12.3 –Encryption Key Security for additional information.

3. Operational Context

Agencies that have investigated encrypted radio traffic should take every reasonable measure to define their operational adversaries for each aspect of their operational picture before utilizing encrypted talkgroups.

In some cases, verification of correct radio programming and encryption provisioning in subscriber units may be necessary to ensure secure interoperable communications are possible. If this is not done, in-field personnel may need to resort to use of an unencrypted, in the clear, talkgroup.

Regional and statewide interoperable talkgroups shall use SLNs/CKRs and KIDs assigned to the ISICSB by the National Law Enforcement Communications Center. In the event of a conflict with local agency KIDs, a substitute KID shall be issued by the ISICS SA.

ISICSB Policy 2015-05 endorses the use of Project 25 (P25) Encryption Standards based security solution using NIST FIPS-197 compliant Advanced Encryption Standard (AES 256-bit) for secure communications and recommends reserving SLN 1 through 20 for nationwide interoperable key management.

The ISICSB recommends that agencies that wish to utilize encryption purchase multi-key AES256 equipped radios. Multi-key will allow agencies to utilize the ISICS interoperable encryption keys and locally managed encryption keys.

4. Recommended Protocol/Standard

The ISICS SA and LSAs are responsible for coordinating the use of SLNs and KIDs across the ISICS Platform. Certain SLNs and KIDs are reserved for the regional and statewide interoperable talkgroups and have been registered with the National Law Enforcement

Communications Center. In addition, one grouping of SLN/CKR, KID and TEK has been pre-allocated as a patch key.

Each county in Iowa has been pre-allocated a set of SLNs/CKRs and KIDs for their local use. The SLNs/CKRs are decimal. KIDs are in hexadecimal. If LSAs wish to utilize any over-the-air rekeying (OTAR) capability, they must also configure the subscriber radios for that functionality in accordance with ISICS standards.

Once SLNs/CKRs are selected by LSAs, they shall send that information to the ISICS SA for entry into the master records.

The ISICS SA is responsible for coordinating with LSAs to ensure they have the SLNs/CKRs and KIDs associated with any interoperable talkgroups on ISICS.

5. Recommended Procedure

Upon receiving the local range of available SLNs/CKRs and KIDs, the LSAs should inform the ISICS SA of which will be used for record keeping.

LSAs should also coordinate with each other if encryption key material will be shared among agencies. It is recommended that any LSAs that share encryption keys with other LSAs, that agreement should be transmitted to the ISICS SA for record-keeping. This will also help ensure that anyone transmitting on an encrypted local talkgroup is authorized to have the TEK.

The ISICS SA should coordinate with LSAs to ensure that the master list of SLNs/CKRs and KIDs is current. If LSAs make changes to local talkgroups, they should notify the ISICS SA of the change within ten (10) business days.

LSAs shall reserve SLN/CKR 2000 and KID 2000 for an ISICS system encryption patch key. The ISICS SA shall provide this key to LSAs.

LSAs shall reserve SLN/CKR 786 for all regional and statewide encrypted interoperable public safety tactical (TAC) talkgroups. LSAs shall reserve SLN/CKR 787 for regional and statewide encrypted interoperable law enforcement TAC talkgroups. There are several associated KIDs for the regional and statewide interoperable public safety and law enforcement. Even if those KIDs are not actively being used, they shall not be used in templates.

The master list of SLN/CKR and KID combinations is considered non-public information under Iowa Code 22.7(50) and is only eligible for disclosure to LSAs and trusted technicians.

In order to save time and money, it is recommended that subscriber radios be provisioned with the proper encryption material upon initial programming. This will help mitigate potential down time.

6. Management

The ISICS SA and LSAs will be responsible for ensuring that all necessary coordination of SLN/CKRs and KIDs is conducted. The ISICS SA is responsible for maintaining a master list of the SLN/CKRs in use. The ISICS SA and LSAs shall also coordinate with the Operations and Technology Committees to ensure this standard is reviewed for accuracy, efficacy and completeness as necessary.