Statewide Interoperability Radio Network (SIRN)
Standards, Protocols, Procedures

Document Section	**Management of the System**	SIEC Sub Committee Date: 6/28/2021
State Standard Number	**2.3.0**	
Standard Title	SIRN Encryption Key Standard	
Date Established	**09/28/2020**	**SIEC Approval**: 6/28/2021
Replaces Document Dated	**NA**	
Date Revised/Reviewed	**05/15/21**	

1. Purpose or Objective

This policy establishes standards for generating, storing, securing, and managing SIRN encryption keys.

2. Technical Background

- **Capabilities**

SIRN uses the APCO-sanctioned AES-256 encryption standard to secure voice transmissions from being intercepted over the air. Certain talkgroups, typically law enforcement or other sensitive communications, will be encrypted. To ensure end-to-end encryption, encryption keys have to be maintained securely and accurately across all applicable devices, including subscriber devices, consoles, voice logging recorders, key management facilities and key fill devices.

- **Definitions**

Traffic Encryption Key (TEK): Unique variable length hexadecimal key used to encrypt and decrypt voice and data traffic.

Key ID (KID): Provides a unique address to identify a TEK and is expressed as a hexadecimal value between 0000 and FFFF. The KID, along with an algorithm identification value, is part of the system P25 data transmission. The radio uses the KID to understand which key to use to decrypt information received.

Unique Key Encryption Key (UKEK): A unique KEK that is common to only an individual subscriber unit (SU) or Key Fill Device (KFD) and the Key Management Facility (KMF) and is used to create a secure link during initialization with an individual unit within the KMF's management.

Storage Location Number (SLN): A common method to refer to an encryption key slot in a subscriber unit. In an OTAR system, each SLN contains two TEK keysets (one active/one inactive). This is a decimal value between 0 and 4095. The SLN is used mostly for subscriber programming. CKR or Common Key Reference in Motorola parlance.

Key Fill Device (KFD): Electronic device used to load keys into subscriber devices.

Key Management Facility (KMF): Network-based server used to manage key and key interoperability across system devices and manage overall encryption distribution workflow.

Over-the-Air-Rekeying (OTAR): Over the air rekeying service.

End Devices: Subscriber hardware or software into which a key may be loaded. Examples includes radios, dispatch consoles, and logging recorders, etc.

- **Constraints**

Proper storage, distribution and management of encryption keys is essential for system security and to ensure interoperable communications across encrypted talkgroups. Additionally, for user equipment to decrypt audio transmissions, the Key ID, CKR and TEK have to match. No two encryption keys (TEKs) should use the same CKR.

3. Operational Context

Encryption enables secure over the air transmission of sensitive communications. A coordinated approach for managing and distributing encryption keys is vital to support seamless communications across encrypted devices.

Uncoordinated use of encryption keys will lead to communications lapses between devices configured with different encryption information.

4. Recommended Protocol/ Standard

General Standards

The State of North Dakota's encryption key plan is designed to

- Be compliant with federal and state regulations
- Avoid key conflicts and duplication at the state and local levels

Crypto Period

Crypto-period or key renewal will occur once every six (6) months or as determined by the SIEC. Crypto-period may be reduced for cause in the event that keys in active circulation have been compromised.

Both active and inactive TEK keysets will be refreshed upon key renewals.

Common Key Resource (CKR)/Storage Location Numbers (SLN)

SIRN Encryption Keys will be generated and assigned per the SLN/KID range tabulated below.

In addition, it is anticipated that all standard law enforcement personnel communications at the State and local levels will share the same encryption key (TEK) with matching CKRs. Special purpose talkgroups such as forensics and investigations may use unique keys (TEKs) per the plan below.

	SLN	SLN Name	KID	Description
1	1101	LE STANDARD SEC	44D	All LE Standard - State and Local
2	1102	HP SP OPS	44E	HP Special Ops
3	1103	LE SP OPS	44F	Other State or Local LE
4	1104	NW LE SP OPS	450	Special Ops Regional, if necessary
5	1105	NE LE SP OPS	451	Special Ops Regional, if necessary
6	1106	SE LE SP OPS	452	Special Ops Regional, if necessary
7	1107	SW LE SP OPS	453	Special Ops Regional, if necessary
8	1108	TBD	454	TBD
9	1109	BCI Internal	455	BCI Internal
10	1110	MA SEC	456	ND MA and ND Regional
11	1111	FIRE SEC	457	Fire Agencies
12	1112	EMS SEC	458	EMS Agencies
13	1113	ALL OTHER SEC	459	Other public safety or public service
15	1115	TBD	45B	TBD
20	1120	*Patch Key*	460	*PATCH KEY*

5. Recommended Procedure

All law enforcement devices MUST initially be loaded with the approved plan (CKR, KIDs, UKEKs) to facilitate future over the rekeying/updates.

Key Management Facility

All SIRN key material will be managed solely by the Key Management Facility. Only the SIRN Statewide System Administrator or designee shall have access to the SIRN KMF**.**

Key Generation and Storage

All encryption keys for use on SIRN will be generated by and stored in the KMF.

SIRN TEK(s) may NOT be

- generated or stored in intermediate devices such as Key Fill Devices
- stored, emailed or transmitted electronically in plain text
- stored in plain text or in devices that can display the keys in plain text

Keying or Rekeying End User Devices

All keying and rekeying of end user devices (radios, consoles, logging recorders, etc.) will be conducted only via the KMF using:

- OTAR for radios or,
- wired over-the-ethernet-keying (OTEK) for consoles and wired devices

Devices must NOT be keyed or rekeyed by a Key Fill Device (KFD).

Over-the-Air Rekeying
Only the Statewide System Administrator or designee has access to the SIRN OTAR capabilities. Requests for rekeying radios via OTAR shall be made in writing to the Statewide System Administrator.

Key Distribution
SIRN Encryption Keys will be distributed or loaded through the KMF to devices previously authenticated by the KMF. Keys cannot be manually entered.

Key Fill Devices
KFDs shall NOT be

- used to generate or store TEKs
- used to rekey devices.

Key Fill Devices shall only be used to load UKEKs into radios. UKEKs enable end user devices to authenticate with the KMF for over the air rekeying.

Key Fill Device(s) (KFDs) must be

- protected by a strong password (with at least 8 characters)
- be stored in a secure location

The Statewide System Administrator shall maintain historical records of all individuals that possess key fill devices, including names, KFD serial number and identifier. When a UKEK is filled into a KFD, the date of transfer and description of device will be reported to the SIRN Statewide System Administrator.

Lost, misplaced, or stolen KFDs must be reported immediately to the SIRN Statewide System Administrator.

Exceptions
Exceptions to rekey radios directly via a KFD (and with locally generated TEKs, i.e., off the KMF) may be granted on a case-by-case basis by the Statewide Administrator or SIEC. Under these limited exceptions, Local Administrators may generate keys (TEKs) and rekey their agency's devices via KFD. Such activity will be prohibited on primary dispatch and shared talkgroups where key conflict can cause interoperability issues.

All radios keyed in this manner must be reported to and will be logged by the Statewide System Administrator.

<u>6. .Management</u>

The SIRN Statewide System Administrator is responsible for managing the State's encryption keys, the

KMF and oversee State and local administrator-owned KFDs.