


Introduction

**UNDERSTANDING  
ENCRYPTION**

LAND MOBILE RADIO SYSTEMS  
“THE BASICS”

Any use of a manufacturer's name in this presentation does not constitute an endorsement.

 **CISA**  
CYBER-INFRASTRUCTURE

2019

1

Welcome to the encryption webinar. The basics of encryption. Is everyone seeing the screen and hearing the audio well. Please keep phone microphones muted and not on hold. Mention that attendees can raise their hand with the controls, type a question or simply speak up. Thank (Person or State) for the opportunity to present the material. It's only going to be the tip of the iceberg. We may arrange some visits to the state , send out a survey, work with your governance committee ,communications vendors etc.

## Introduction

Cybersecurity and Infrastructure Security Agency (CISA)  
Emergency Communications Division (ECD)

Dave Dato

[ddato@lafayettegroup.com](mailto:ddato@lafayettegroup.com)

847-217-2000

Please familiarize yourself with the exits and areas of refuge in  
your current environment



2

BIO INFO

## Introduction

We have four main areas to discuss today, so that you gain an understanding of encryption basics and understand the overall framework that is necessary for a successful encryption program.



3

Again this is only the tip of the iceberg . You do not have an insurmountable issue but it will take some time to develop a good workable framework. I understand that most state interoperability committees do not have any regulatory authority but cooperation and coordination goes a long way. Encryption is not just about operability but also interoperability.

What if the police sergeants monitored the fire dispatch or tactical channels regularly for situational awareness or the FD monitored the police frequencies for the same reason and one or the other or for that matter both agencies encrypted and didn't develop a plan? What happens to that situational awareness and the efficiencies and effectiveness of working together? It's something we need to think about and work on. It will take cooperation and trust. Ponder that as I move through the presentation as sometimes the technical issues are easier to fix than the institutional issues. Let's look at the four areas that we want to touch on today.

## Topic Sections

- Best practices
- The technical basics of encryption
- Tools and hardware
- The path forward (open discussion )



4

Best practices .... What others have done that works and the big picture for what you need to do to successfully implement encryption in Idaho.

Basics of Encryption.... I will try not to make your heads spin and your eyes gloss over. But we do have some technical concepts to discuss so that everyone has a general understanding when we get into the actual discussions.

Tools and hardware.... A brief explanation of some of the tools used to use encryption and some of the radio equipment that must be taken into consideration when implementing encryption.

The path forward .... An open discussion about a number of topics that will help move the project forward.

## The Decision to Encrypt Has Been Made By Some Agencies

We will not be discussing the merits of the decision to encrypt or not to encrypt.

What we will be discussing is the ability to maintain communications operability and interoperability with the implementation of encryption.

Much discussion internal and external to the agencies involved with the decision to encrypts starts to develop. Be prepared Press, scanner enthusiasts' other agencies etc.....  
 The decision to encrypt has already been made by some agencies I view our task as how to now maintain operability and interoperability within that implementation environment.

## Encryption Best Practices

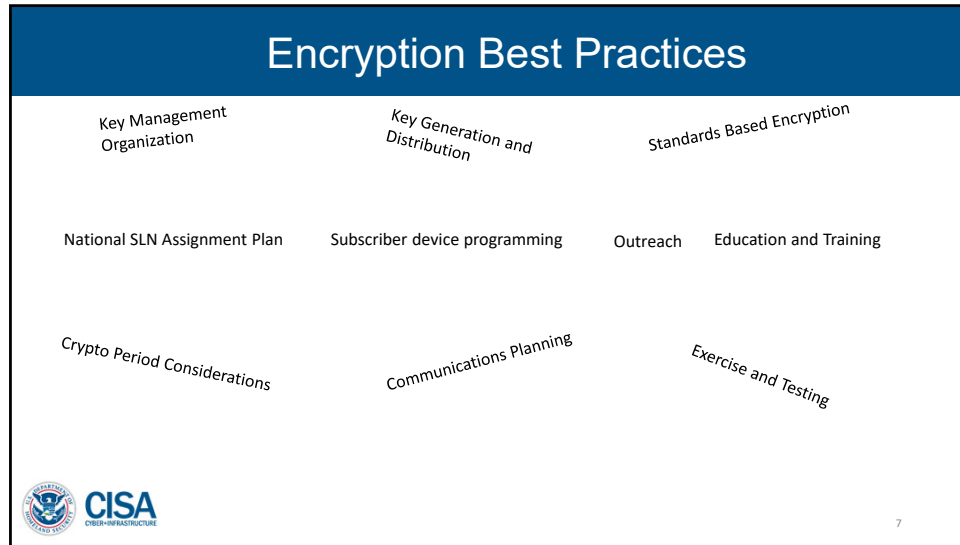
Public safety can and has achieved encrypted interoperability at the local, regional, state, and national level by collaborating with the other agencies, users and encryption specialists.

Effective planning, cooperation, governance, and a basic understanding of how key parameters are coordinated can lead to successful encryption program.



6

As a reminder....



We'll briefly touch on a handful of concepts in no particular order.....

## Encryption Best Practices

### Education and Training

Develop training for system operations ,  
dispatch and field personnel to improve  
effectiveness in the use of encryption.



8

Implementing encryption or any program for that fact without education and training is headed for failure. The users should understand what is going on in the background. It is no longer acceptable to just turn on the radio and not understand the tool you are using or the infrastructure you are using it on.



## Encryption Best Practices

### Communications Planning

Develop Communications system plans and purchases that incorporate encryption considerations. **Transitional cost-effectiveness is a must.**



9

System specifications should include consideration for the use of encryption. There is a saying that I like and it goes something like this....The cost is inversely proportional to the amount of time spent planning . In other words implementation is going to cost you more if you don't consider all of your options up front.

## Encryption Best Practices

### Standards Based encryption

Utilize the P25 Advanced Encryption Standard (AES)-256. It is the algorithm identified not only in the P25 standard but also in grant requirements where encryption is specified as part of a grant funded purchase.



10

It's all about using something that someone else can interface with. The implementation of proprietary equipment or operations causes problems with operability and interoperability in the long run.

We all like grant money (when it's available) make sure you optimize your chances to get it by using standards-based specifications.

If a manufacturer includes a non-P25 standard encryption in a radio they must also include AES256. This rule came from the P25 Compliance program published in early 2017. It aimed to stop manufacturers from providing subscriber units with a non-P25 standard encryption, without also including P25 standard Advanced Encryption Standard (AES) 256 encryption.

## Encryption Best Practices

### National SLN assignment plan

Adopt a standardized Storage Location Number (SLN) and key ID (KID) plan to minimize operational conflicts.

\*The National Law Enforcement Communications Center (NLECC) has some options available.



11

Ah Ha .... The technical terms are starting to sneak in.. SLN , KID NLECC.... We'll take some more about these terms and The National Law Enforcement Communications Center shortly...

## Encryption Best Practices

### Subscriber device programming

Be sure that subscriber device programming personnel (Radio shops) understand not only the technical aspects of encryption use, but also the operational requirements of the public safety users.



12

Programmers need to understand what you want to accomplish operationally. If they have an understanding of what you want to do they can make programming changes to adapt to those needs. i.e. an officer is assigned to a task force which shares a channel between officers. Not all officers have the encryption. The programmer can make the radio so that the officer can turn encryption for that particular channel on and off. (Not a good practice but doable). A better example is for the technicians to know what agencies need to work together and coordinate the encryption parameters.

## Encryption Best Practices

### Crypto periods

Develop reasonable policies and plans as they relate to when and how to change encryption keys.



13

How long do you keep keys in radios and why would you change them....Lost or stolen radios ?

## Encryption Best Practices

### Exercise and testing

Exercise and testing are essential to successful operations.



14

Earlier I touched on education and training similarly... exercise and testing are essential to maintaining assurances that people and the system can both function when needed.

## Encryption Best Practices

### Key management organization

A recordkeeping plan and an organization (clearinghouse) are essential to prevent operational conflicts with encryption schemes. When and where possible keep all frequency bands and systems under the same encryption plan.



15

An agency or agencies need to coordinate this activity. It is possibly the most essential function for encryption implementation and ongoing maintenance.

## Encryption Best Practices

### Key generation and distribution

Determine who (what agencies) will be responsible for generating keys and how they will be distributed.



16

What agency is going to accept responsibility to coordinate a very important activity? More discussion to follow on how that activity is going to get done.



## Encryption Best Practices

### Outreach

Collaborate to ensure effective encryption implementation.



17

Coordinate and **make sure all agencies know what is taking place in the state**. The coordination will help prevent missteps along the way. When an agency “doesn’t know” unknowing actions are taken and mistakes happen.



Does anyone have any questions at this point? Ok we are going to get into the technical basics of encryption. As mentioned earlier I will try not to make your head spin or your eyes gloss over. If I do stop me in my tracks and I will try to clarify the point. Don't hesitate to ask for clarification along the way.

## Technical Basics

### Know the Rules

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

FCC R&O PS DOCKETS No. 13-209 and 15-199 Revising section 90.20(i).  
Information from Scott Wright presentation State of Connecticut



19

Some agencies have inadvertently used some of the channels in an encrypted mode not knowing the law as outlined in the Federal Communications Commission Regulations. There are channels / Frequencies that you can use as will be highlighted in the next slide.

# Technical Basics

## Know the Rules

The FCC Order does not apply to certain channels / frequencies, where encryption may be used:

- 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

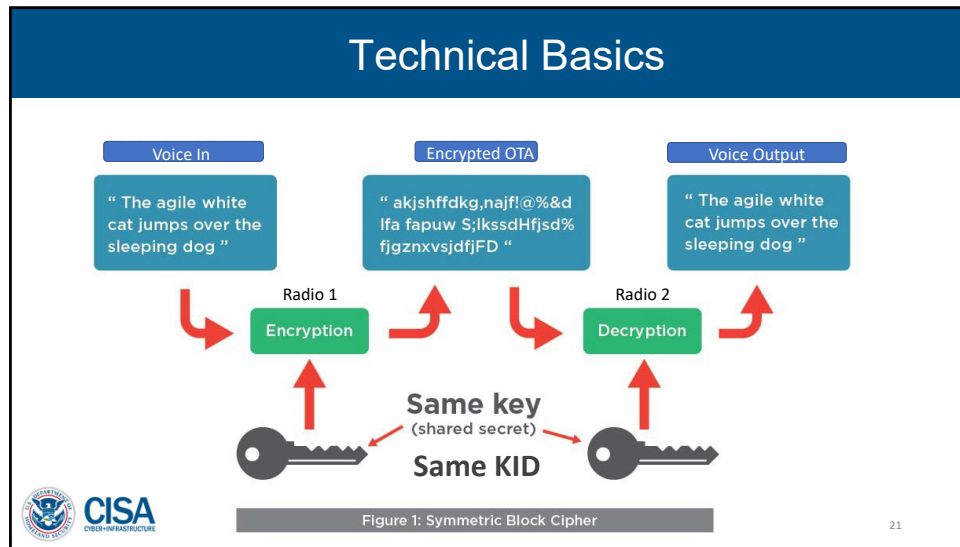
Keep in mind that on the interop frequencies where encryption is permissible by FCC rule, radios employing encryption must have a readily accessible switch or other readily accessible control that permits the radio user to disable encryption. FCC 47 CFR 90.553



Information from Scott Wright presentation State of Connecticut

20

Keep these frequencies / channels in mind as planning options. I have an example of what has been doing in another state coming up. Changing a channel to disable encryption is ok. (strapped and un-strapped ) discussion.



Very basic diagram of what the process is when you encrypt. Encryption is often confused with digital operation. Scanners can still listen to most digital operations. Scanners cannot decrypt encrypted operations. Inversion scrambling is not encryption, Advanced Digital Privacy (ADP) is not standard encryption, Next Generation Digital Narrowband (NXDN) 15 bit encryption is not P25 standard encryption. Don't get sucked into non-standard "non-P25" encryption AES 256 is the standard anything else may be inexpensive up front but cost you in the long run financially and from an operability and interoperability standpoint.

## Technical Basics



radio display with AES encryption shown as present on the display



22

How a channel or talkgroup display looks with encryption active

## Technical Basics

### Often talked about Algorithm (key) types

ADP/ ARC4- also known as Advanced Digital Privacy (software encryption)  
40 bit key) 10 characters  
(Proprietary encryption)

DES- Digital Encryption Standard (DES, DES-XL, DES-OFB 64 bit) 16  
characters (Old and in general use before AES 256 was developed.)

AES- Advanced Encryption Standard ( 128 and \*256 bits) 32 /64  
characters



23

Using standard and not proprietary encryption is important in order to maintain operability and interoperability.

## Technical Basics

### Key Security

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	$4.2 \times 10^9$
56-bit (DES)	$7.2 \times 10^{16}$
64-bit	$1.8 \times 10^{19}$
128-bit (AES)	$3.4 \times 10^{38}$
192-bit (AES)	$6.2 \times 10^{57}$
256-bit (AES)	$1.1 \times 10^{77}$

AES 256 has  
115,792,089,237,316,195,423,570,985,008,687,907,853,2  
69,984,665,640,564,039,457,584,007,913,129,639,936  
possible combinations. (78 digits)



24

An AES 256 code would take half the time the universe has been in existence to brute force crack with the most powerful super computers.

Originally only one manufacturer provided ADP now a couple have it. Also known as ARC4



## Technical Basics

Time needed to crack AES encryption with today's fastest supercomputer

Key Size	Time to Crack
56-bit	399 seconds
128-bit	$1.02 \times 10^{18}$ years
192-bit	$1.872 \times 10^{37}$ years
256-bit	$3.31 \times 10^{56}$ years



25

An AES 256 code would take half the time the universe has been in existence to brute force crack with the most powerful super computers.

Originally only one manufacturer provided ADP now a couple have it. Also known as ARC4

## Technical Basics

### Encryption Terminology

- **STORAGE LOCATION NUMBER (SLN)**—This is a decimal value between 0 and 4095. It is a common term to refer to an encryption key slot in a subscriber device. (It is also sometimes referred to as the Common Key Reference / CKR).
- The Storage Location Number (SLN) is a location reference and “place” in a radio that the radio program logic uses to reference what key to send when the radio transmits.



26

The storage location number is important . It indicates what encryption key the radio needs to send on a particular channel or talkgroup. Your state Coordination needs to start here. A *radio can only hold 1 SLN of the same value*. A *keyloader can only hold one SLN of the same value*.

## Technical Basics

### Screenshot of subscriber device (radio) software programming screen

Key Name	CKR #	Indexed	Slot A	Slot B	Selectable ADP Key	Selectable ADP Key
CKR 1	1	<input type="checkbox"/>	0	0	*****	0000
CKR1400	1400	<input type="checkbox"/>	1	1	*****	0000
SIEC1401	1401	<input type="checkbox"/>	2	2	*****	0000
LAW1402	1402	<input type="checkbox"/>	3	3	*****	0000
FIR1403	1403	<input type="checkbox"/>	4	4	*****	0000
EMA1404	1404	<input type="checkbox"/>	5	5	*****	0000
DOT1405	1405	<input type="checkbox"/>	6	6	*****	0000



27

The same SLN / CKR can be assigned to multiple channels or talkgroups in the same radio. In other words the same key can be used for different channels and / or talkgroups.

## Technical Basics

Screenshot of subscriber device (radio) personality programming screen



The screenshot shows a software interface for configuring a radio personality. At the top, there is a 'Talkgroup' dropdown menu set to 'Default' and a '1' in a text box. Below this is a table with the following columns: Talkgroup Name, Talkgroup ID, Priority Talkgroup, Secure / Clear Strap, Key Select, Talkgroup Failsift, and Failsift Rx Frequen. The table contains three rows: SECLAW 1, SECLAW 2, and Talkgroup 3. The 'Key Select' column for SECLAW 1 and SECLAW 2 is 'LAW1402', while for Talkgroup 3 it is 'CKR 1'. The 'Failsift Rx Frequen' column for all rows is '851.01250'. There are checkboxes in the 'Talkgroup Failsift' column, which are checked for SECLAW 1 and SECLAW 2, and unchecked for Talkgroup 3. At the bottom left of the screenshot, there is a 'Call / Page' dropdown menu.

Talkgroup Name	Talkgroup ID	Priority Talkgroup	Secure / Clear Strap	Key Select	Talkgroup Failsift	Failsift Rx Frequen
SECLAW 1	5969 - 1751	<None>	Secure	LAW1402	<input checked="" type="checkbox"/>	851.01250
SECLAW 2	5970 - 1752	<None>	Secure	LAW1402	<input checked="" type="checkbox"/>	851.01250
Talkgroup 3	1 - 1	<None>	Clear	CKR 1	<input type="checkbox"/>	851.01250



28

The same SLN / CKR can be assigned to multiple channels or talkgroups in the same radio. In other words the same key can be used for different channels and / or talkgroups.

## Technical Basics

### Encryption Terminology

**KEY ID (KID)** Provides a unique address to identify a Traffic Encryption Key (TEK). This is expressed as a hexadecimal value between 0000 and ffff (65,535 combinations).

The KID, along with an algorithm identification value are sent as part of the P25 data stream. It is from this information that the receiving radio understands what key to use to decrypt information (audio) sent.

The KID is EXTREMELY important! This is more important than the SLN!

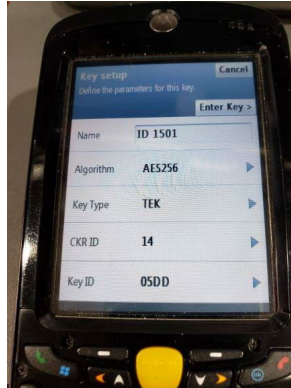


29

KIDs and TEKs have to match from radio to radio and agency to agency or the encryption will not work. Explain that sometimes the key is not strapped any key in the radio might be able to be used on any channel / talkgroup.

## Technical Basics

CKR / SLN entered in Key Variable Loader KVL along with KID (Hex format) . Sixty Four characters are entered or auto-generated for TEK



Motorola KVL 4000  
KVL stands for Key Variable loader.  
The generic term is Key Fill Device (KFD).

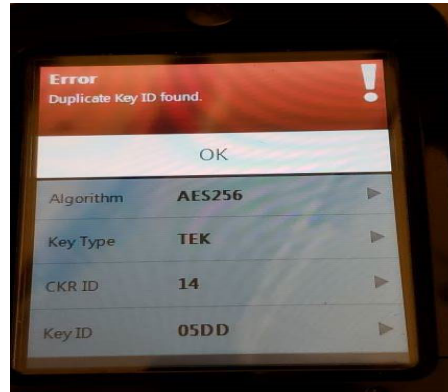


30

Lets put some of these terms into action by looking at what gets entered into a key fill device. Explain what is being looked at.

## Technical Basics

### No Duplicates Allowed



31

I already had a key 05DD (Hex) 1501 decimal therefore I got a warning. If there are multiple # 1 CKRs or KIDs there need to be multiple keyloaders, and multiple systems to operate on. It is simply a bad idea to duplicate any of the parameters. A system needs to be developed to create a fair and reasonable migration to a coordinated system of encryption.

Let's look at some examples in the next couple of slides of combination of parameters that work and those that won't.

## Technical Basics

### Encryption Terminology

#### *Unique Key Encryption Key (UKEK) and KMMs*

A key assigned to a re-keyable unit for encrypting keys within an individually delivered OTAR command. For OTAR, the UKEK is used to inner-layer encrypt the Key Management Messages (KMMs.)

The KMF uses Key Management Messages (KMMs) to communicate encrypted information to radios, infrastructure, and data devices.



32

Was called shadow key in Advanced Securenet Operations (ASN) .Used for encrypted transfer of data from KMF to KVL through dial-up . It is also used to load keys through a remote head into a radio. This encrypted information may include the following information for

the Subscriber Units: Keys, Key IDs, and associated CKR associations (TEKs, CKEKs, and UKEKs), Keysets, Keyset IDs, Keyset Names, and active states, Radio Set Identifiers (RSIs) (Individual and Group)



## Technical Basics

### Encryption Terminology

**Radio Set Identifier (RSI)** Is loaded into the KVL by the KMF operator, and Is then loaded into the radio from the KVL.

The KMF requires a Radio Set Identifier (RSI) in order to operate in the OTAR system. The KVL only accepts keys and KMMs from the KMF with this RSI.



33

Used for transfer of data from KMF to KVL usually through dial-up . It is also used to load keys through a remote head into a radio along with an RSI. A radio record must be defined for each radio that uses secure voice and OTAR services. The radio record identifies the Radio Set Identifier (RSI), Unique Key Encryption Key (UKEK), and transport systems on which the radio operates.

## Technical Basics

Theoretically, different agencies could have different SNL's refer to the same Traffic encryption keys, but it is not a good practice.

AGENCY	SLN	KID	HEX	DEC	TRAFFIC ENCRYPTION KEY
Agency A	0001	KID: 12AF	4783		TEK:1234567890ABCDEF
Agency B	1234	KID: 12AF	4783		TEK:1234567890ABCDEF
Agency C	4095	KID: 12AF	4783		TEK:1234567890ABCDEF

The SLNs and Key IDs in the table refer to the same traffic encryption key (TEK)

The radios should decode the radio traffic because the key IDs and traffic encryption keys are the same.

This scheme will work but it is not an ideal situation.



34

The example shown works despite the fact it has various CKRs / SLNs because the KIDs and actual TEKs are identical. Each agency is sending the same encryption information.

The front door keys are kept in different pockets by each agency .

They are all Schlage keys for a certain type of Schlage lock.

Each of the same keys are cut exactly the same.

Even though each agency keeps the key in a different pocket each agency can still go to each of the other agencies and open the lock on the front door.

## Technical Basics

Different agencies with uncoordinated CKR/KID/TEK assignments can create an interoperability nightmare....

AGENCY	SLN	KID HEX and DECIMAL	TRAFFIC ENCRYPTION KEY
Agency A	0001	KID: 12AF / 4783	TEK:8234567890ABCDEF
Agency B	0001	KID: 12AF / 4783	TEK:1294911402AC5767
Agency C	0001	KID: 12AF / 4783	TEK:3456777890ABDDE4

SLNs are all the same and KIDs are the same... HOWEVER THEY ALL REFER TO DIFFERENT TRAFFIC KEYS!!!



35

Every parameter here is the same with the exception of the traffic encryption key (TEK) Not only will it not work it may cause some issues because with the same KIDs the radio thinks it's receiving a correct TEK.

## Technical Basics

- When possible, keep all frequency bands and systems under the same encryption plan.



36

Even if none agreed upfront today to share keys / encryption an organized plan will be in place for the future. In the next slide lets look at a resource that can help with key organization and generation.

## National Law Enforcement Communications Center

### National Law Enforcement Communications Center (NLECC)

- NLECC is a Department of Homeland Security / Customs and Border Protection facility whose primary mission is to manage all aspects of DHS/CBP land mobile communications.
- NLECC will generate and assign Keysets (KID, Key, ALGID) for agencies at all levels of government . The process generally assures the parameters are unique and will not conflict with other systems that also use NLECC services.



37

DHS ECD ICTAP can help initiate the discussions and actions necessary between Idaho and NLECC. The NLECC is a Department of Homeland Security/Customs and Border Protection facility whose primary mission is to manage all aspects of DHS/CBP land mobile communications but has gained expertise in providing key management services to many other agencies at all levels of government. The use of the NLECC to generate and assign Keysets (KID, Key, ALGID) for agencies at all levels of government assures that these parameters are unique and will not conflict with other systems that also use NLECC services. Using a national coordination entity helps to ensure a more uniform approach to key management..

Located in Orlando FL.

# National Interoperability Keys

National Interoperability Keys

SLN	KID	Algorithm	Use	SLN Name	Crypto Period Annual Changes are completed on 1 <sup>st</sup> working Monday of October
1		DES	Public Safety Interoperable	ALL IO D	Annual
2	052C	DES	Federal Interoperable	FED IO D	Annual
3	460F	AES	Public Safety Interoperable	ALL IO A	Annual
4		AES	Federal Interoperable	FED IO A	Annual
5	06BA	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6	4319	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static
7		AES	US-Canadian FED Law Enforcement Interoperability	FED CAN	Static
8		AES	US-Canadian PS Interoperability	USCAN PS	Static
9		DES	National Tactical Event	NTAC D	Single Event Use-Not to exceed 30 Days
10		AES	National Tactical Event	NTAC A	Single Event Use-Not to exceed 30 Days
11	340	DES	Multiple Public Safety Disciplines	PS IO D	Static
12	377C	AES	Multiple Public Safety Disciplines	PS IO A	Static
13	031D	DES	National Fire / EMS/ Rescue	NFER D	Static
14	370E	AES	National Fire / EMS/ Rescue	NFER A	Static
15		DES	National Task Force Operations	FED TF D	One time use as needed for special ops
16		AES	National Task Force Operations	FED TF A	One time use as needed for special ops
17		DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for special ops
18		AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for special ops
19		AES	Federal-International Law Enforcement Interoperability	FED INTL	When needed by operational requirement
20		AES	Federal-International Law Enforcement Interoperability	PS INTL	When needed by operational requirement



This is a sample of the current National interoperability plan available for use by local, state federal and tribal agencies that is coordinated by the NLECC. Highly recommend use of the interoperability keys

# State Talkgroups and Keys Example

Zone Secure BZ

SECURE BZ	TG ID	CKR/SLN	KEY ID Name	KEY ID HEX	Authorized Entities
SECURE 1	5961	1401	SIEC1401	579	All Disciplines
SECURE 2	5962	1401	SIEC1401	579	All Disciplines
SECURE 3	5963	1401	SIEC1401	579	All Disciplines
SECURE 4	5964	1401	SIEC1401	579	All Disciplines EXCEPT PSCC
SECURE 5	5965	1401	SIEC1401	579	All Disciplines EXCEPT PSCC
SECURE 6	5966	1401	SIEC1401	579	All Disciplines EXCEPT PSCC
SECURE 7	5967	1401	SIEC1401	579	All Disciplines EXCEPT PSCC
SECURE 8	5968	1401	SIEC1401	579	All Disciplines EXCEPT PSCC
SECLAW 1	5969	1402	LAW1402	57A	Law Enforcement Agencies Only
SECLAW 2	5970	1402	LAW1402	57A	Law Enforcement Agencies Only
SECFIR 1	5971	1403	FIRE1403	57B	Fire Department Agencies Only
SECFIR 2	5972	1403	FIRE1403	57B	Fire Department Agencies Only
SECEMA 1	5973	1404	EMA1404	57C	All Disciplines EXCEPT PSCC
SECEMA 2	5974	1404	EMA1404	57C	All Disciplines EXCEPT PSCC
SEC DOT 1	5975	1405	DOT1405	57D	All Disciplines EXCEPT PSCC
SEC DOT 2	5976	1405	DOT1405	57D	All Disciplines EXCEPT PSCC

All encryption will utilize AES256 protocol.

Illinois Example table of SLN / CKR Information



This is an example of secure trunked talkgroups set aside in a single zone in the Illinois statewide trunked system. This is also an example of coordinated effort at the Statewide Interoperability Executive Committee. You can see some talkgroups are for all disciplines and others are discipline specific

## State Talkgroups and Keys Example

SECURE BY								
CH	Zone SECURE BY Channel Tag	CKR SLN	KEY Name	RX Freq	NAC Code	TX Freq	NAC Code	Authorized Entities
1	7MOB59DE	1401	SIEC1401	770.89375	SF7E	770.89375	\$293	All Disciplines except PSCC
2	7MOB79DE	1401	SIEC1401	774.50625	SF7E	774.50625	\$293	All Disciplines except PSCC
3	7LAW81DE	1402	LAW1402	774.00625	SF7E	774.00625	\$293	Law Enforcement Only
4	7LAW82DE	1402	LAW1402	774.35625	SF7E	774.35625	\$293	Law Enforcement Only
5	7FIRE83DE	1403	FIRE1403	773.50625	SF7E	773.50625	\$293	Fire Department Only
6	7FIRE84DE	1403	FIRE1403	773.85625	SF7E	773.85625	\$293	Fire Department Only
7	7MED86DE	1403	FIRE1403	773.00625	SF7E	773.00625	\$293	Fire/EMS Only
8	7MED87DE	1403	FIRE1403	773.35625	SF7E	773.35625	\$293	Fire/EMS Only
9	7MOB59E	1401	SIEC1401	770.89375	SF7E	800.89375	\$293	All Disciplines
10	7MOB79E	1401	SIEC1401	774.50625	SF7E	804.50625	\$293	All Disciplines
11	7LAW81E	1402	LAW1402	774.00625	SF7E	804.00625	\$293	Law Enforcement Only
12	7LAW82E	1402	LAW1402	774.35625	SF7E	804.35625	\$293	Law Enforcement Only
13	7FIRE83E	1403	FIRE1403	773.50625	SF7E	803.50625	\$293	Fire Department Only
14	7FIRE84E	1403	FIRE1403	773.85625	SF7E	803.85625	\$293	Fire Department Only
15	7MED86E	1403	FIRE1403	773.00625	SF7E	803.00625	\$293	Fire/EMS Only
16	7MED87E	1403	FIRE1403	773.35625	SF7E	803.35625	\$293	Fire/EMS Only

All encryption will utilize AES256 protocol.  
Example of Encrypted 700 MHz Nationwide Interoperability Channels as used in Illinois



Remember where the rules were described regarding what non-federal interoperability channels could be encrypted. This chart is a sample of a coordinated plan where a ckr and kid is identified along with the national channel name and frequency information.

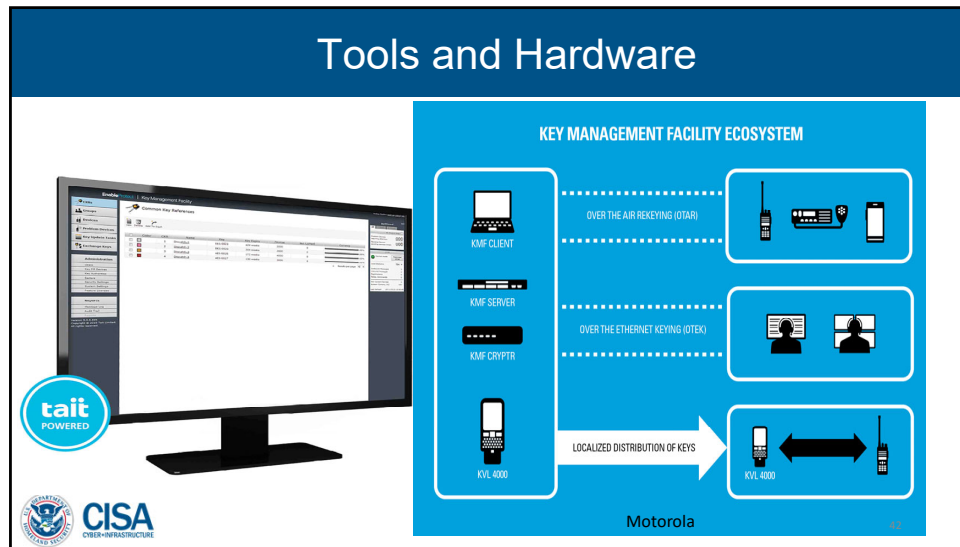


# Simple Spreadsheet Tracking

User / Agency	SLN / CKR 1-4095 (Decimal)	Key ID 0000-FFFF (HEX)	Algorithm				
Motorola	1	1	DES				
ICC	1	1	DES				
SOS	1	1	DES				
IDPH	1	1	DES				
Rockford #1	1	1	ADP				
Barrington	12	18	ADP				
Glen Carbon	12	18	ADP				
Cook County #1	13	19	AES				
Maryville	13	19	ADP				
NWCD Dispatch	31	1F	AES				
NWCD Dispatch	32	20	AES				



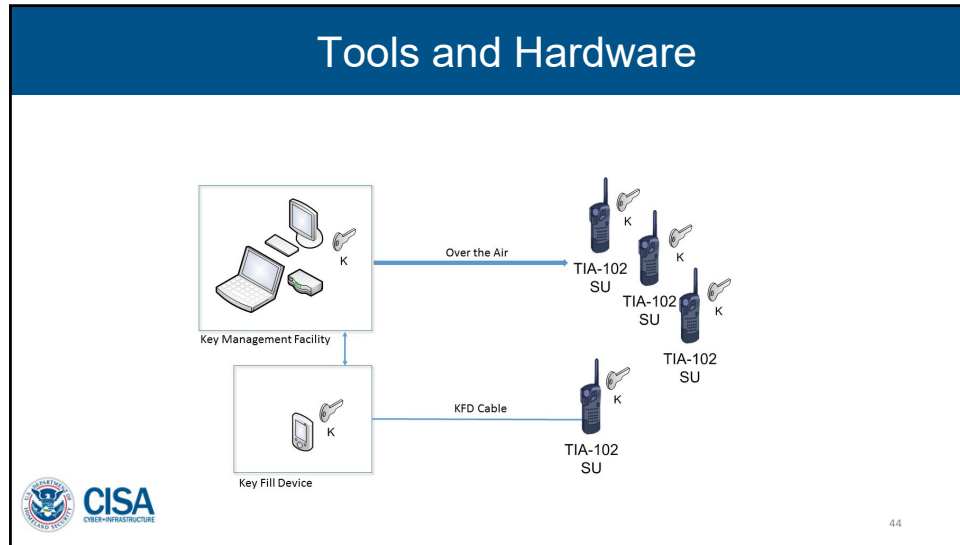
Your record keeping can be as simple as a spreadsheet an example of which is shown. Those which are green are ok. Alternating red/ white or yellow are problematic in some way.



Some brief basics about the hardware available for key loading. The screen on the left illustrates a key management facility (KMF) which is kept in a stationary location and can be partitioned to hold multiple systems. Also illustrated are multiple methods by which to achieve keyloading. **Explain the methods**



Key fill devices (explain each) . Describe why consoles are shown. Patching, consoles tied to a core versus radios tied to an individual resource.



Key fill devices (**explain each**) . Describe why consoles are shown. Patching, consoles tied to a core versus radios tied to an individual resource.

With KMF it's one to many over the air or over a IP network usually located in agency facilities.

I WANT TO SHOW YOU A KEY MANAGEMENT FACILITY THAT SHOULD NOT BE CONSIDERED.

## Basic Specifications

Considerations when specifying features for subscriber devices (Radios)



- Encryption type needed (P25 standard AES 256)
- Number of encryption keys needed ?
- How can the radio be keyloaded ?
  - Direct key fill ?
  - Over the air ?
- Selectable keys / keysets ?



45

Why should basic specifications be considered for subscriber devices ? Standards and operability / interoperability



An encryption key management program is not quite as simple as this.

## The Path Forward

(open dialog)

- Statewide Interoperability Executive Committee or other appropriate guidance / governance body
- System(s) Operator(s)
- Vendor (Radio shops discussion)
- Assessment survey ( Distributed to agencies)
- Survey analysis and Plan development (Agencies and tech shops)
- Implementation
- Ongoing monitoring and adjustments



47

- Let's open the discussion on these topics and possibly set some future plans.
- Public Safety Communications Commission, SIEC, DIGBs ( Are these the groups that encryption should be coordinated through?)
- Vendors ( We need the input and technical system knowledge from vendors)( They need to be part of the plan
- Assessment survey and a survey analysis needs to be completed in order to get an understanding of the current encryption environment.
- A plan needs to be developed based upon the survey results and through a willing coalition of agencies.
- Implementation takes place..... more than likely over a number of years
- Ongoing monitoring and adjustments.



Does anyone have any questions at this point?





### The basics of encryption

Agency	SLN / CKR (DECIMAL)	Key ID (HEX)	Key ID (Decimal)	Encryption Type
Lake County	42	42	66	AES
Lake County	43	43	67	AES
Lake County	44	44	68	AES
Lake County	45	45	69	AES
Will County EMA	46	46	70	?
Livingston County	47	47	71	ADP
Madison County	47	47	71	ADP
Homeland Security	48	48	72	AES
Clark County	48	48	72	ADP
Sangamon Cnty	49	49	73	DES
Springfield PD	74	4A	74	DES
Livingston County	75	4B	75	ADP
Clark County	76	4C	76	ADP
Muscatine	77	4D	77	ADP

Your record keeping can be as simple as a spreadsheet an example of which is shown.