Presentation to the DuPage County ETSB PAC

UNDERSTANDING AND PLANNING LMR ENCRYPTION

2023

Introduction

Dave Dato

ddato@dhsgov.net

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

Resources

Resource Materials

- Guidelines for Encryption in Land Mobile Radio Systems - 2016
  (PDF, 222.55 KB)
- Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems - 2016
  (PDF, 634.25 KB)
- Developing Methods to Improve Encrypted Interoperability in Public Safety Communications (Fact Sheet) - 2016
  (PDF, 162.26 KB)
- Considerations for Encryption in Public Safety Radio Systems - 2016
  (PDF, 321.33 KB)
- Considerations for Encryption in Public Safety Radio Systems Fact Sheet - 2016
  (PDF, 183.94 KB)
- Encryption Key Management Fact Sheet - 2020
  (PDF, 134.80 KB)
- Operational Best Practices for Encryption Key Management - 2020
  (PDF, 3.00 MB)
- Communications Security – Protecting Critical Information, Personnel, and Operations White Paper - 2022
  (PDF, 445.92 KB)

Tip of the Iceberg

The goal this morning is to hit on a few key points about encryption planning and implementation.

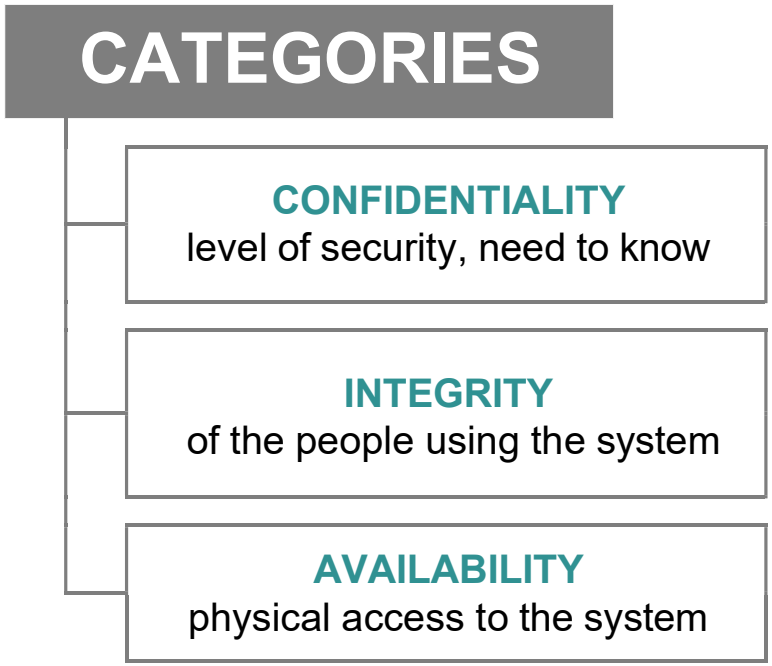
Keep These Items In Mind

- Best practices
- The technical basics of encryption
- Tools and hardware

The End Goal

To ensure operability and interoperability while utilizing encryption.

Security



There is an inverse relation between ease-of-use and level of security.

How Many Keys Are Needed?

Statewide Key 1 is the patch key…Do you have the correct key 1

- LAW
  - Local dispatch (Common Key)
  - Law general
  - Law tactical
  - Shared Ops LE / Fire
  - Regional Secure TGs or channels
    - SWIT Secure TGs
    - Neighboring agencies
  - National Shared Keys
    - Fed IR and LE UHF and VHF
    - CG Com & CG Tac

- FIRE
  - Local dispatch (Common Key)
  - Fire general
  - Fire tactical
  - Shared Ops LE / Fire
  - Regional Secure TGs or channels
    - SWIT Secure TGs
  - National Shared Keys
    - Fed IR
    - CG Com CG Tac

Elements of Encryption Best Practices

Key Management Organization

Key Generation and Distribution

Standards Based Encryption

National SLN Assignment Plan

Education and Training

Outreach

Subscriber device programming

Key Management Facility (KMF)

Crypto Period Considerations

Exercise and Testing

FIPS 140-3 Standard

Communications System Planning

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.

ADP IS WEAK AND ANY USE SHOULD BE CAUTIONED!
WILL YOU PATCH YOUR SECURE TGs TO AN ADP TG ?

Encryption Best Practices

National SLN assignment plan

Adopt a standardized Storage Location Number (SLN) and key ID (KID) plan that minimize operational conflicts. (Already Completed at the state level)

National Interoperability Keys

National Interoperability Keys

SLN	KID	Algorithm	Use	SLN Name	Crypto Period Annual Changes are completed on 1st working Monday of October
1		DES	Public Safety Interoperable	ALL IO D	Annual
2		DES	Federal Interoperable	FED IO D	Annual
3		AES	Public Safety Interoperable	ALL IO A	Annual
4		AES	Federal Interoperable	FED IO A	Annual
5		DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6		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		DES	Multiple Public Safety Disciplines	PS IO D	Static
12		AES	Multiple Public Safety Disciplines	PS IO A	Static
13		DES	National Fire / EMS/ Rescue	NFER D	Static
14		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

Encryption Best Practices

Subscriber device programming

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

Encryption Best Practices

Crypto periods

Develop reasonable policies and plans as they relate to why, when and how to change encryption key material.

Encryption Best Practices

Key generation and distribution

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

Private Entity vs. Public Safety Agency

Encryption Best Practices

Outreach

Share encryption plans and implementation information with all agencies whether they utilize encryption or not, as they may in the future.

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

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 where encryption is permissible on interop frequencies by FCC rule, the 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

Technical Basics

Encryption Terminology

- ***STORAGE LOCATION NUMBER (SLN) AKA Common Key Reference (CKR)***–This is a decimal value between 0 and 4095. SLN is a generic term used to refer to an encryption key slot in a subscriber device.

- The Storage Location Number (SLN) is a “location reference” or “place” in a radio, that the radio program uses to reference what encryption key to send when the radio transmits.

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).

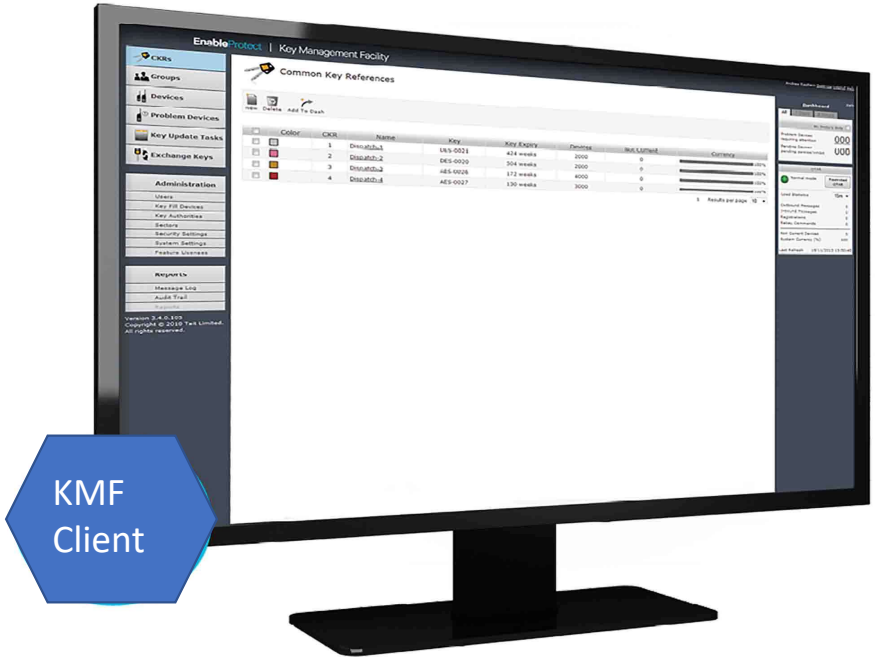
The KID, along with an algorithm identification value are sent as part of the P25 data stream. It is from this information that the receiving radio understands what key to use to decrypt information (audio) sent.

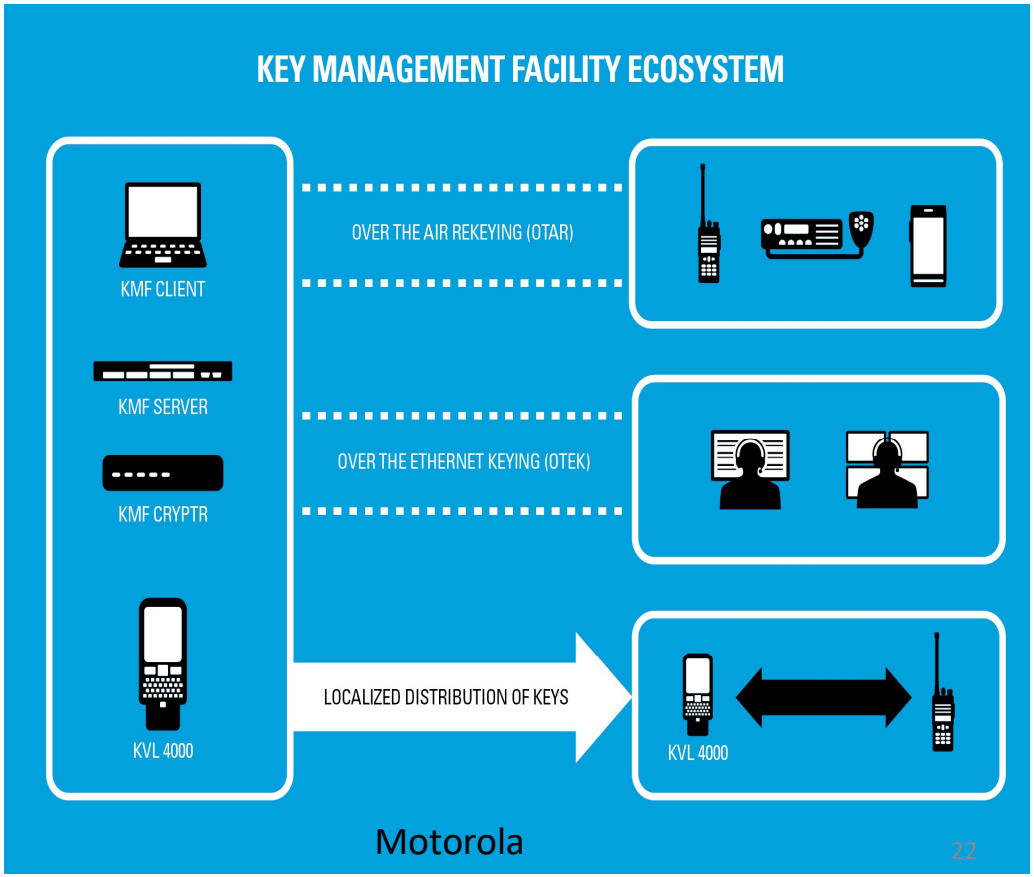
Simple Spreadsheet Tracking of SLNs and KIDs

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

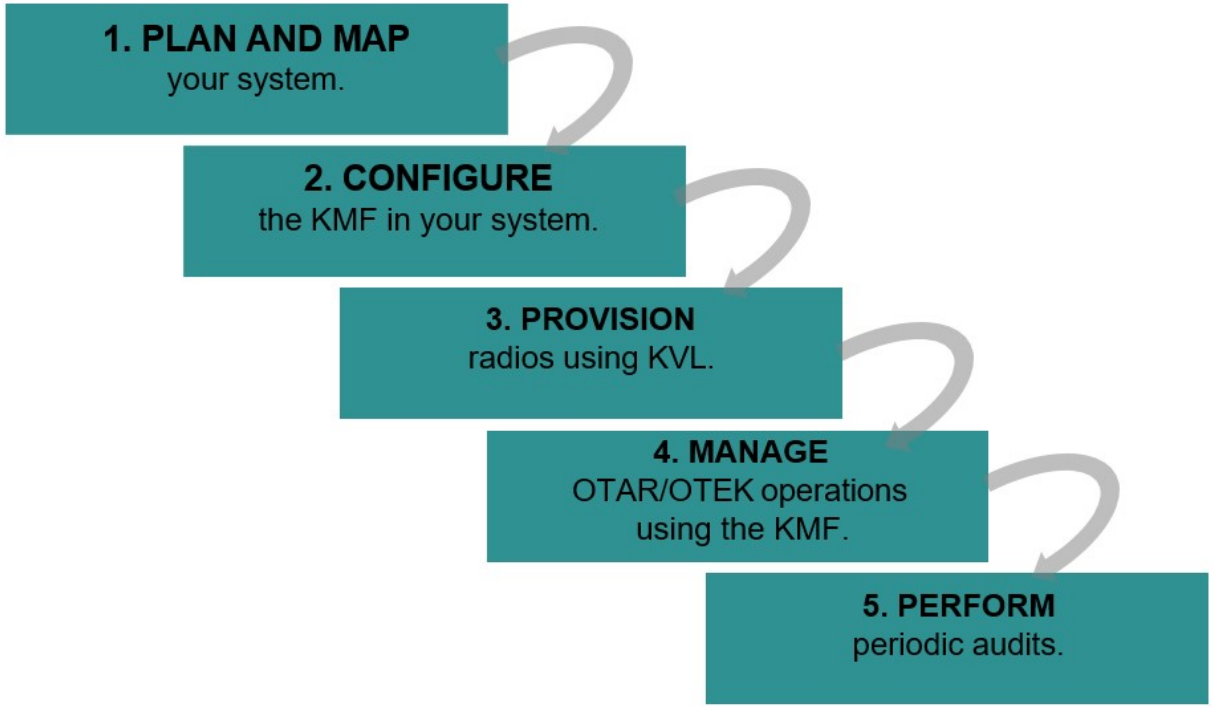
Tools and Hardware

Key management facility examples from different manufacturers.





Set-up and Management of the System



Key Types

Key Type	Description
Master Key	A key used to encrypt and decrypt all key material stored in the KMF database.
Traffic Encryption Key (TEK)	Encrypts voice, data, or Over-The-Air Rekeying (OTAR) and is assigned to Common Key References (CKRs). For OTAR, the TEK is used to outer layer encrypt the KMMs.
Unique Key Encryption Key (UKEK)	A key assigned to a subscriber for encrypting keys within an individually delivered OTAR command. For OTAR, the UKEK is used to inner layer encrypt the KMMs.
Common Key Encryption Key (CKEK)	A key assigned to a group of units for encrypting keys within an OTAR command delivered using the group OTAR method. It is provisioned on the trunking system but only used for conventional OTAR channels.
Key Loss Key (KLK)	Enables a KMF to restore a unit's UKEK after it has been erased by using the unit's Key Loss Key to receive OTAR commands.

Key use and Storage

Common Key Reference (CKR) and **Physical Identifier (PID)** are two types of Key Storage.

- Dispatch Console with VPM (Trunking and Conventional systems) or CRYPTR , CORE Connected vs. Remote consolette
- Digital Interface Unit (ASTRO® 3.1 Conventional systems)
- RNC Radio Network Controller (ASTRO® 3.1 Conventional systems)
- ASTRO® 25 digital radios
- Key Management Facility (KMF)
- KVL
- CDEM Encryption Unit (Conventional systems)
- Archiving Interface Server (AIS) Recorder
- Dispatch Console without VPM (Software Load or OTEK)
- Provisioning Manager (PM)
- Wave Server (CRYPTR)
- CRYPTR

Key Management

Centralized Key Management	Decentralized Key Management
• KMF loads keys through KVL and Store and Forward	• Keys entered with KVL • KMF not used to load keys through Store and Forward

How Will You Keyload ?

- Manual key distribution through the KVL
- Store and forward rekeying through the KMF
- Over-the-Air Rekeying (OTAR)
- Over-the-Ethernet Keying (OTEK)
- Tactical OTAR

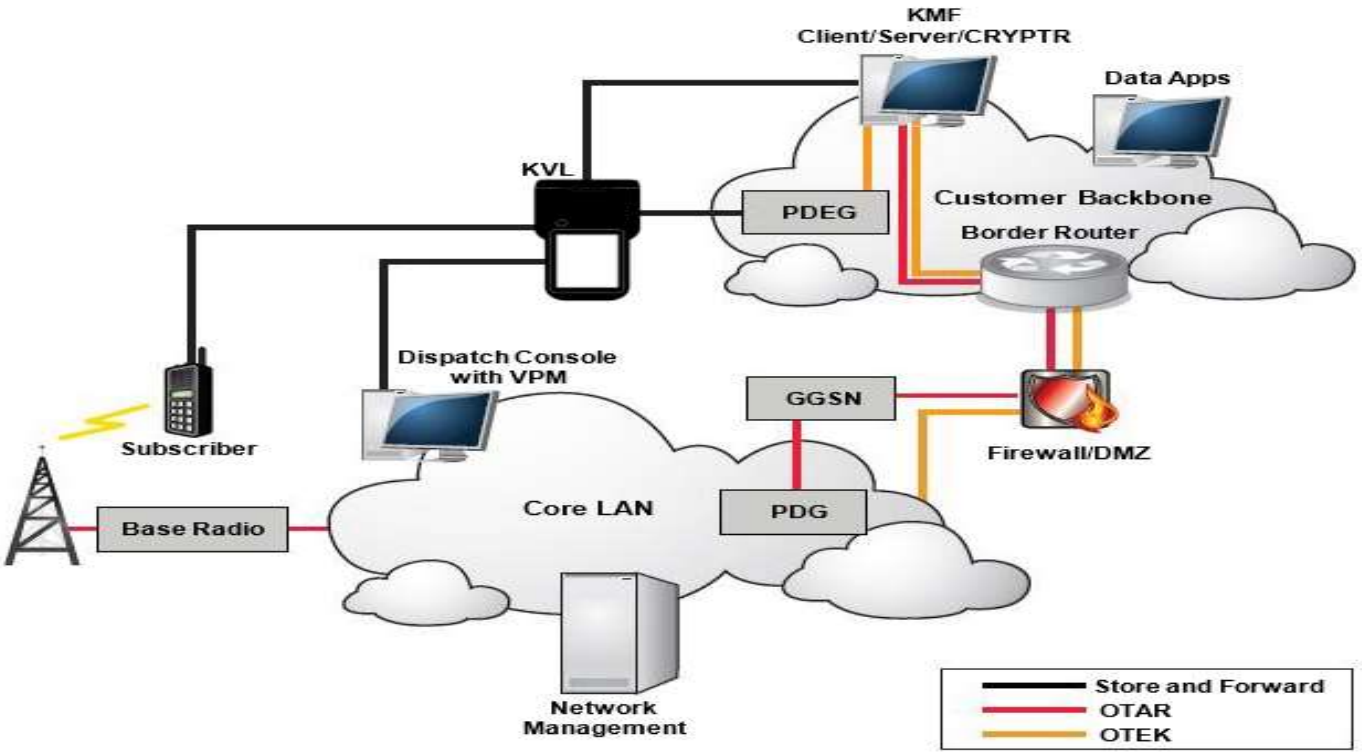
- Do the methods fit your needs?

Available KMFs

- Motorola (Stand-alone) (Private)
- Triad (Kankakee, Grundy, and WESCOM) (Government)
- Lake County ETSB (Government)
- Northwest Central Dispatch (Government)

  - The Starcom Network does not currently have network capacity to provide the ability to tie the KMFs together. Triad, Lake County and NWCD plan on utilizing a different means to connect their KMFs together.

Moving Key Material in the Trunked System



Key Management Security

- **Control Physical Access to All Secure Devices**:
- Radios
- Key Management Facility (KMF)
- Key Variable Loader (KVL)
- Dispatch console with VPM (trunked or conventional)
- Dispatch console without VPM (CRYPTR)
- MGEG (trunked)
- DIU/RNC (conventional)
- PDEG Encryption Unit (trunked)/CDEM (conventional)

Provisioning Manager

- Talkgroup Configuration
- Supergroup Configuration
- Secure Private Call
- Secure Interconnect Call

Subscriber Configuration

- OTAR
- CKR Alias
- Erase Previous Keyset
- Infinite Key Retention
- CKR Alias
- Patch Key, Failsoft Key, Dynamic TG Key, Private Call Key…

- Tactical OTAR ??

KVL

- Admin and Operator passwords
- Audit logging
- TEKs , KEKs and UKEKs

- Store and Forward (Downloads KMMs from KMF to KVL to subscriber devices)(Devices a target for keyloading)
- KVL used for provisioning subscriber devices

Questions / Comments

Thank you