Encryption 101

Todd Velderman
MPSCS
Encryption history on the MPSCS

• 1996-2012  14 Keys added
• 2013-2019  75 Keys added

• ADP – 25 Keys
• DES-OFB – 46 Keys
• AES – 16 Keys
• UKEK – 2 Keys

Total Keys – 89
What is encryption?

• Encryption is a way to secure communication between two or more radios using the same algorithm and key in those radios so only authorized parties can access it.

• It must be the same algorithm, same key data, and the same KID for them to work properly.
Reasons for Encryption

• Top ensure transmissions are accessed only authorized personnel.
• So the radio traffic can not be rebroadcast over the internet
• Keep your traffic off of scanners!
<table>
<thead>
<tr>
<th>Incidents Displayed Below Provided by Incident Page Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident</td>
</tr>
<tr>
<td>VIOLENT CRIME 02/04/19 19:04</td>
</tr>
<tr>
<td>VIOLENT CRIME 02/04/19 19:05</td>
</tr>
<tr>
<td>VIOLENT CRIME 02/04/19 14:18</td>
</tr>
<tr>
<td>SUSPICIOUS DEVICE 02/03/19 19:38</td>
</tr>
<tr>
<td>1-ALARM FIRE 02/03/19 19:31</td>
</tr>
</tbody>
</table>

*Incidents delayed up to 2 hours. Details here.*
f.y.i. - U.P. Breaking News Drill Advisory 12-4-17 5:43 p.m. ET
It is only a drill - do not be alarmed.
A drill is underway to deal with the scenario of an active shooter at a UP Health System - Portage in Houghton County. Numerous officials are responding to the drill - It is only a drill. Not sure how many locations this will involve as staging is being set up near ER and rehab. Hancock Fire is currently in charge of incident command. This drill just started.
Reasons for not using Encryption

• Do not use encryption if an agency is using your talkgroups but do not have encryption in their radios.
• Must use the same level of encryption to maintain interoperability.
• Certain talkgroups can not be encrypted. County Com, certain event talkgroups, interop talkgroups.
Types of Encryption

• **ADP (Advanced Digital Privacy)/ARC4** Low level software based encryption. Usually loaded in template but can be loaded with keyloader.

• **DES-OFB (Digital Encryption Standard Output Feed Back)** Mid Level encryption that is usually loaded with keyloader but can be loaded with software.

• **AES (Advanced Encryption Standard)** Federal grade encryption that can be loaded with Keyloader or software (in some radios).
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Length</th>
<th>P25</th>
<th>Date Introduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES-XL</td>
<td>56 Bit</td>
<td>No</td>
<td>1987</td>
</tr>
<tr>
<td>DES-OFB</td>
<td>56 Bit</td>
<td>No</td>
<td>1996</td>
</tr>
<tr>
<td>AES 256</td>
<td>256 Bit</td>
<td>Yes</td>
<td>2002</td>
</tr>
<tr>
<td>ADP</td>
<td>40 Bit</td>
<td>No</td>
<td>2003</td>
</tr>
</tbody>
</table>

**Key data as typed into keyloader**

**ADP** – 0123456789  
**DES-OFB** – 0123456789ABCDEF  
**AES** -  
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
ADP encryption

• “Free” encryption that comes with all APX radios. May be a paid feature in the future.
• Least secure of all encryption types.
• Not P25 Compliant
• Compatible with ARC4 encryption in other radios.
• Basically only good for keeping radio traffic off of scanners.
• Key can not be read from radio but can be seen in the template that was sent from the State.
DES-OFB Encryption

• Mid tier encryption that is widely in use on the MPSCS.
• Was a P25 standard until May 2005
• Used in the event zones I and J (selectable)
• Needed to maintain compatibility with older radios.
AES Encryption

• High tier encryption
• Not many agencies on the MPSCS use this
• Federal standard used by all federal agencies
• Several different types but AES256 is the standard on the MPSCS
How to tell if radio has encryption

• Can not tell if the radio has encryption just by looking at the radio. Nothing in the flashcode says what algorithm is loaded. Must go thru the menu options to see what is in it.
Strapping

Used to tell the radio how to transmit encryption.

- **Clear** – will only transmit clear traffic. Can not be changed to encrypted.
- **Selectable** – Can be selected for either clear or encrypted traffic. Changed with either a button or switch.
- **Strapped** – Will only transmit encrypted traffic. Can not be changed to clear.
Receiving Encrypted Traffic

• Encryption is a transmit feature so you can’t turn it on or off for receiving encrypted traffic. It must be turned on when you transmit.

• Most radios will decrypt encryption even if it is turned off.

• Can see if the traffic is encrypted by the ☰ on the display that will flash when receiving encrypted traffic.

February 19-22, 2019
KVL Keyloader

• A device that stores keys and loads them into a unit when encryption is needed.

• Can be used for both Radios and Consoles
• Used for OTAR functions
• Used to add encryption feature to radios
Types of Keyloaders used by the MPSC

- **KVL 3000** – ASN mode only
- **KVL 3000 Plus** – ASN and Astro 25 Mode

- **KVL 4000** – ASN, Astro 25 Mode and Radio Management
  - Consist of two pieces. The MC55 (top) and secure adaptor (bottom).

- **KVL 5000** ?
Software vs Hardware Keys

• **Software Keys**
  – Manually typed into the software and then programmed into the radio.
  – Must know the key data in order to load it and is less secure.
  – Code may be seen in the codeplug in some radios.

• **Hardware Keys**
  – Must be loaded with a keyloader.
  – The key data is not known and more secure

• In Motorola radios you can not have both hardware and software keys at the same time. You have to convert the software to a hardware key and load with a keyloader.
• In other radios you can have both at the same time.
OTAR – Over the Air Rekeying

• Radios can be rekeyed thru the radio system without using a keyloader
• MPSCS has a KMF (Key Management Facility) located in a secure location that can be used to rekey radios over the system.
• Radios must be provision with the OTAR and Data options for it to work properly.
• Require a store and forward process before the radios can use the OTAR function.
CKR’s

• CKR – Common Key Reference
• Used as a reference between the template in the radio and the keyloader.
• Can be different between groups but need to be the same between the keyloader and template when keyloading.
KEY ID’s

• Four digit code (hex) that is used to transmit what key is used across the system.
• Must be the same in both transmitting and receiving unit to decode traffic
• Can not have the same KID’s in the same keyloader.
Adding encryption to radios

• In older radios encryption was added by manually installing an encryption module
• In newer radios encryption is added with a software upgrade.
• Motorola APX radio need to be upgraded using a KVL.
Supergroup Key (CKR 1)

- When a patch is created in the console a supergroup is created. This allows multiple takgroups that may have different encryption in them to be used as a single resource in the system. Because multiple keys may be used it uses a supergroup key instead. This key must also be loaded in the radios for the encryption to work.
Patch/Failsoft/Private Call Keys

• This tells the radio what key to use during certain events. Only one key can be selected for each event and is applied on a radio wide basis.
• If you have the wrong key for the event then you will not be heard on the other end.
• There is no notification that you are using the wrong key.
Single Key/ Multi Key

- **Single Key** – Can have only one key in the radio at a time.
  - You can have multiple algorithms (ADP, AES) but only one key.

- **Multi Key** – Can have multiple keys from multiple algorithms.
  - OTAR radios come with multikey.
Infinite Key Retention

• If unchecked (default setting!) you will loose any keys if the radio looses power.

• Recommend that this box is checked.
How to get Encryption on the system

• Several things to consider when adding encryption to your radios.
  – What level of encryption to use
  – What talkgroups would use encryption
  – What other agencies use your encrypted talkgroups.
  – Contact MPSCS radio programming for setup.
    • Coordinate existing keys
    • Setup of new keys
    • Template layout
    • Key management
Conclusion

• To maintain interoperability you must coordinate with all agencies that are using the talkgroups that are encrypted.

• It is possible to be too secure.
Questions?