ENCRYPTION INTEROPERABILITY, IMPLEMENTATION AND BEST PRACTICES

PANEL PRESENTATION AND DISCUSSION – SUTTER, BUTTE AND PLACER COUNTIES + ROSEVILLE

NORTHERN CALIFORNIA APCO CHAPTER MEETING

2/11/2021

AGENDA

- What is Encryption and Why Use It?
- Essential Components
- Best Practices
- Why is Planning So Important?
- Interoperability Planning Examples
- Next Steps
- Resources
- Panel Discussion, Q&A

WHAT IS ENCRYPTION AND WHY USE IT?

- Encryption is a way to secure comms between only radios using the same key
- Encrypted transmissions can only be decrypted by radios that are capable of, provisioned, AND programmed to do so
- Different algorithms (i.e. ADP, DES, AES) and key bit sizes (i.e. 40, 128, 256)
  - Federal standard = AES 256-bit
- FBI and CalDOJ require radio transmission of CJI and PII to be encrypted
- Ensures protection of sensitive data as defined in FBI and CLETS policies, practices and procedures

ESSENTIAL COMPONENTS

- Required: P25 Digital provisioned infrastructure, control stations, dispatch consoles, logging recorder, subscribers and key variable loader (KVL)
- Optional: key management facility (KMF), over the air rekeying (OTAR)
- Traffic Encryption Key (**TEK**): the unique key used to encrypt/decrypt traffic
- Key ID (**KID**): provides a unique address to identify a **TEK**
- Common Key Reference (**CKR**): a 'slot' the radio uses to reference what key to send when the radio transmits (aka Storage Location Number (SLN))

BEST PRACTICES

- Effective planning, regional cooperation and a basic understanding of how essential components are coordinated leads to a successful encryption program
- Education and training – agency (ops & tech) and vendors
- Communications planning – spend time up front to avoid interop issues later
- Standards-based encryption – AES-256 (Advanced Encryption Standard, 256 bits)
- KID and CKR assignment plan – assignments minimize operational conflicts
- Subscriber radio programming – operational objectives determine parameters
  - Common key available for general interop purposes (i.e. Omaha)

BEST PRACTICES, CONTINUED

- Exercise and testing – essential to successful operations, refine ICS 217/205
- Key management organization – a regional/state clearinghouse is essential to mitigate operational conflicts
  - Be mindful of federal CKR/KID reservations and aware of default CKR/KID assignments
- Key generation and distribution – what agencies are responsible for creating and providing encryption keys
- Outreach – collaborate to ensure effective regional/state implementation

WHY IS PLANNING SO IMPORTANT?

- Lack of encryption coordination can gravely impact agencies' ability to interoperate on an encrypted channel
- Can take years and lots of money to undo and/or fill gaps
- What agencies are currently programmed in your radios? Do they have plans to begin or increase use of encryption that could hamper interoperability?
- What are you willing to share with other agencies?
- Examples
  - Bad: CHP AirOps challenges or ?
  - Good: Sac-Placer-Butte-Roseville CKR plan

CKR PLANNING EXAMPLE – HIGH LEVEL

Jurisdiction		CKR Range
City of Roseville		1100 - 1199
Placer County		1500 - 1599
Sac Co/SRRCS		2000 - 2199
Sac Sheriff		2200 - 2299
City of Sacramento		2500 - 2599
Butte County BRICS		2800 - 2899

CKR/KID PLANNING EXAMPLE - DETAILED

Group	Low	High	HEX Low	HEX High	A-Key ID Low	A-Key ID High	A Key ID Range	B-Key ID Low	B-Key ID High	B Key ID Range	User
1	1	99	0001	0063	A001	A063	40961 - 41059	B001	B063	45057 - 45155	Federal
2	100	199	0064	00C7	A064	A0C7	41060 - 41159	B064	B0C7	45156 - 45255	Federal
3	200	299	00C8	012B	A0C8	A12B	41160 - 41259	B0C8	B12B	45256 - 45355	Federal
4	300	399	012C	018F	A12C	A18F	41260 - 41359	B12C	B18F	45356 - 45455	Federal
5	400	499	0190	01F3	A190	A1F3	41360 - 41459	B190	B1F3	45456 - 45555	
6	500	599	01F4	0257	A1F4	A257	41460 - 41559	B1F4	B257	45556 - 45655	
7	600	699	0258	02BB	A258	A2BB	41560 - 41659	B258	B2BB	45656 - 45755	Federal
8	700	799	02BC	031F	A2BC	A31F	41660 - 41759	B2BC	B31F	45756 - 45855	Federal
9	800	899	0320	0383	A320	A383	41760 - 41859	B320	B383	45856 - 45955	Federal
10	900	999	0384	03E7	A384	A3E7	41860 - 41959	B384	B3E7	45956 - 46055	
11	1000	1099	03E8	044B	A3E8	A44B	41960 - 42059	B3E8	B44B	46056 - 46155	
12	1100	1199	044C	04AF	A44C	A4AF	42060 - 42159	B44C	B4AF	46156 - 46255	City of Roseville
13	1200	1299	04B0	0513	A4B0	A513	42160 - 42259	B4B0	B513	46256 - 46355	
14	1300	1399	0514	0577	A514	A577	42260 - 42359	B514	B577	46356 - 46455	
15	1400	1499	0578	05DB	A578	A5DB	42360 - 42459	B578	B5DB	46456 - 46555	
16	1500	1599	05DC	063F	A5DC	A63F	42460 - 42559	B5DC	B63F	46556 - 46655	Placer County
17	1600	1699	0640	06A3	A640	A6A3	42560 - 42659	B640	B6A3	46656 - 46755	
18	1700	1799	06A4	0707	A6A4	A707	42660 - 42759	B6A4	B707	46756 - 46855	
19	1800	1899	0708	076B	A708	A76B	42760 - 42859	B708	B76B	46856 - 46955	
20	1900	1999	076C	07CF	A76C	A7CF	42860 - 42959	B76C	B7CF	46956 - 47055	
21	2000	2099	07D0	0833	A7D0	A833	42960 - 43059	B7D0	B833	47056 - 47155	Sac Co/SRRCS
22	2100	2199	0834	0897	A834	A897	43060 - 43159	B834	B897	47156 - 47255	Sac Co/SRRCS
23	2200	2299	0898	08FB	A898	A8FB	43160 - 43259	B898	B8FB	47256 - 47355	Sac Sheriff
24	2300	2399	08FC	095F	A8FC	A95F	43260 - 43359	B8FC	B95F	47356 - 47455	
25	2400	2499	0960	09C3	A960	A9C3	43360 - 43459	B960	B9C3	47456 - 47555	
26	2500	2599	09C4	0A27	A9C4	AA27	43460 - 43559	B9C4	BA27	47556 - 47655	Sac City
27	2600	2699	0A28	0A8B	AA28	AA8B	43560 - 43659	BA28	BA8B	47656 - 47755	
28	2700	2799	0A8C	0AEF	AA8C	AAEF	43660 - 43759	BA8C	BAEF	47756 - 47855	
29	2800	2899	0AF0	0B53	AAF0	AB53	43760 - 43859	BAF0	BB53	47856 - 47955	Butte Co BRICS
30	2900	2999	0B54	0BB7	AB54	ABB7	43860 - 43959	BB54	BBB7	47956 - 48055	

NEXT STEPS

- Take inventory of current encryption provisioning and capabilities
  - Components: subscribers, consoles, infrastructure
  - Single vs. multi-key
  - Algorithm: proprietary (i.e. ADP, RC4) vs. AES-256
  - If already using encryption, what are the CKR and KID assignments
- Ensure DOJ CLETS and FBI compliance or ID workaround
- Operational goals → technical objectives → identify funding
- Follow best practices: educate, plan, organize, implement, exercise, outreach
- Participate in NorCal APCO, build relationships, attend RPC meetings

RESOURCES

- CalDOJ bulletin link:

https://oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/20-09-cjis.pdf

- CalDOJ contact info:
  - Email the CLETS Administration Section @ CAS@doj.ca.gov or call (916) 210-4240
- FBI CJIS Security Policy (i.e. 5.10.1.2 Encryption, page #64)

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

- DHS Cyber & Infrastructure Security Agency – Encryption best practices

https://www.cisa.gov/publication/encryption

- NorCal APCO monthly chapter meetings – ops and frequency coordination

http://www.napco.org

PANEL DISCUSSION

- Q & A
- Discussion