TOUCHLESS KEY PROVISIONING

SIGNIFICANTLY REDUCE TIME SPENT ENCRYPTING RADIOS

LEVERAGE RADIOCENTRAL AND THE KEY MANAGEMENT FACILITY TO ADD ENCRYPTION KEYS REMOTELY

As the public-safety climate evolves, the need for secure and encrypted radio communications is growing. Physically connecting a Key Variable Loader (KVL) to each radio to enable encryption can be a time consuming process, especially for agencies with large fleets.

The APX NEXT® radio family now offers the ability to reduce time and effort spent on enabling encryption with Touchless Key Provisioning (TKP). Forget the cable. Radios can receive encryption keys remotely.

TKP is a one-time process used to deliver initial encryption keys to APX NEXT radios with the help of RadioCentral, the Key Management Facility (KMF), and Over-the-Air Rekeying (OTAR). The encryption provisioning process is streamlined - key pairs are generated by each radio right in the Motorola Solutions factory. Before radios arrive, RadioCentral is used to export a TKP factory public key for one or more radios into a file that can be imported into the KMF.

Once the public key file is imported into the KMF, a unique key (UKEK) can be assigned by the KMF operator and delivered to the radio encrypted with a key that has been agreed between the KMF and the radio at the start of OTAR using the radio's factory key pair. As the UKEK is delivered to the radio, the TKP process is complete and the normal OTAR process is used moving forward.

DELIVERY

TKP requires a one-time charge to purchase the KMF license fee and the required radio features ordered on APX NEXT radios.

COMPATIBLE PRODUCTS

APX NEXT family radios.

DEPENDENCIES

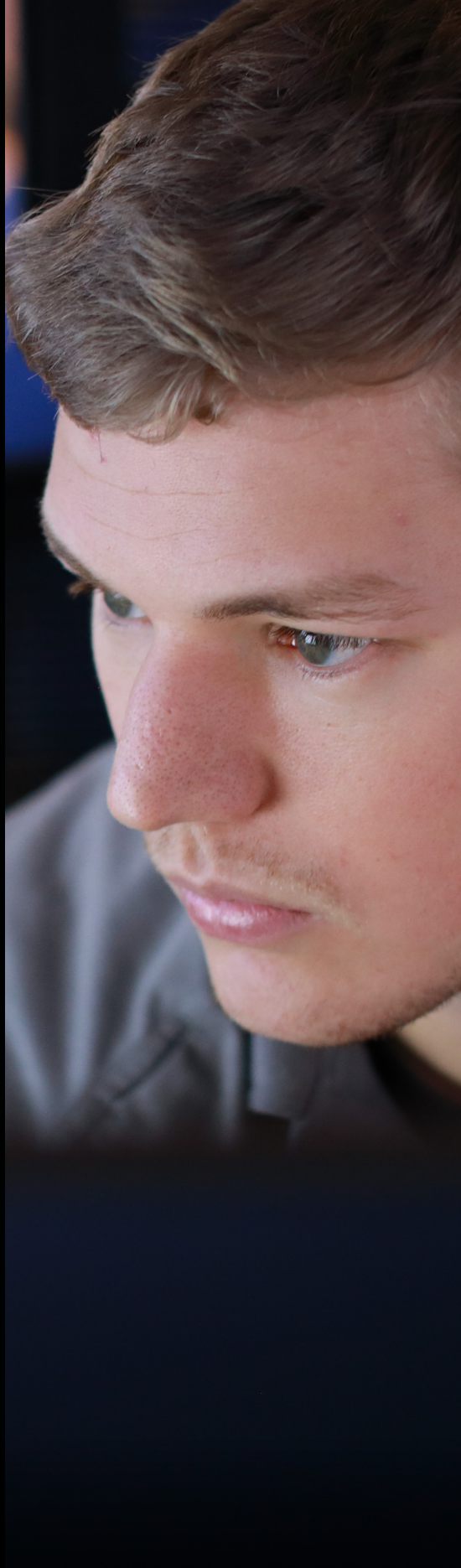
- Not supported on Astro 3.1 conventional
- TKP requires SR2020.3 radio software

INFRASTRUCTURE IMPACT

- RadioCentral
- KMF Requirements
  - KMF version R10.00.0510 and later
  - KMF CryptR
  - TKP license on KMF CA03643AA
  - AES-256 algorithm on KMF CryptR
- Radio Feature Requirements
  - Digital IMBE Operation
  - Over-the-air rekeying (OTAR)
  - Multikey
  - AES-256 required, DES, DES-XL, DES-OFB, DVP-XL, ADP* optional

SECURITY

Factory key pairs are created in the radio's hardware security module and private keys cannot be extracted. The KMF operator controls TKP per radio. TKP must be enabled prior to the APX NEXT radio registration with the KMF for OTAR. Once the KMF provisions keys, it will automatically disable TKP for that radio to prevent a zeroized radio from re-obtaining keys.



*ADP encryption keys loaded via Radio Central rather than the KMF

1. MOTOROLA SOLUTIONS FACTORY

Motorola Solutions factory generates the codeplug and a key pair for each radio in the factory. A public key file is distributed to the customer from MSI via RadioCentral.

2. SYSTEM PLANNING

Assign radio IDs and talk groups. Map keys to talk groups in RadioCentral, Key Management Facility, and Provisioning Manager.

3. RADIO CENTRAL

Enter radio ID, enable encryption and OTAR in the radio code plug, assign Common Key References (CKRs), add KMF profile information. Export public key file. Enter ADP keys into the code plug (if applicable).

4. KEY MANAGEMENT FACILITY

Import the public key file, create keys and assign them to CKRs, add radio records for each radio - each radio added to radio talk group in KMF, enable TKP for each radio.

5. PROVISIONING MANAGER

Enter each radio into radio records and assign CKRs, assign talk groups to CKRs.

6. APX NEXT

On your APX NEXT radio, change to the talk group or channel that is associated with the KMF.

BENEFITS

- Quickly enable end-to-end encryption without the use of a KVL
- Radios can receive encryption keys remotely
- Choose to provision encryption on one or batches of radios
- Encrypted devices can ship directly to users in the field without Radio Tech/Administrator needing to physically enable encryption

For more information, please visit
www.motorolasolutions.com

APX NEXT

MOTOROLA SOLUTIONS