



White Paper – April 2009

BK Radio KNG-P150/P400

Wireless Tactical OTAR

The BK Radio KNG-P150/P400 APCO P25 Digital Handheld from RELM Wireless Corporation meets or exceeds the highest performance specifications of all comparable digital two-way radios, providing clearest sound with least distortion.

The KNG-P150/P400 meets or exceeds requirements for APCO Project 25 (P25) and TIA Class A specifications including interoperability with other P25-compliant VHF/UHF radio products.

Smaller and lighter than any other P25 portable radio, the KNG-P150/P400 is infused with advanced features, yet designed for ease of use and custom-programming in the field.

In response to a US Army requirement for encryption key management in AFGHANISTAN, Relm Wireless has developed a Wireless Tactical OTAR feature for the KNG Series APCO P25 Digital handheld, enabling lower echelons within the military that have no access to Key loaders or KMF infrastructure to quickly re-key group member radios from a previously designated master radio.

Summary

Per Federal Information Processing Standard (FIPS) 140-2 and CENTCOM Land Mobile Radio (LMR) policy Advanced Encryption Standard (AES) 256 is the standard that will be used for encryption of transmission systems such as LMR. In order for a radio to be technically acceptable it must meet this requirement. In addition, industry best engineering practices that have been adopted by CJTF-101 dictate that Over-The-Air Re-key (OTAR) is a must. This provides the fastest mechanism for LMR to receive the newest key in order to facilitate secure communications between US Forces when re-key is necessary. This re-key option allows Soldiers at remote locations to re-key their radios with little or no additional infrastructure equipment whenever needed in order to be able to talk securely to other units.

The only other options are to talk un-secure which could result in the loss of lives or to suspend operations for days at a time while soldiers manually re-key each LMR. The requiring organization is fully aware of the OTAR capability that is provided by industry which involves attaching a Key Loader component to a radio.

The Key Loader component is not a viable option because it requires additional pieces of equipment and infrastructure in order to use this capability. The radio will be used throughout the entire theater of Afghanistan. Remote FOB's and COP's where base infrastructure are limited and may not always be able to support the resources needed to operate/maintain the required equipment needed to re-key key loader dependent LMR.

Relm Wireless has developed a Wireless Tactical OTAR feature, and except for the initial setup of the radio equipment is entirely independent of any other Key management hardware, such as a KMF (Key Management Facility) or Key loader.

Tactical OTAR Setup and Operation

Radio Setup using KVL3000PLUS

```
ENTER THE
KMFRSI>
999999
LOAD
```

1. Set and load KMFRSI.

```
ENTER THE
TGTRSI>
123456
LOAD
```

2. Set and load TGTRSI. It is recommended that the TGTRSI be programmed to match the radio's P25 ID.

```
ENTER THE
MNP>
5535
LOAD
```

3. Set and load MNP.

```
CKR▶0001
ALG: AES-256
KID: 1111
LOAD
```

4. Load up to 32 TEK keys. CKR numbers must match the SLN assigned with the radio editor software under the "Encryption" tab. (See "Configuration set with Radio Editor" for SLN setting information.)

```
CKR▶61440
ALG: AES-256
KID: 1234
LOAD
```

5. Load a Common KEK (CKEK) key. The CKR number of the CKEK must be between 61440 and 65535. This number must match the CKEK number set with the radio editor software under the "Tactical OTAR" tab. (See "Configuration set with Radio Editor".)

```
CKR▶12345
ALG: AES-256
KID: 1313
LOAD
```

6. Load a MAC TEK (MTEK) key. The CKR number of the MTEK must be between 1 and 61439. This number must match the MTEK number set with the radio editor software under the "Tactical OTAR" tab. (See "Configuration set with Radio Editor".)

Sending the new TEK utilizing Wireless Tactical OTAR



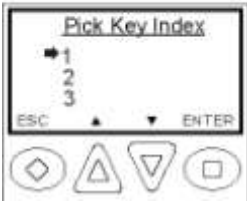
1. Select the channel designated as the OTAR channel.



2. Press the programmed "Menu" button.
3. Use the Up/Down buttons to scroll to "Tact. OTAR" and press the enter button.



4. Use the Up/Down buttons to select the desired encryption key. Programmed key labels are displayed. To view the label and key index press the "#" button.
Alternatively the key can be selected directly via the keypad by pressing 1-32.



5. If the "Key Pick List Target" is programmed (see "Target Radio Options" under "Key Source Radio Configuration") the pick list target screen is displayed. Use the Up/Down buttons to select the desired target key slot. This is the key pick list slot where the target radio will store the transferred key.



6. Press the enter key to begin the key transfer. When the key information has been sent the radio will momentarily display "Key Transfer Successful".

Should the key transfer fail for any other reason a failure message with a two digit error code will be displayed.

Receiving the new TEK utilizing Wireless Tactical OTAR

Select the channel designated as the OTAR channel to receive the re-key information.



Upon successful key transfer the radio will show the received key's programmed label and "Key Received". The key received message remains displayed until radio power is cycled. The radio will operate normally even while the message is displayed.