KENWOOD

P25 Advanced Network Key

User Manual

Ver 1.0

Version: *1.0*

Last Updated: *2011.06*

Language: *English*

Revision History

Date	Description
2011.27.06	Initial release

Table of Contents

Table of Figures

About this Technical Document

This document describes the design and use of the Advanced Network Key function in the KPG-95DG FPU. It is intended to provide a technical description of the features and behavior of the Advanced Network Key.

It is intended to be read by P25 System Operator and their authorized personnel.

1 Introduction

Currently, Kenwood Communications offers two levels of security for trunked, radio system network information, in the TK-5x10 series of APCO P25 radios. These two levels, defined by software license ID, are Dealer level and System Operator level. The major difference between to the two software license levels is the ability to define, or edit, the network configuration parameters to be programmed into the radios. In this current security model commonly changed parameters, such as talk group ID lists, are included in the information that is only editable with a System Operator level software license ID.

Many system owners/operators require a greater level of flexibility in the parameters that field personnel have the ability to edit, but, without the need to give each of them the full access of the System Operator software license ID. System Operators have also expressed the desire to restrict programming access, by field personnel, to physical radios defined by either ESN or serial number, and the Unit IDs (UID) assigned to those radios. These are the concerns the Advanced Network Key functionality, to be added to the programming software for TK-5x10 series radios attempts to address. In this document, the components and operation, of the Advanced Network Key will be outlined. These components included the actual hardware key as well as the procedures of use.

2 Hardware

The Advanced Network Key will make use of a "smart key" in the form of a USB dongle. This dongle will be created by System Operators, and then given to authorized field personnel, and will contain radio network information, as well as radio parameter access permissions. This section will describe some of the features of the actual dongle hardware. How those features are used is described in section 3 Software.

2.1.1 Master Key (KWD-ANK-MK)

The master key is to be created by Kenwood personnel, and serves the same purpose as a system key file (SKF), serves currently. It will define the Home System ID (HSID) that the System Operator is authorized to create a network information file for, as well as, provide access to all network programming fields in the FPU. In addition to those legacy features, the master key will allow the system operator to create access keys (described later), that can use issued to field personnel.

Only one master key with a single HSID is supported by the software.

2.1.2 Access Key (KWD-ANK-AK)

An access key, created by a System Operator, will contain the network information for a maximum of 1 HSID, as well as, any access permissions assigned by the System Operator. If a Dealer needs network information from several different System Operators, then an access key will need to be obtained from each System Operator. The FPU will support up to 16 access keys to be used in programming, which matches the radio's limit of 16 networks.

3 Software

Although KPG-95DG has the capability to configure all TK-5x10 P25 radios, the use of the Advanced Network Key features is restricted to hardware version 3 radios and above only. This section will describe how the features are enabled and a description of those features.

3.1 Enabling the Advanced Network Key Features

After installing the software on a PC, the System Operator will then navigate to the "Tools->License ID" menu and check the "Use Advanced Network Key" checkbox. At that time, the user will be prompted to restart the FPU, so that the additional features can be enabled.

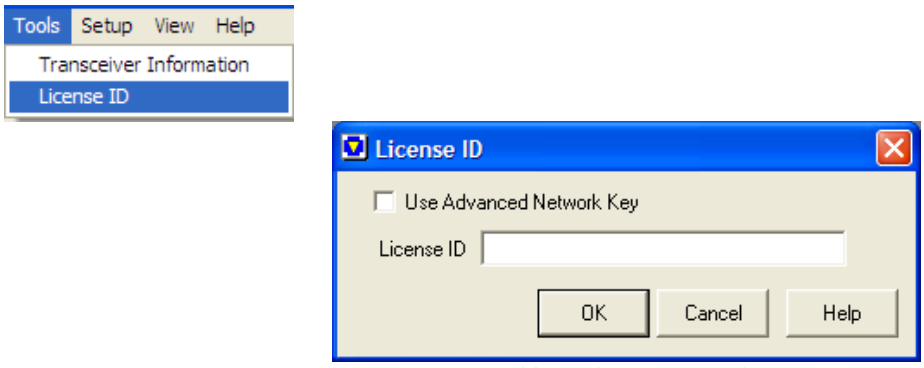

Figure 3.1-1 Enabling Advance Network Key Features

Once the features are enabled, the FPU will attempt to detect and validate, any dongles connected to the computer. If no dongles are connected or, a dongle is connected, but not valid for the license ID of the software, the Advanced Network Key functions will be disabled. When the Advanced Network Key functions are enabled, the FPU will behave in the same manner that is defined by the software license ID.

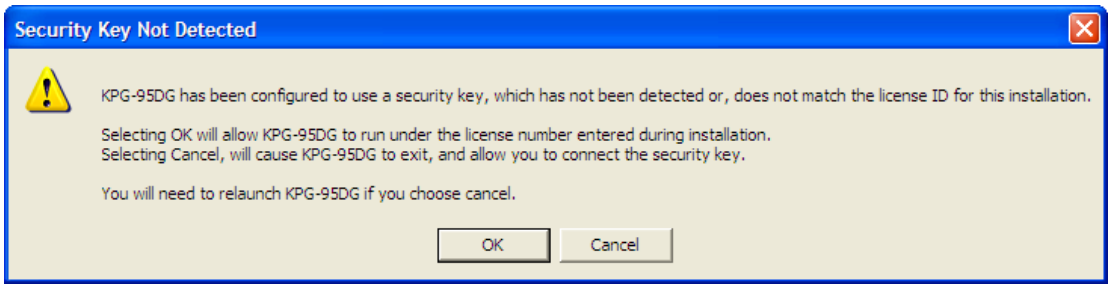

Figure 3.1-2 Dongle Not Detected Warning

For a System Operator, this would make it impossible to edit network information because they do not have a valid SKF file to authorize the network editing functions. It is the master key that authorizes those functions, when “Use Advanced Network Key” is checked. For a Dealer, it would make it impossible to edit, open or save any network files created with information from an access key.

When a System Operator has the Advanced Network Key features enabled, and has a valid master key connected to the computer, the string “Master” will display in the FPU’s statusbar where previously it read, “System Operator”.

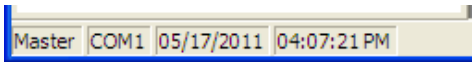

Figure 3.1-3 Master Mode Enabled

3.2 Network Information Security

In order to ensure that network information cannot be distributed to unauthorized entities; there are several security measures that are in place. These measures make use of a combination of the security features included in the USB dongle, and security measures included in the FPU itself.

3.2.1 Key Detection

When creating an access key (described later), the System Operator will enter the software license ID, of the person that they wish to authorize access for. That person must also be using the version of KPG-95DG that supports the Advanced Network Key features, and those features must be enabled using the procedure outlined in section 3.1.

If the features are not enabled, the FPU will not even attempt detection of any attached USB dongles. If the features are enabled, but no access key matching the dealer's software license ID are found, the message shown in Figure 3.1-2 will be displayed and the Advanced Network Key functions will be disabled

3.2.2 Key Network Data Encryption

If the previous conditions of correct version of the FPU, Advanced Network Key features enabled, and valid access key matching the software license ID of the user are met, the user can then load (or import) the network information contained on the key, into the network file in the FPU. Because the user may have permissions to edit the actual network data, and because they cannot write any edited information back to the key, the user may choose to save edited network data to their local hard drive, to be loaded at a later time.

This data written to the hard drive is secure. Only the access key with the correct hardware ID will be capable of generating the 128-bit encryption key needed to decrypt the network data. In addition, if the access key has been updated after this information was saved, the "update counter", in the encrypted data description header will not match the key's current value, and so the file will not be opened. This prevents users from open older saved files when the System Operator wants them using the most recent information on the access key (see Figure 3.2-1).

3.2.3 FPU Network File Encryption

After adding network information, from an access key, a Dealer may make several changes that affect the network file, as a whole. Also, when writing to a radio or saving a personality data file, the FPU requires that the network file be saved to the hard disk. When information loaded from an access key exists in a network file, that information will be encrypted before saving a network file. Only the key with the matching hardware ID and that has not been updated since the information was saved, will be able to successfully decrypt and open the saved network file.

3.2.4 Key Verification

Once network information has been either saved to the hard drive, or written to a radio, it will not be possible to open a network file or read data from a radio, without the specific access key used to create the data. This is done using the unique hardware ID assigned to each USB dongle.

In addition, loading network files from the hard drive requires the information on the access key to be the same "data version" as when the files were when the file was created. If the access key data was updated by the System Operator, after a network file was saved, the dealer will no longer be able to open that network file. He will need to create a new network file, with the updated network information, using the updated access key.

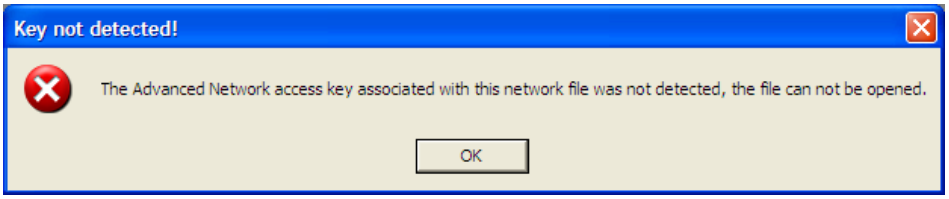

Figure 3.2-1 Trying to Open Network File without Proper Access key

3.2.5 Summary

The network information security described forms the foundation of the secure nature of the Advanced Network Key. It is only when the FPU system can keep information secure and up to date that it allows System Operators to feel comfortable with allowing field personnel more access to network information. The several layers of key detection mixed with encrypted data, enables the KPG-95DG FPU to secure network information, and increase the chances that only authorized personnel are able to use that information. Also, that they will only be able to change information that have been authorized to change.

3.3 Feature Set

This section will give a brief overview of some of the features of the Advanced Network Key.

3.3.1 System Operator

Most of the new functionality of the Advanced Network Key system will be only viewable by a System Operator. These functions are only visible if two conditions are met. First, the FPU must be operating under a System Operator Level software license ID and secondly, there must be a valid master key connected to the PC that matches the FPU software license ID. If one of these conditions is not met, the FPU will operate will whatever license level is currently set, with no access to Advanced Network Key features.

3.3.1.1 Advanced Network Key Management

The features available to the System Operator are basically divided into two areas, permissions and data. The permissions are fields that a dealer using that network information, contained on the access key, will be authorized to edit. The information contained in any field of the network information is visible by a user of the access key. However, only if System Operator has enabled the permission on the access key, will a user be able to actually change the value of the information. The data is the network information, for one network, currently defined in the System Operator's FPU.

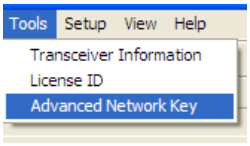

Figure 3.3-1 Advanced Network Key Menu Item

Below is a picture of one of the permissions screens. A check in the box next to the item, gives the access key user, permission to edit the function. No check means the user cannot edit the item (more on permissions in the programming access keys section). This window is accessed, by a menu option, only visible when the FPU is in master mode, "Tools->Advanced Network Key".

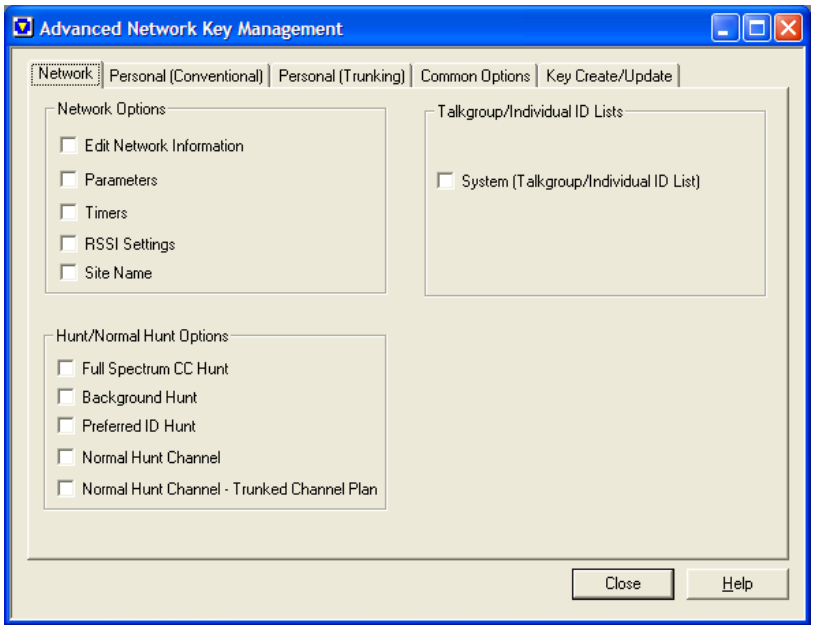

Figure 3.3-2 Example of Permissions Screen

The data portion of the System Operator feature set, allows the System Operator to select the network information and the software license ID of the user that the access key is being created for (more on creating keys in the programming access keys section). This screen is also only available when the FPU is in master mode.

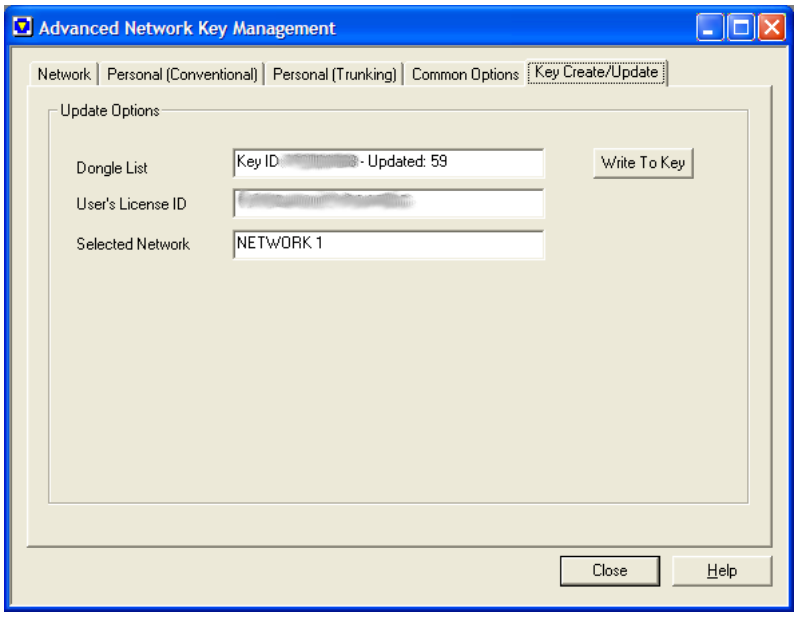

Figure 3.3-3 Example of Network Information Screen

3.3.2 Dealer

The visible differences in the Dealer software license ID are small, and also shared with the System Operator. When a Dealer enables the Advanced Network Key features, then connects an authorized access key, assigned to the same software license ID, to new menu options will be shown, in the "File" menu of the FPU. The "Load Network" and "Save Network" options will be shown, when these two conditions are met.

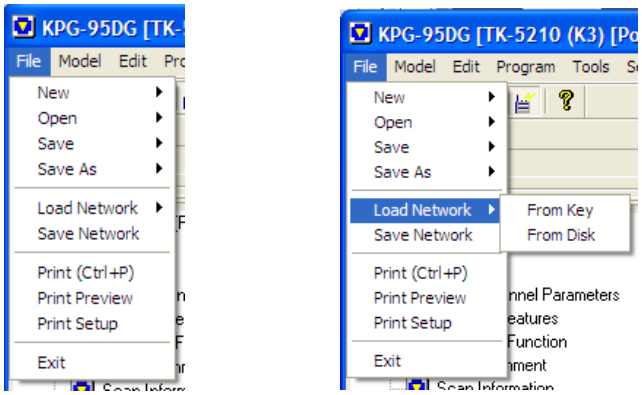

Figure 3.3-4 Load and Save Network Menus

Under the "Load Network" menu, the two additional menu options of "From Key" and "From Disk" appear. The "From Key" option will load network information, contained on an access key, into the network file of the FPU. The "From Disk" option will allow the user, to save network information in the network file, loaded from an access key, on to the local hard drive. This is useful to the user because, over time, the network information on the access key may change, this allows the user to save any

changed information, but leaves the access key in the same state as when received from the System Operator.

The “Save Network” option is used to save information, loaded from an access key, on to the hard drive of the PC.

4 Using the Advanced Network Key Features

In this section it will be explained how users actually make use of the additional features of the Advanced Network Key. There are four main parts that will be covered, creating the master keys, using the master keys, creating access keys and using access keys.

4.1 Creating Master Keys

Creating master keys for System Operators will be handled by KUSA R&D. This is the same as the current procedure when KUSA R&D creates the System Operator license ID and SKF file for the user. Initially, and until development can start on a Kenwood tool, the master keys will be generated using a development tool included in the manufacturer’s SDK package. There is a plan to develop a dedicated, Kenwood master key creation, application. During Phase 1, master keys will authorize one HSID, with a plan to offer multiple HSIDs in a future release.

4.2 Using Master Keys

Using a master key requires the fewest amount of steps. The System Operator simply installs KPG-95DG using the System Operator software license ID. Then after initially launching the FPU, navigate to the “Tools->License ID” menu option (show in Figure 3.1-1), enable the Advanced Network Key functions, connect the master key and restart the FPU.

4.3 Creating Access Keys

Probably the most complex task in using the Advanced Network Key features is the creating of the access keys. This requires not only sharing network information, but also setting permissions as to the data that will be editable by the user. This can bring about conflicts. Resolving those conflicts is beyond the scope of this document. However, in this section, the steps to create an access key will be described.

4.3.1 Generating Network Information

The first step in creating an access key is to use the FPU to set up the network information that will be written to the key. When the System Operator initially opens the “Network Information” section in the settings, a default network will be shown, with the specific HSID assigned to the master key filed in.

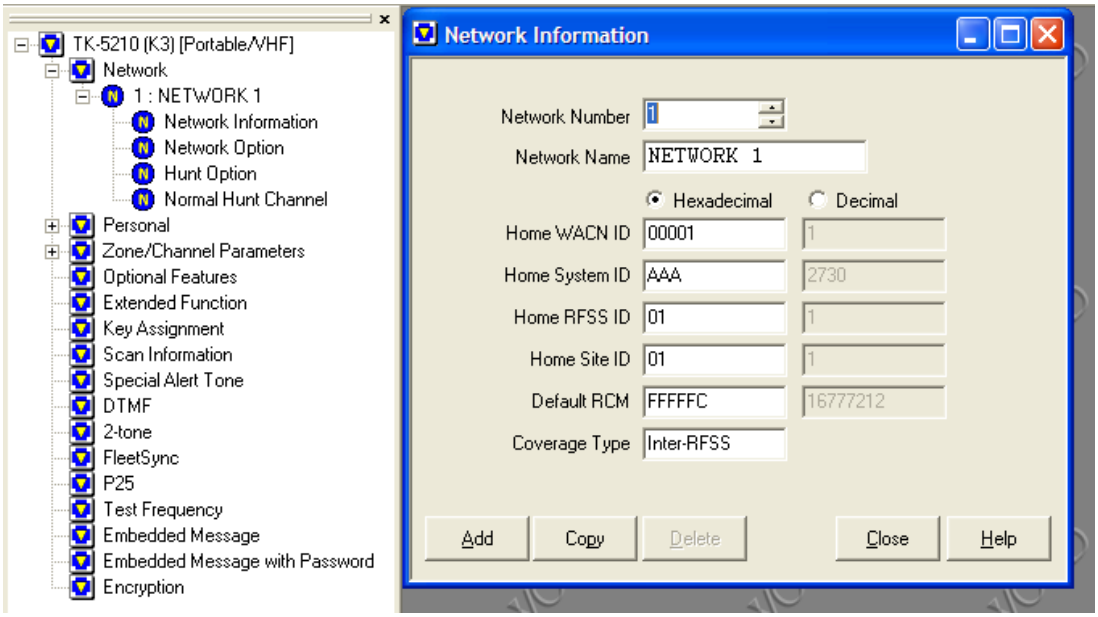

Figure 4.3-1 Initial Network Information Values

The System Operator can then choose to rename the network in a more descriptive manner and adjust any other parameters, as needed. The System Operator will continue this process on the remaining network information windows until the information has been configured as the System Operator requires for the access key user.

At this point it is important to remember that “Personality” data is not saved to the access key. However, if the System Operator wishes to restrict the access key to specific talkgroup IDs, a trunking system will need to be created, with the talkgroup values that should be used on the key. Again, only the talkgroup IDs contained in that system, are save to the access key. None of the other “System” data will be written.

4.3.2 Personality Information

If the System Operator wishes to include Personality data, such as encryption key lists or system data, a Personality file (.dat) will need to be created with the information, and given to the access key user separately. Only network data is saved to the access key. Any Personality data must be provided via a Personality file.

4.3.1 Selecting the Access Key

The Advanced Network Key features allows for multiple access keys to be detected by the FPU. Because of this, the before beginning the process of setting access key permissions, the System Operator must select which access key the permissions will be applied to, first. This selection is made in the using the “Dongle List” field in the “Key Create/Update” tab of the Advanced Network Key Management window.

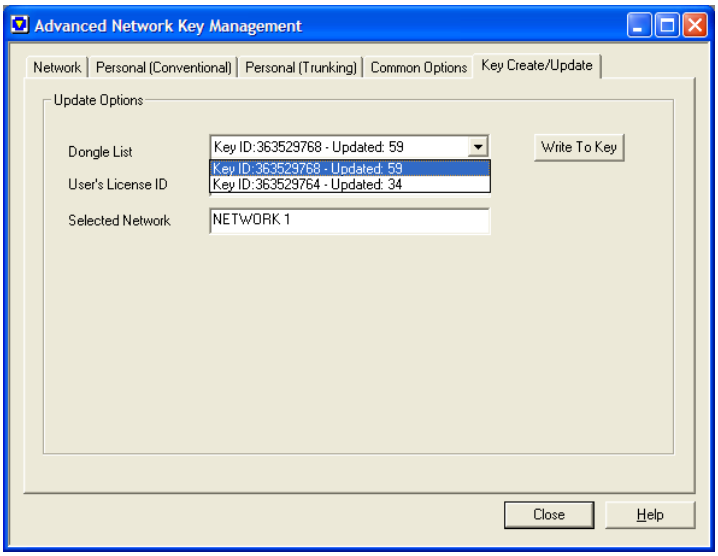

Figure 4.3-2 Selecting an Access Key

Selecting the access key to be written causes the information existing on the key, if any, to be displayed in the fields of the key management window. If the key is not selected first and values are set, when the desired key is selected, that key's information would be loaded and the previous changes discarded.

Now that the desired key has been selected, the user can move on to setting the access permissions for the key.

4.3.2 Access Key Permissions

Once the network information has been configured, the next step is to set the access permissions that will be assigned to the access key user. This assigning of permissions is handled in the "Advanced Network Key" configuration menu.

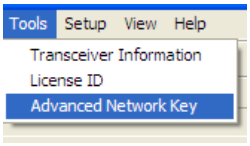

Figure 4.3-3 Advanced Network Key Menu Item

After selecting the menu item, the user will be presented with the "Advanced Network Key Management" window. If no programmable access keys are connected to the PC, all items in this window will be disabled. These values are based on what has been read, or what is to be written, to an access key. If no access key is connected, then there is no information to display or edit.

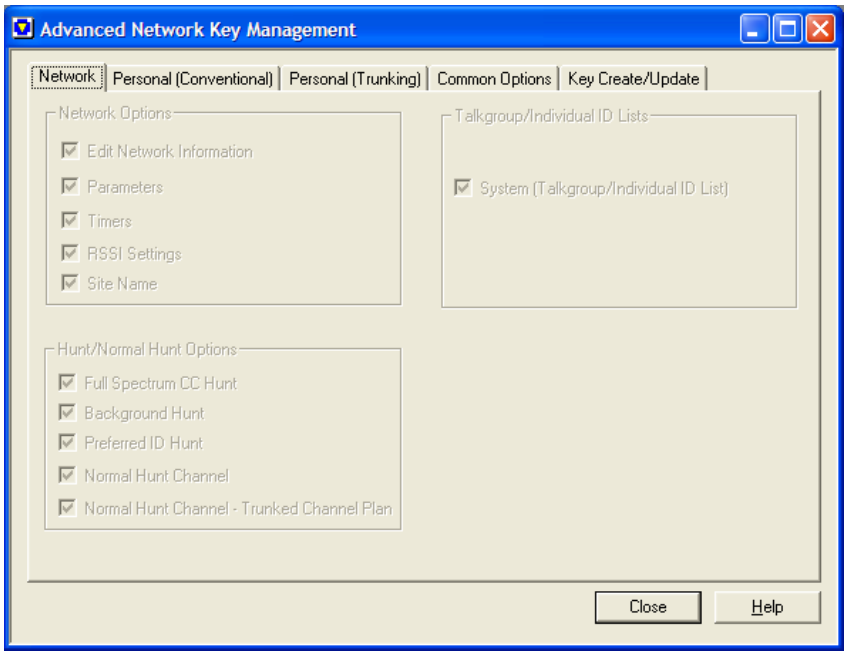

Figure 4.3-4 Advanced Network Key Management Window with No Access Key Connected

Once an access key is connected, the FPU will attempt to read any information that may have been written to the key previously and will enable the fields for editing.

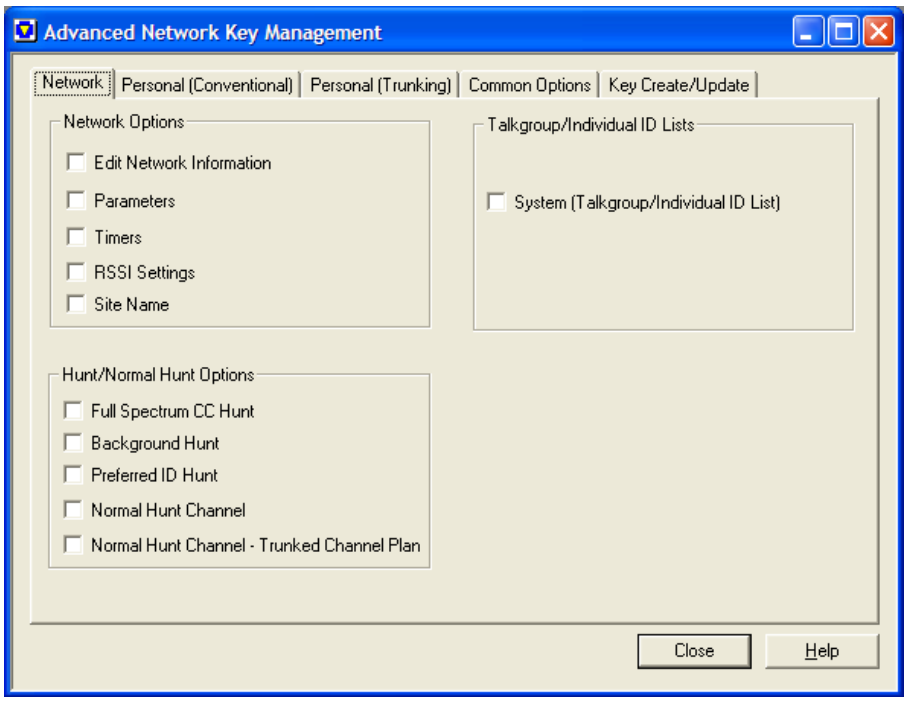

Figure 4.3-5 Network Key Management Window with Access Key Connected

The tabs and fields of the Advanced Network Key Management window, correspond to the various configuration screens in the FPU itself. On the “Network” tab, we can see that there are checkboxes that

correspond with each screen in the "Network" configuration screens. Placing a check next to a particular option will give the user of the access key permissions to edit those fields when using the access key.

For example:

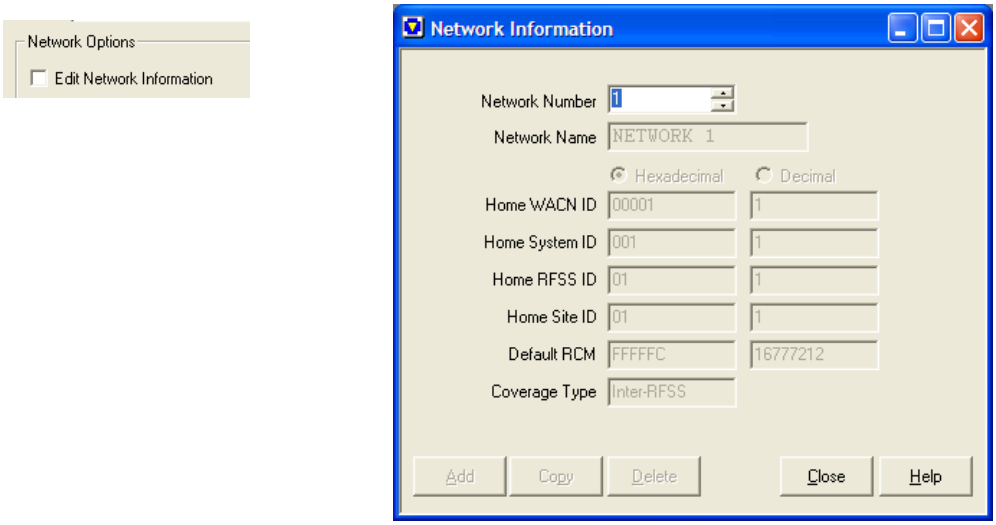

Figure 4.3-6 Edit Network Information Permission Disabled

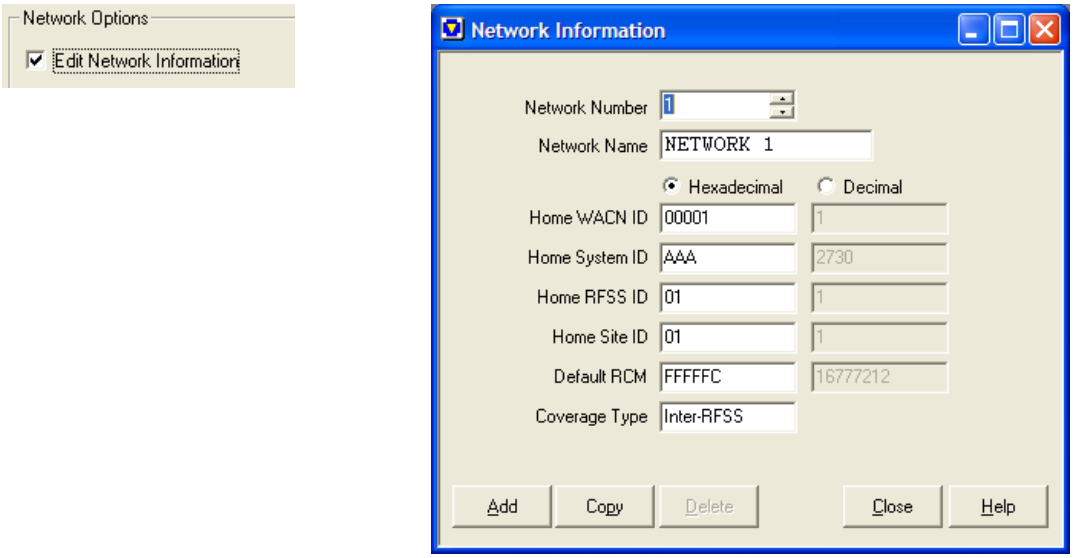

Figure 4.3-7 Edit Network Information Permission Enabled

As can be seen from figures 4.3-5 and 4.3-6, enabling or disabling a feature's permission, enables or disables that entire configuration screen for the user of the access key.

An important note about access permissions, if a user connects multiple access keys to the computer, the permissions assigned will be a sum of all the access keys connected. For example, if a user connects

two access keys to his computer and one access key allows the editing of network information and one does not, then the sum of the two permissions will not allow the user to edit network information. In this way, System Operator should be very careful when assigning permissions to access key users, and make sure that there is good reason for restricting access to any programming functions, outside of network information.

4.3.3 Writing to an Access Key

Once the two steps of configuring the network information and the data access permissions have been completed, the information is ready to be written to the access key. The System Operator, at this point, will click on the "Key Create/Update" tab, in the Advanced Network Key Management window. After clicking, the System Operator will be presented with a screen, displaying three fields of data.

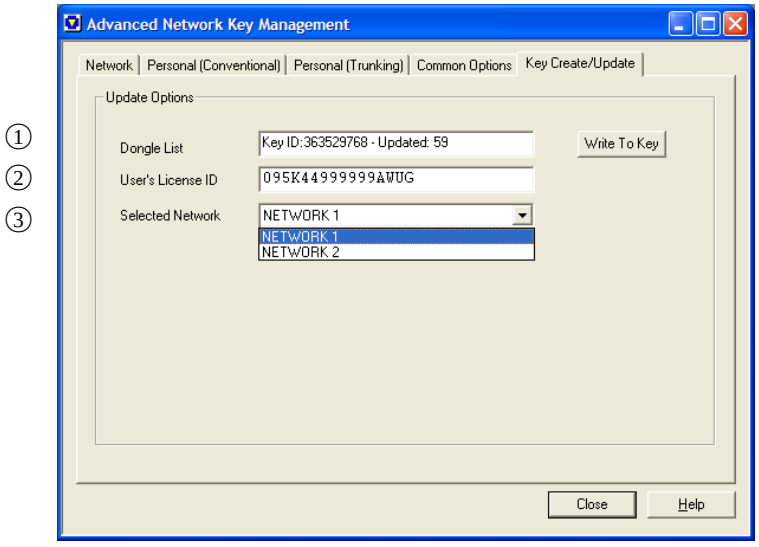

Figure 4.3-8 Key Create/Update Tab

The first field will allow the system operator to select which access key the information will be written two. If multiple access keys are connected to the PC, the user will be able to select from the writable access keys detected. The desired key to be created should have been selected before this point to ensure that any permissions set are not lost (see section 4.3.1 about selecting the access key).

The second field is where the System Operator will enter the software license ID of the Dealer or System Operator that will be using the access key. The access key will only function properly as an access key, if the license ID written to the key matches the license ID of the person using it.

The third field is where the System Operator will select which network information will be written to the key. If only one network is defined in the network file, it will be the only choice. If multiple networks are defined the user must select which network will be written. Only networks that the System Operator is authorized to distribute (the HSID the System Operator's own system), will appear in this list. A System Operator cannot create an access key for a network that is not authorized by his master key.

After the information is entered into these fields, the user can then click the "Write To Key" button. When click the "Write To Key" button the FPU will confirm that the license ID entered is valid and, if the license ID is a System Operator level, it will ask the user to confirm that they have entered the value in the field that they wish to be written to the key.

After the license ID has been validated, the user will be presented with the "Write To Key" dialog box.

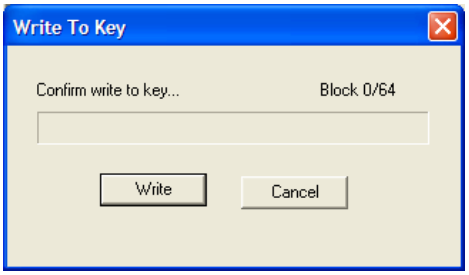

Figure 4.3-9 Write to Key Dialog

At this point, the user can click the "Write" button, to begin programming the access key or, click the "Cancel" button to exit the writing operation, and return to the Advanced Network Key Management window.

4.4 Using Access Keys

When a Dealer or System Operator receives an access key, they must verify that they are using a version of KPG-95DG that supports the Advanced Network Key features, add that the features have been enabled. If those two conditions are met, then the user can make use of the Advanced Network Key features and the access key information given to them.

4.4.1 Loading Network Information

The first step in using the information contained on an access key is to load that information into the network list of the FPU. To load the network information from the access key the user will navigate to the "Load Network->From Key" menu item, under the "File" menu.

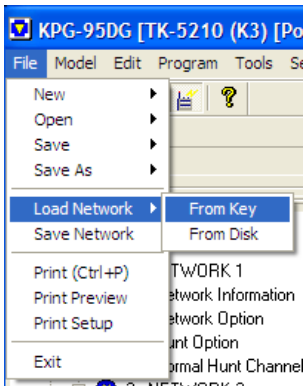

Figure 4.3-1 Loading Network from Access Key

After selecting the menu item, the user will be shown a dialog box that will allow the user to select the access key that he wants to load data from.

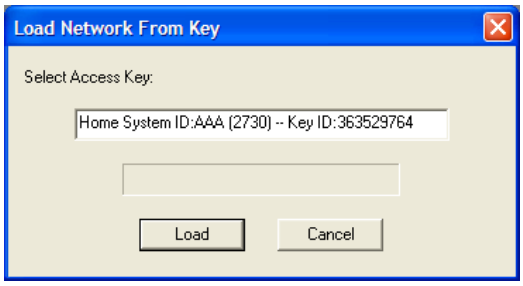

Figure 4.3-2 Selecting Access Key to Load Information From

If multiple access keys are attached, the user may click the field and a drop-down list of all the currently connected, valid keys, which the user can select from.

After selecting the key, the user can choose to push the “Load” button, to import that information into their current network information. Or, they may choose to cancel the operation by clicking the “Cancel” button.

After clicking the “Load” button, the user will be shown a warning that the information will be added to the network list, and ask the user to confirm this action. If only one network is currently defined, the FPU will ask if the user would like to have that information over written by the information from the access key. This question is asked because if the one defined network is just the default network; the user may not have permission to delete the entry from the network list, so they would prefer to overwrite it. If they choose not to overwrite it, the network information from the key will be appended to the network list as network number 2.

Once the information is loaded successfully, the user may continue with programming of FPU functions, according to the permissions set by the key.

4.4.2 Saving Network Information

Saving network information can be accomplished in two different ways, one method is optional, and the other is not. The optional method is to use the “Save Network” menu item, under the “File” menu. The non-optional method is when the network file gets saved as a part of writing information to a radio, or saving a personality file. This section describes the difference between the two.

4.4.2.1 Using the Save Network Function

Using the “Save Network” option in the file menu, will take network information that was imported from an access key into the network list, and save that information to the PC’s hard drive. The information saved only contains the network information, basically the same information that is on the access key, it is not an entire FPU network file. This function is useful because if a user has permissions to edit the network information, loaded from an access key, they may want to save the changes to that network information so that they will not have to make the same changes each time they add the information to the network list. In this situation, the user would select the “Load Network->From Disk” option under the file menu, instead of the “Load Network->From Key” option, to load this edited data into the network list.

Choosing the “Save Network” menu item will cause a file dialog to be shown, allowing the user to select the file name and location for the saved data. The default extension for these network information files is (.ank). These files can only be opened by the FPU if the Advanced Network Key features are enabled and the key that the network information was initially loaded from is connected to the PC, and has not been updated since the file was created.

4.4.2.2 Saving FPU Network Files

Before writing data a radio or, when saving a personality file, the FPU requires that a network file be saved to the user’s local disk. However, if the FPU is operating with a Dealer level software license ID, saving a network file is not an option available to the user from the file menu. The FPU does allow saving of a network file if the data being written to a radio contains trunking information and also when the user attempts to save a personality file that contains trunking information.

If one of these situations occurs, the FPU will allow the user to save the network file. But, if the file contains information loaded from an access key, the information written to the disk, will be encrypted. This file will only be able to be decrypted if the actual dongle that was used to encrypt the information is connected to the PC, and that key has not been updated since the file was created.

4.4.3 Reading/Writing Radios

As discussed in the previous section, when writing data that contains trunking information to the radio, the user will be prompted to save the network file before writing. That saved file will require that the dongle used to encrypt the file, be connected to the PC, to load that file at a later time. Reading from a radio, that contains network information loaded from an access key, will also require that the access

keys that were used to create the network information, be connected to the PC to allow the radio network information to be read. If more than one access key was used to program the radio, all access keys that supplied information to the radio, must be connected before the radio can be read.