Tactical Key Management Device (TKMD)

May 31, 2018

Introduction: The Tactical Key Management Device (TKMD) is a multi-purpose implementation of Project 25 Over-the-Air Rekey (OTAR) intended for both stand-alone and networked radio systems. In the FIPS mode the, TKMD complies with the Federal Information Processing Standard (FIPS 140-2) at Assurance Level 3. In a network application, multiple TKMDs each are connected to individual nodes (Base Stations or interconnected groups of Base Stations). The Internet Protocol connections between TKMDs are used to provide updates as needed to the status of individual OTAR Subscriber Radio Units to the network participants. The network IP connection can also be used to distribute new cryptographic key material to the participant TKMDs for redistribution to the appropriate Subscriber Radio Units.

TKMD Exterior View

TKMD Operating Modes: The TKMD can function in the following Modes:

1. **OTAR KMF** The TKMD can operate as a Key Management Facility (KMF) for a stand-alone or networked Project 25 OTAR System.
2. **OTAR Subscriber Unit** The TKMD can participate as a Project 25 OTAR Subscriber Unit and interact with another Key Management Facility to receive Key Material from that KMF. If desired, that Key Material can be redistributed to other Subscriber Units while the TKMD is operating as the OTAR KMF.
3. **Key Fill Receive** The TKMD can operate as a Subscriber Unit and receive Key Material from Project 25-compliant Key Fill Device (KFD).

4. **Key Fill Device** The TKMD can act as a Key Fill Device for any Project 25-compliant Subscriber Unit.

Base Station Options: The TKMD can utilize the following Radio RF resources (Base Stations or Network) for OTAR KMF or OTAR Subscriber Unit operations:

1. **V.24 Equipment** The TKMD has the capability to operate with Motorola Conventional Astro Equipment with a V.24 interface. This includes the Quantar™, GTR-8000™ (with optional V.24 interface), ATAC-3000™, PDR-3500™, or DIU-3000™. The TKMD is also capable of operating with the TXM-2000™ using the Asynchronous HDLC option.
2. **DFSI Version 2 Equipment** The TKMD can operate over Internet Protocol with equipment compatible with the TIA Project 25 Digital Fixed Station Interface (DFSI) Version 2 (TIA 102-BAHA-A). This includes Project 25 equipment manufactured by Codan and ICOM (Eclipse). The TKMD will also interoperate with a Christine Wireless, Inc. RIC-M using DFSI Version 2 which allows IP connection to V.24-capable equipment not collocated with the TKMD.
3. **Portable Radio** The TKMD has a Serial Line Interface (SLIP) port for use with a compatible Portable Radio.

Stand-Alone Operation: In the KMF mode the TKMD can support up to 500 (optionally expandable to 3000) Subscriber Units with OTAR in a small regional or "campus" type environment.

The TKMD can be directly or indirectly connected to the RF Resource(s). In this case, Key Material can be entered from a Key Fill Device (KFD) or via a file upload one or more encrypted Key Kettle Files. Subscriber assignments can be done manually or by upload of encrypted Subscriber Files.

Once configured, the TKMD can operate autonomously and will interact with OTAR Subscriber Units. When a Subscriber Unit attempts to register on the OTAR data network, the TKMD will provide any new or previously unsent Key Material that is assigned to the Subscriber Unit.

The TKMD Key Fill Device function can be used to load the initial Key Material into each Subscriber Unit.

Network Operation: Distributed verses Centralized: In a traditional OTAR System, a central KMF services all radios in the system and hence requires full time data connectivity to all RF Resources in the system. For a large system with potentially 10's of thousands of Subscriber Units, maintaining this connectivity as well as being able to have adequate KMF resources to handle multiple simultaneous Subscriber Unit OTAR operations can be challenging and result in frequently failed or delayed OTAR operations.

The TKMD in a network environment is a distributed OTAR System where each of the distributed TKMDs support only the Subscriber Units in range of the connected RF Resource. Connectivity to the IP Network is not required for basic OTAR operation. Connectivity to the IP network is only required to import new Key Kettle Files (when the Key Material is updated), to share the encrypted updated Subscriber Unit Files after OTAR operations (if enabled) or to request the Subscriber File from the network if an unknown Subscriber Unit attempts to perform an OTAR Registration on the local node.

TKMD Setup and Monitoring: The TKMD has a built-in Internet Protocol web server operating in https mode (TLSv1.2 AES-256 Encryption, Diffie-Helman Ephemeral Key Establishment). After initial log on the Crypto Officer is required to establish a unique User Name and strong User Password before commissioning the TKMD and loading Subscriber Unit and Key Material information.

After Subscriber Unit and Key Material are established by the Crypto Officer, the TKMD can be left to run in KMF autonomous mode without the PC connected. Subsequent import of updated or requested encrypted Subscriber Unit files or encrypted Key Kettle files can be enabled to occur autonomously once the base transport encryption key used for the derivation of the file name-specific transport encryption key is loaded by the Crypto Officer.

Autonomous KMF Operation: In the autonomous KMF mode of operation, when Subscriber Unit attempts to OTAR Data Register on the OTAR network the Subscriber Unit record will be searched for in the internal TKMD encrypted non-volatile memory. If the record is found, it will be decrypted and any outstanding OTAR operation including sending newly updated Key Material will be performed. If the Subscriber Unit record is not found and the TKMD is enabled for file sharing, an inquiry will be sent to the network requesting the encrypted file for the Subscriber Unit. If the file for the Subscriber Unit is found on one of the network participants, in a few seconds it will be sent to the requesting TKMD which will decrypt the file and perform any indicated OTAR operations on the Subscriber Unit.

If Subscriber File Sharing is enabled, each time an OTAR Subscriber Unit is updated, a copy of the Subscriber File is encrypted and sent to each IP address on the File Share Transmit list via a further encrypted TLSv1.2 connection. When the TKMD receives a shared file, it will decrypt the file, check if the Subscriber unit is in its local data base and if it is, will update the Subscriber Unit file to reflect any new information contained in the received file. Optionally, if the Subscriber Unit is not in the local data base, it can be added. This feature is primarily for smaller systems where the total number of subscribers is not large.

TKMD Packaging The TKMD is a single Printed Circuit Board housed in an aluminum case 6.5” wide, 6.5” deep and 2.25” high. All User connections are located on the front panel of the unit. The majority of the TKMD case has been potted with hard black epoxy to meet FIPS 140-2 Assurance Level 3 requirements. A backup rechargeable battery in located at the rear of the epoxy potting to power the volatile memory storage of Cryptographic variables when there is no power applied to the TKMD. Disconnection of the backup battery and removal of the main power will cause erasure of all Cryptographic variables from the TKMD.

TKMD Backup Battery and Extent of Epoxy Potting

The front panel of the TKMD shown below has the following User connections:

1. 2.0 mm 12 VDC input power jack
2. Ethernet connection for https web connection and shared with UDP Base Station/network connection
3. USB connector for debug monitor
4. 4 Light Emitting Diode (LED) status indicators
5. RS-232 for debug monitoring or SLIP Base Station connection
6. V.24 connector for use with RF Resources with compatible connections
7. 6 Pin Hirosi connector for KFD or Subscriber Unit key fill use
8. Zeroize switch to erase cryptographic variables stored in volatile memory

TKMD Front Panel

TKMD File Sharing: If the feature is enable, the TKMD can securely share encrypted files (Subscriber Unit configuration or Key Kettle) files with networked TKMDs or a network server. Permission to use this feature and the recipients (IP address) are established by the Crypto Officer. The individual files are encrypted by an AES-256 key derived from the Base Transport Key, the file name and a nonce specific to the file type. Thus, each file is encrypted with a file-unique key. The Base Transport Key must be loaded into the TKMD by the Crypto Officer.

When a file is to be shared, a new TLSv1.2 connection is established with the remote unit/server (TLSv1.2 AES-256 Encryption, Diffie-Helman Ephemeral Key Establishment). The encrypted file is then sent. At the receiving end, the file is decrypted from the TLSv1.2 connection encryption, decrypted from the derived Transport Key Encryption (AES-256 Key Wrap File Encryption) and encrypted with the unique Storage Key (AES-256 Key Wrap File Encryption) at the receiving end prior to storage in non-volatile memory. In the case of the receiving end being a file server, there is no need to decrypt the transport encryption key wrap since the file can simply be stored as received with the file name for serving at a later time if that file name is requested by a TKMD. Only the latest version of a given file name are stored on the server.

The Subscriber Unit File contains a complete image of the information needed to support a Subscriber Unit including up to 40 keys.

Each Key Kettle File contains all Key Material and metadata for up to 40 keys. Keys in the Key Kettle are cross reference to Subscriber Unit assigned keys. If new key Material is found in a Key Kettle file, each reference to that key in the Subscriber Unit records will be automatically updated and the key will be flagged to be sent to the Subscriber unit on the next OTAR opportunity.

Firmware update: The TKMD is an infinite loop "bare metal" processor with no operating system. Firmware update is accomplished by uploading a hex file of the entire program space image over a TLSv1.2 secure connection. Only an authenticated Crypto Officer can upload new firmware. When the image is uploaded the TKMD calculates the Message Digest for the image (SHA-2 HMAC). The Crypto Officer must upload the correct Message Digest before the stored firmware image will be transferred to the TKMD processor program memory. This process ensures that the firmware image is correct and that it comes from an authorized source due to the need to have the HMAC key used to verify the firmware image.

TKMD Configuration Setup

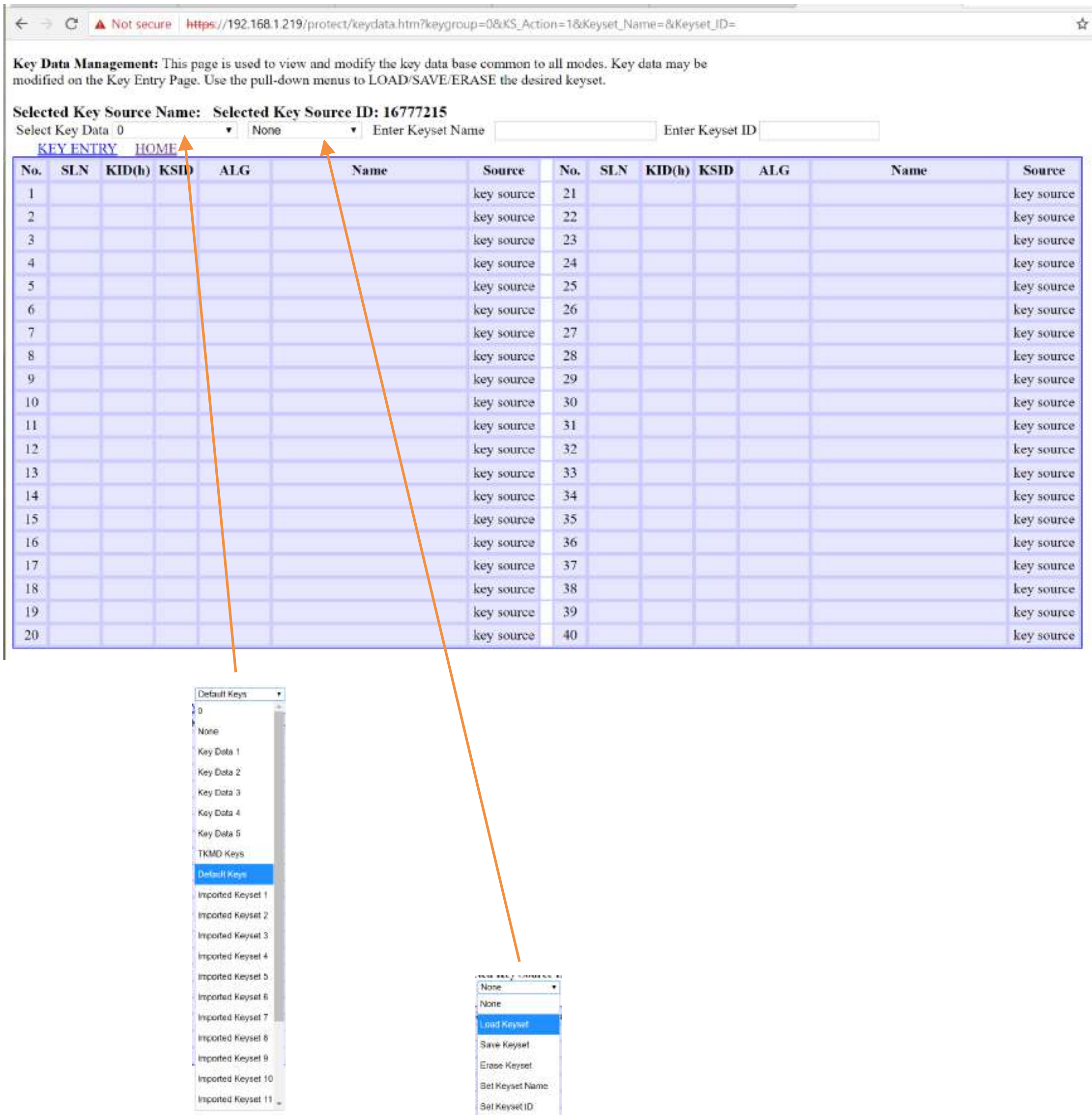
The following sections give brief description of the setup of the various features of the TKMD via the secure TLSv1.2 (https) web page interface.

Web Page Access: The default IP address for the TKMD is 192.168.1.204. In a web browser (Google Chrome is the recommended web browser-make sure that you have a recently updated version of Chrome) enter https://192.168.1.204 in the browser address box. Chrome will attempt to connect and will produce a security warning because the TKMD uses a self-signed X.509 certificate that the browser cannot verify with a Certificate Authority. Click the Advanced hypertext and click go to the site anyway. The browser will open a warning page with DHS language warning against accessing the site if not authorized to do so.

At the bottom of the warning web page, click Logon which will produce a window for the user name and password. The default user name is "admin" and the default password is "tkmdboard". In production versions of the TKMD, it will be necessary to change the User Name and User Password to gain access to the TKMD setup web pages. For the production version of the TKMD, the User Password is required to meet the DHS requirements for a strong password.

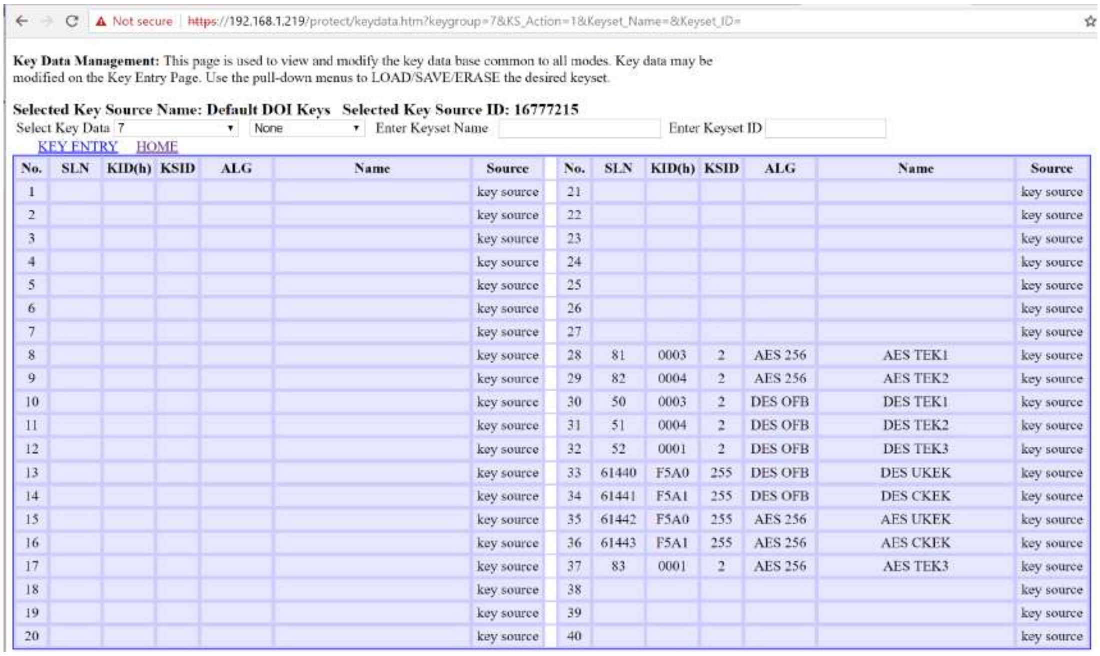
After Login is accepted the browser will go to the Board Configuration web page. If a new User Name and User Password is required (first login on Production TKMD) it will not be possible to access any other configuration web page without successfully entering the new credentials.

Key Data Selection; Use the web page navigation buttons on the web page to access the Key Data web page shown below.



No.	SLN	KID(h)	KSID	ALG	Name	Source	No.	SLN	KID(h)	KSID	ALG	Name	Source
1						key source	21						key source
2						key source	22						key source
3						key source	23						key source
4						key source	24						key source
5						key source	25						key source
6						key source	26						key source
7						key source	27						key source
8						key source	28						key source
9						key source	29						key source
10						key source	30						key source
11						key source	31						key source
12						key source	32						key source
13						key source	33						key source
14						key source	34						key source
15						key source	35						key source
16						key source	36						key source
17						key source	37						key source
18						key source	38						key source
19						key source	39						key source
20						key source	40						key source

Use the Select Key Data pulldown menu to select a source key set and the adjacent pulldown menu to load the keyset. The above selection of Default Keys and Load Keyset produces the following Key Data web page.



https://192.168.1.219/protect/keydata.htm?keygroup=7&KS_Action=1&Keyset_Name=&Keyset_ID=

Key Data Management: This page is used to view and modify the key data base common to all modes. Key data may be modified on the Key Entry Page. Use the pull-down menus to LOAD/SAVE/ERASE the desired keyset.

Selected Key Source Name: Default DOI Keys   Selected Key Source ID: 16777215

Select Key Data 7 | None | Enter Keyset Name | Enter Keyset ID

KEY ENTRY   HOME

No.	SLN	KID(h)	KSID	ALG	Name	Source	No.	SLN	KID(h)	KSID	ALG	Name	Source
1						key source	21						key source
2						key source	22						key source
3						key source	23						key source
4						key source	24						key source
5						key source	25						key source
6						key source	26						key source
7						key source	27						key source
8						key source	28	81	0003	2	AES 256	AES TEK1	key source
9						key source	29	82	0004	2	AES 256	AES TEK2	key source
10						key source	30	50	0003	2	DES OFB	DES TEK1	key source
11						key source	31	51	0004	2	DES OFB	DES TEK2	key source
12						key source	32	52	0001	2	DES OFB	DES TEK3	key source
13						key source	33	61440	F5A0	255	DES OFB	DES UKEK	key source
14						key source	34	61441	F5A1	255	DES OFB	DES CKEK	key source
15						key source	35	61442	F5A0	255	AES 256	AES UKEK	key source
16						key source	36	61443	F5A1	255	AES 256	AES CKEK	key source
17						key source	37	83	0001	2	AES 256	AES TEK3	key source
18						key source	38						key source
19						key source	39						key source
20						key source	40						key source

There are 3 DES TEKs, 3 AES TEKs, 2 DES KEKs and 2 AES KEKs in the Default keyset.

Once the Keyset has been selected, it is available for assignment to Subscriber Units on the Client Configuration web page as discussed later in this document.

Local Keysets The Key Data web page can also be used to select one of up to 5 sets of Local Keys. Local Keysets can be manually created and saved on the Key Entry web page.

TKMD Keys The Key Data web page can be used to load Keys that have been entered into the TKMD from a KFD or from participation in an OTAR network while acting as a Subscriber Unit.

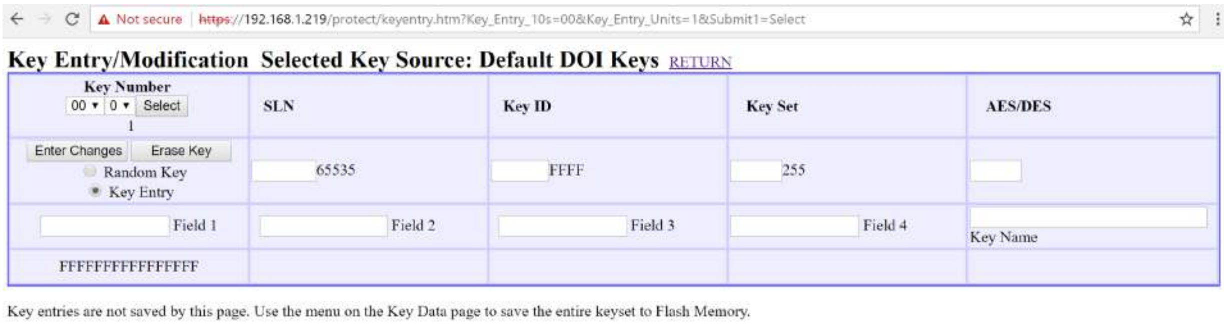
Imported Keysets The Key web page can be used to select one of up to 16 Key Kettle Files that have been uploaded into the TKMD from a secure network connection.

Keyset Name The Enter Keyset Name is used along with the pulldown menu to the left of the entry box to establish a name for the keyset (except for Default and TKMD keysets which are fixed-named).

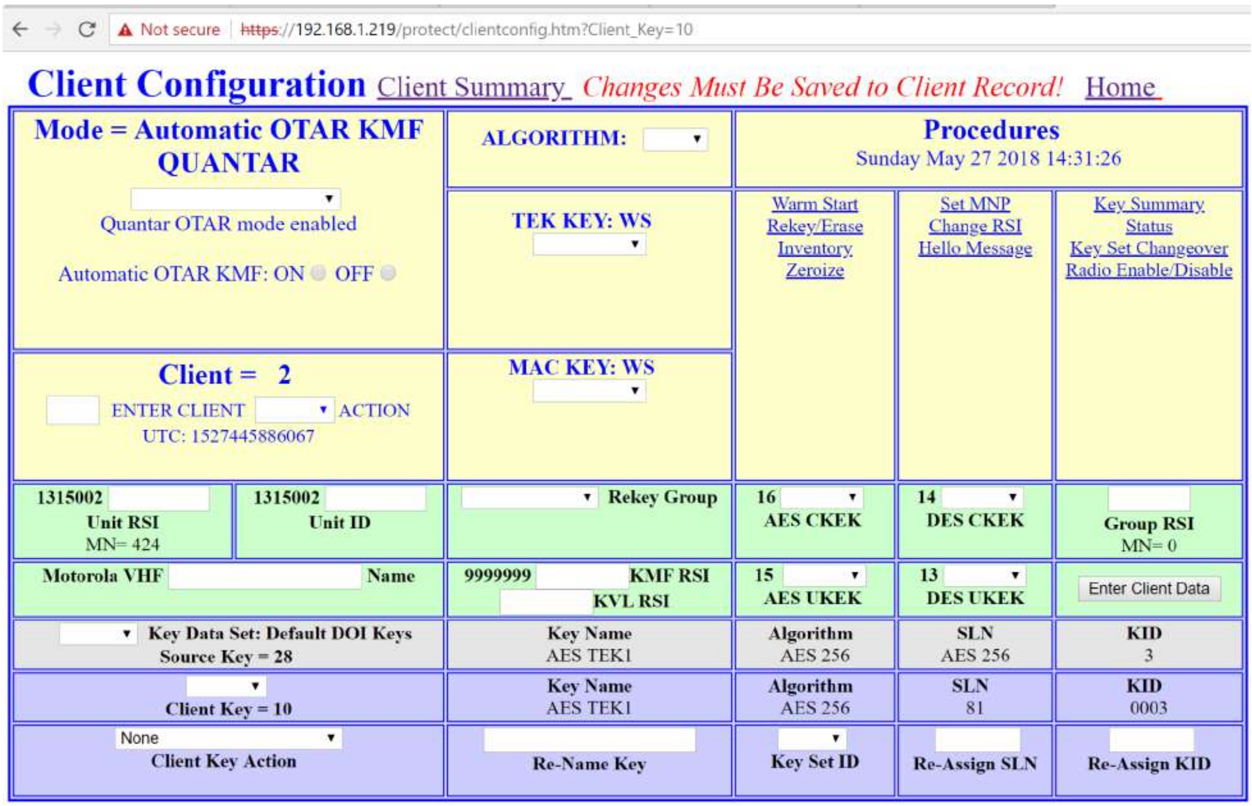
Keyset ID The Enter Keyset ID box and the action pulldown menu are used to establish a Keyset ID which is used to cross reference keys to a keyset. This cross reference allows the TKMD to recognize when a Subscriber Unit key needs to be updated due to receipt of an Imported Keyset with the same Keyset ID reference.

Keyset Erase/Save The action pulldown menu can also be used to save or to erase a selected keyset.

Key Entry: The Key Entry web page is accessed by clicking the Key Entry blue hypertext at the top of the Key Data Web Page. This page allows creation of Local keys manually and selective modification of Imported keys.



Client Configuration Web Page: The most important web page on the TKMD is the Client Configuration web page. A typical view of this web page is shown below.

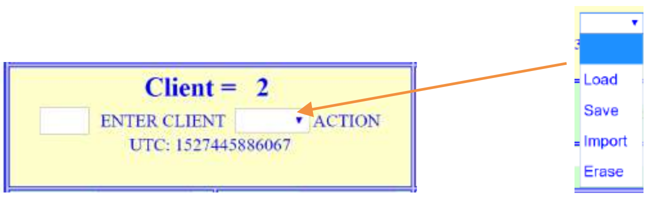


The yellow background blocks are to setup OTAR/Key Fill operations and to select the Client (Subscriber Unit). The green background blocks are to setup the specific Client. The grey background blocks are to select a source key (the source Keyset is selected on the Key Data web page). The blue background blocks are to assign the source key to the Client and to modify the key attributes if desired. At the top of the Client Configuration is a hypertext field to move to the Client Summary web page and a hypertext field to move to the Home web page.

TKMD Operating Mode The Crypto Officer has the option of manually setting the Operational Mode for the TKMD from the pulldown menu on the upper left hand corner of the yellow background section of the Client Configuration web page.

If Automatic OTAR KMF is desired, click the button for ON and then select one of the three options for OTAR KMF. If the TKMD is to be left in Automatic OTAR KMF (the normal unattended state for the TKMD) select the KMF Mode and Auto OTAR "ON" on the Board Configuration page (enter and save is required for this page).

Client Selection Use the second block on the left side of the yellow background section of the Client Configuration web page to select the Client (Subscriber Unit) to be viewed.



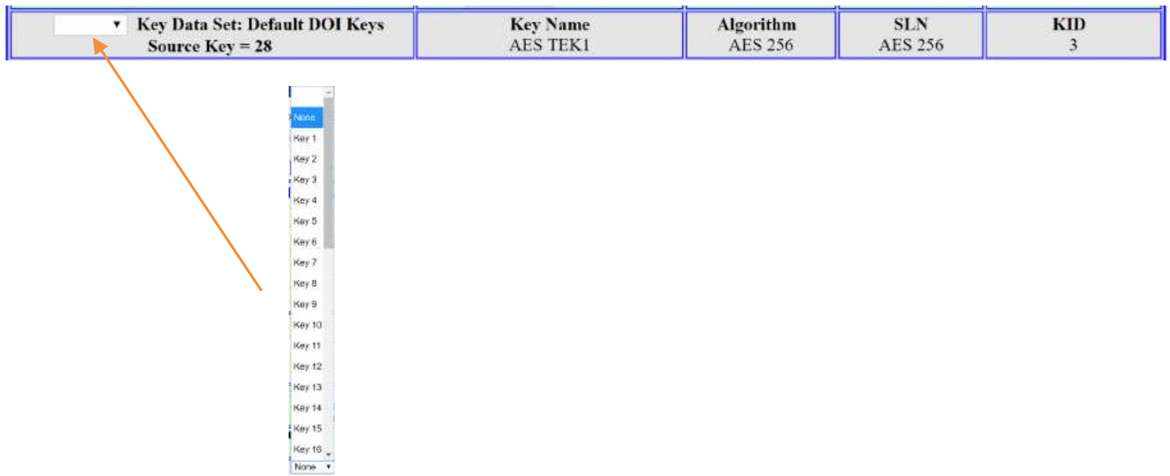
The balance of the yellow background section is for configuring manual OTAR/ key fill operations and viewing the resultant changes in the Client status. These will be discussed in later sections of this document.

Individual Client Configuration The green background blocks on the Client Configuration web page are used to setup, view and modify parameters for the selected individual Client.

> **Unit RSI** The RSI (Radio Set Identifier) is the OTAR identity of the individual Client. The RSI is only used in OTAR and key fill operations and is often set to be the same as the Unit ID, though the two parameters need not be the same. The Unit RSI in the TKMD is entered as a decimal number between 1 and 9,999,999. This block also shows the current Message Number for the selected Client. Message numbers are used in Project 25 OTAR to mitigate against replay attacks.
>
> **Unit ID** The Unit ID is the RF Identification Number used by the Client over-the-air.
>
> **Name** The Name field is provide to assist the Crypto Officer in keeping track of the individual Clients.
>
> **Rekey Group** This block is used to associate the Client with a Rekey Group (11 Rekey Groups are supported by the TKMD) for Group OTAR operations. This will be discussed more in later sections.
>
> **KMF RSI/KVL RSI** These entries are used to set the RSI used by the Client for OTAR and for KFD (key fill) operations.
>
> **KEK Identification** The following 4 blocks are used to identify which Key Encryption Key is used for Individual OTAR (UKEK) and Group OTAR (CKEK) for the AES and DES algorithms. Once KEKs have been assigned to the Client, only keys with the appropriate algorithm and keyset (255) will be displayed in the respective pulldown menus. These identifications are used to assist the TKMD in the use of an appropriate key for encrypting key material during OTAR operations.
>
> **Group RSI** This block is used to enter the RSI used by the Client for Group OTAR operations. The block also displays the Message Number for Group OTAR operations for the OTAR Group.

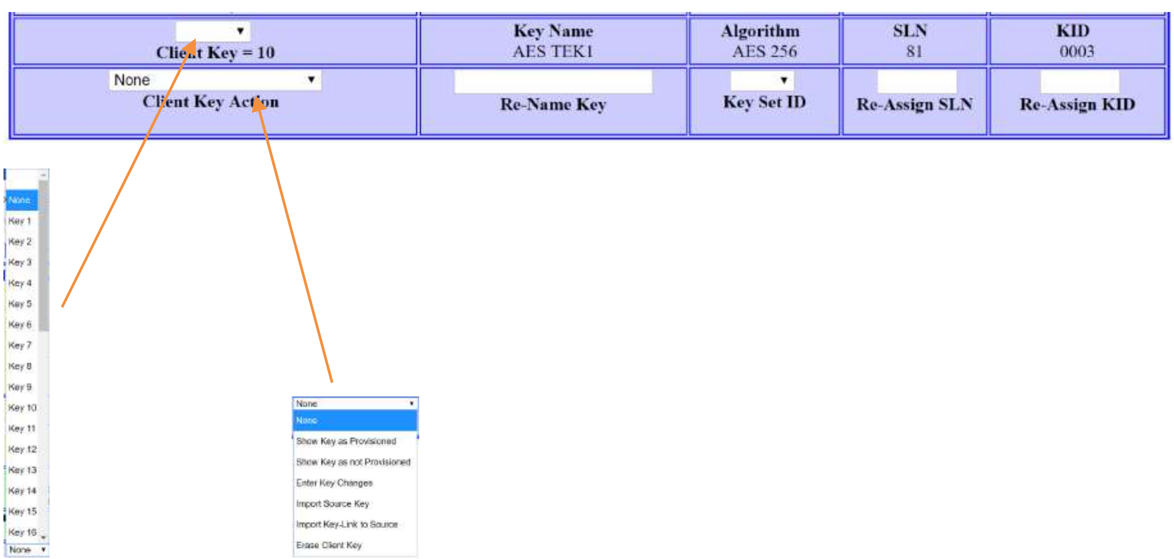
Enter Client Data This button is used to enter (Save) any entries made to the above settings.

Source Key Selection The grey background blocks are to select the Source key from the Key Data Set and to view the key parameters. The Key Data Source is selected on the Key Data web page.



The Key Name, Algorithm Storage Location Number (SLN) and Key Identification (KID) parameters will be displayed for the selected key.

Client Key Selection The blue background blocks are used to select, view and modify the Source key for use in the Client assigned keys.

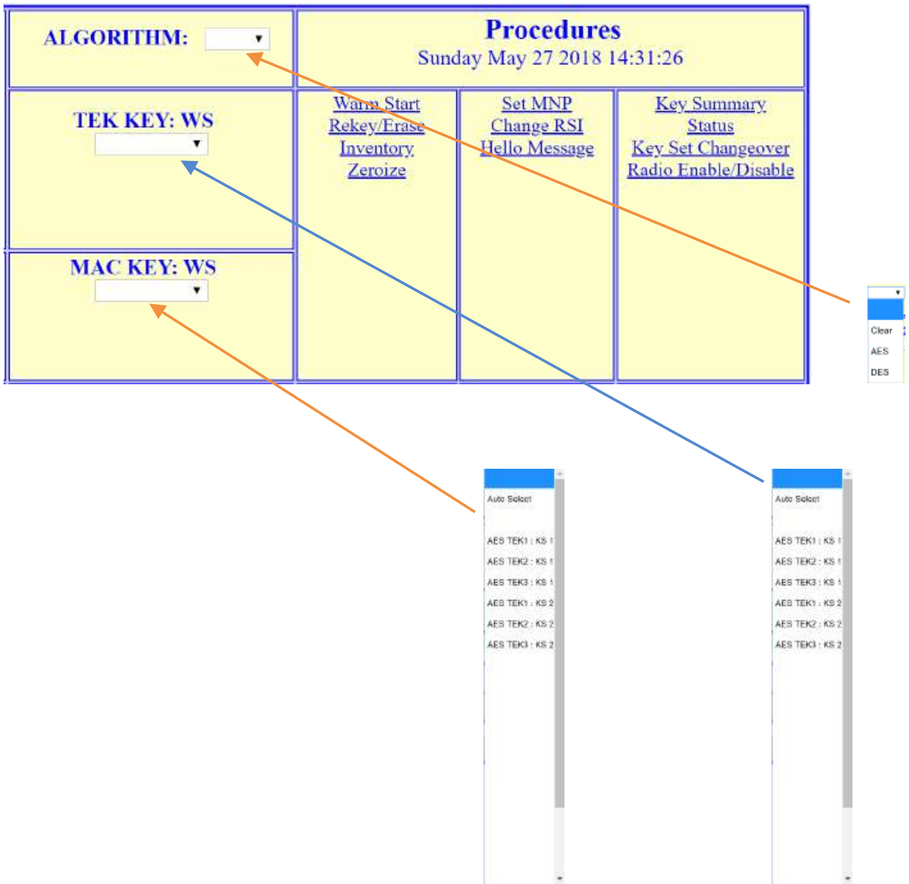


The Client Key Action pulldown menu is used to execute the desired action on the Selected Source key for the Selected Client target key location. If changes are desired for the Key Name, Key Set ID, SLN or KID, the changes can be entered in the appropriate entry block and they will be saved to the Client Selected target key location.

The current Client assigned keys can be viewed by selecting Key Summary under the Procedures yellow background section of the Client Configuration web page. This will open a new window in the browser with the currently assigned keys. The keys are color coded with Black: Assigned, Red: Assigned but Zeroized and Green: Assigned and confirmed loaded in the Client.

Key Number	ALG	Keyset No.	SLN	Key ID	Key Name
Key #1	DES OFB	1	50	0003	DES TEK1
Key #2	DES OFB	1	51	0004	DES TEK2
Key #3	DES OFB	1	52	0001	DES TEK3
Key #4	AES 256	1	81	0003	AES TEK1
Key #5	AES 256	1	82	0004	AES TEK2
Key #6	AES 256	1	83	0001	AES TEK3
Key #7	DES OFB	2	50	0003	DES TEK1
Key #8	DES OFB	2	51	0004	DES TEK2
Key #9	DES OFB	2	52	0001	DES TEK3
Key #10	AES 256	2	81	0003	AES TEK1
Key #11	AES 256	2	82	0004	AES TEK2
Key #12	AES 256	2	83	0001	AES TEK3
Key #13	DES OFB	255	61440	F5A0	DES UKEK
Key #14	DES OFB	255	61441	F5A1	DES CKEK
Key #15	AES 256	255	61442	F5A0	AES UKEK
Key #16	AES 256	255	61443	F5A1	AES CKEK

Manual OTAR Operation The balance of the yellow background blocks can be used by a knowledgeable Crypto Officer to direct manual OTAR/Key Fill operations.



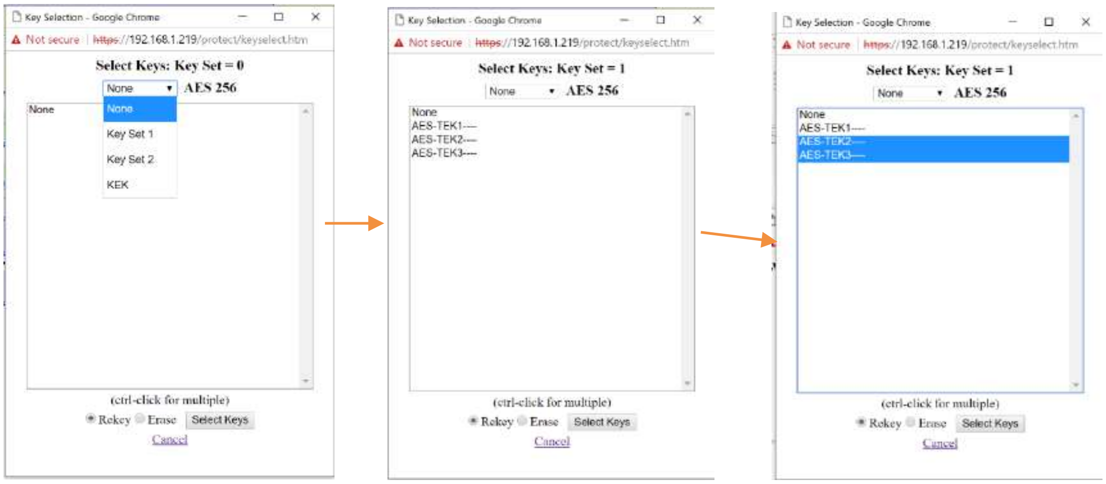
The algorithm must be set for OTAR KMF and KFD operations. Once the algorithm has been selected, the Traffic Encryption Key (TEK) and Message Authentication Code Key (MAC) must be set for OTAR KMF but not for KFD operation. The TEK is used to encrypt the entire OTAR message and the MAC Key is to calculate the Message Authentication Code for the unencrypted message. The MAC and TEK keys can be the same, but they are not required to be so. The pulldown menu only displays keys that are confirmed to be loaded into the Client and are of the correct algorithm. If a Warm Start operation has been completed, the Warm Start TEK can be used for both the TEK and MAC roles. The TKMD ensures that only single operational use of the Warm Start key can take place.

Under Procedures are11 hypertext fields that will each open a new window for the Crypto Officer's use. Each of the result windows will be discussed separately in the following sections.

Warm Start The Warm Start window is only used for OTAR KMF operation. It is necessary to set the algorithm before opening the Warm Start web page. The Warm Start web page shown below is used to send a one-time Traffic Encryption Key (TEK) to the Client. The TEK is encrypted with a KEK that it is believed the Client has. The Client decrypts the TEK using the appropriate KEK and sends back a message encrypted with the TEK sent in the Warm Start message. If the TKMD correctly decrypts this message this confirms:

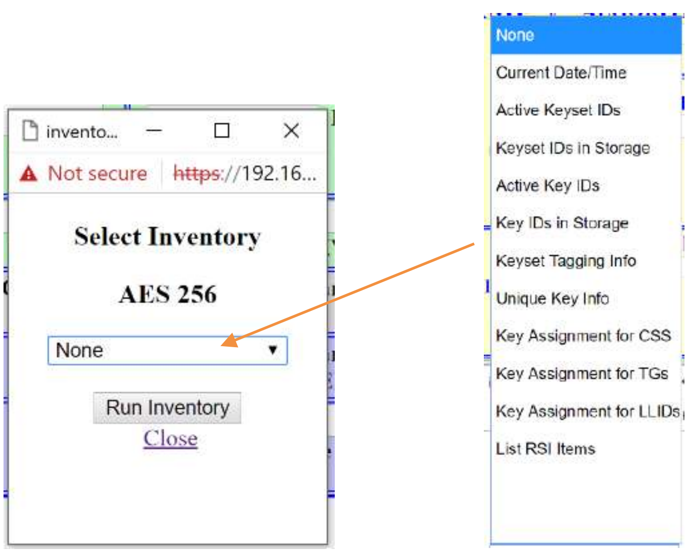
- The Client is an authenticated OTAR Client by possession of the appropriate KEK and
- The Client now has a TEK that can be used for a single OTAR Rekey operation.

Rekey/Erase The Rekey/Erase web page is shown below. The first entry is the selection of the keyset (1, 2, KEK) for the operation.



The Keys to be included in the Rekey Erase process, whether the action is Rekey or Erase and clicking the Select Keys button caused the indicated action to take place. Multiple keys can be selected by using shift or ctrl click. This window is used to select keys for both the OTAR and KFD operational modes.

Inventory The Inventory Web Page is used to ask the Client to provide inventory information to the TKMD.



The Inventory type pulldown menu lists the possible types of inventories for the TKMD Operating mode. Not all types of inventory actions will be successful due to the wide range of differences between manufacturers in implementing OTAR standard features.

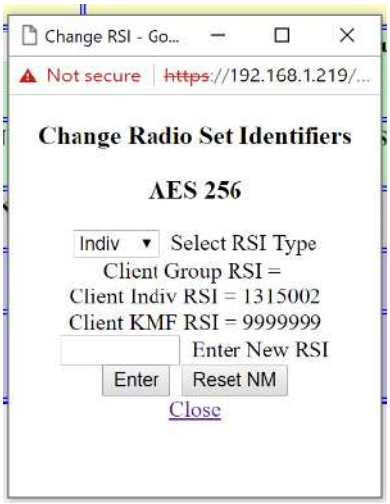
Zeroize The Zeroize web page can be used to completely erase all keys in the Client.

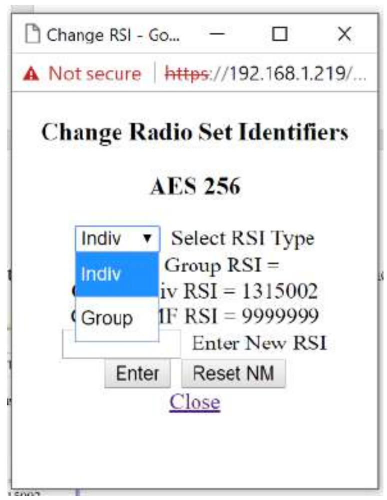
The Zeroize web page is used in both the OTAR KMF and KFD modes.

Set MNP The Set MNP (Message Number Period) is used in the KFD mode to adjust the size of the window used to decide whether to reject the incoming OTAR message based on too large Message Numbers. Generally, most Client radios reject messages with Message Numbers smaller than the last received Message Number.

The desires MNP (up to 65535) is entered in the window and confirm is clicked to send the KFD command.

Change RSI The Change RSI is used in both the OTAR KMF and KFD modes to change either the Individual or Group RSI on the Client. The current settings on the Client are also displayed on this web page.



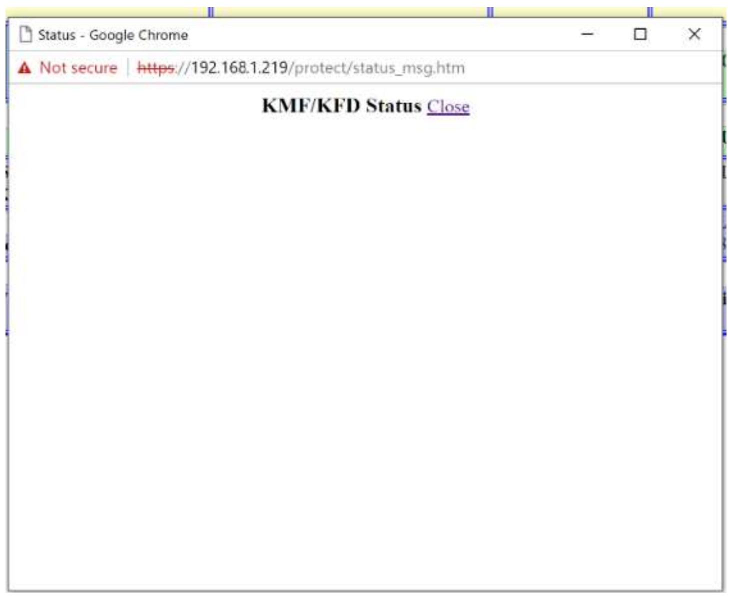


The type of RSI should first be selected, the new RSI entered and Enter clicked to execute.

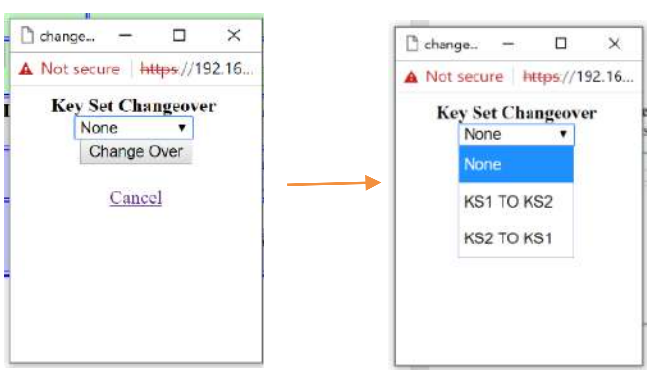
Send Hello Message The Send Hello Message is only used in the OTAR Client mode to send a Hello message back to the KMF to make the KMF aware of the Client or to request a Rekey.

Key Summary The Key Summary web page has been discussed previously.

Status The Status web page gives the Crypto Officer a brief summary of the results of the last OTAR KMF or KFD operation. This web page can be left open during manual operations to provide visual confirmation of the progress of OTAR KMF and KFD actions. The web page will be of limited utility during Automatic OTAR operations since the entries will be quickly overwritten by the consecutive Automatic OTAR processes.



Keyset Changeover The Keyset Changeover web page is used in both the OTAR KMF and KFD modes to cause the Client to change from on active keyset to an inactive keyset.

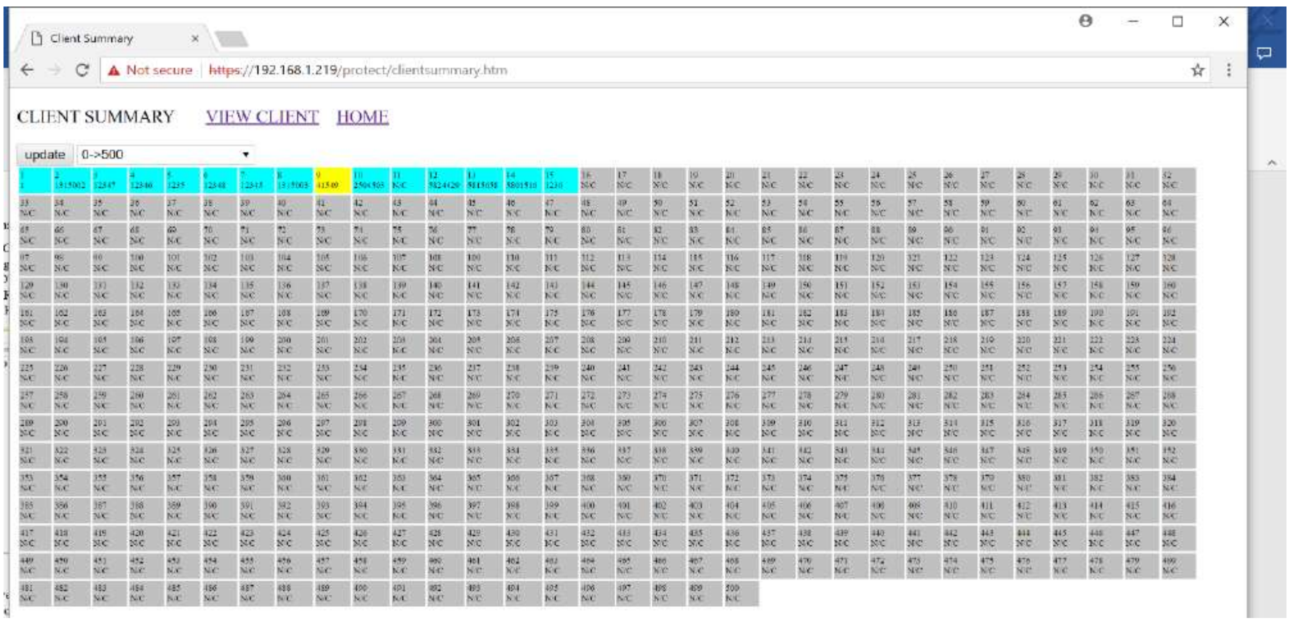


Radio Enable/Disable This is a planned web page to send an encrypted Radio Disable/Radio Enable message to a Client.

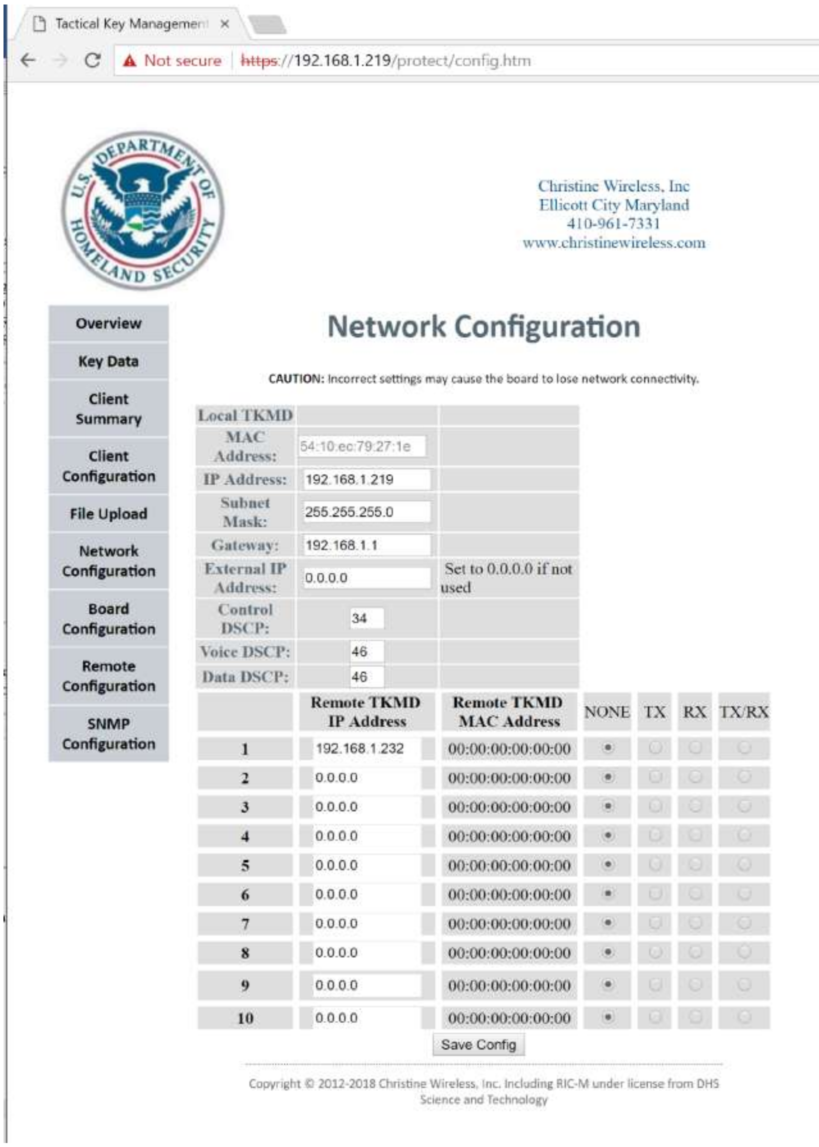
Client Summary The Client Summary web page is auto refreshed every 5 seconds. The web page shows groups of 500 Clients with the Client number, Client RSI, and a color-coded background gives the status of each Client in the group.

If a Client has not been configured, the block background color is grey and the RSI is listed as "N/C".

If a Client is currently registered on the OTAR Data Channel, it will have a green background if it has all of the keys it is supposed to have and a blue background if there are keys needing to be sent to the Client. If the Client is not registered on the OTAR Data Channel, a client having all of its assigned keys will have a yellow background and if the Client needs keys, the background will be aqua.



Network Configuration The Network Configuration web page in addition to the standard RIC-M parameters has a list of up to 10 IP addresses and file sharing enable selections for each.

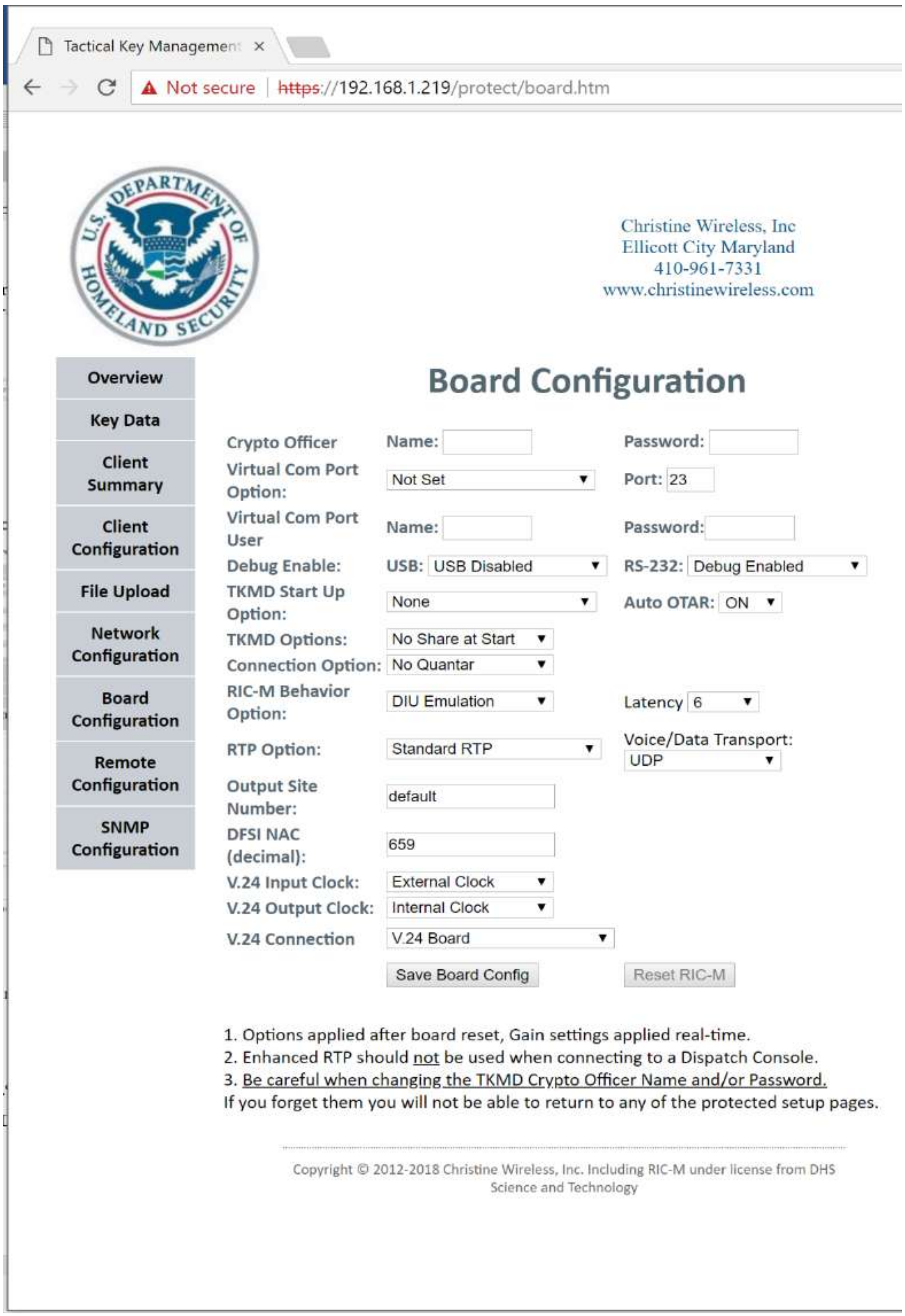


The IP addresses can be other TKMDs or file servers. Sharing options include:

- None No sharing
- Tx Send files to address
- Rx Receive files from address
- Tx/Rx Send to and receive from address.

All file sharing with external IP address TKMDs/Servers is on a TLSv1.2 https link separately established for each file sharing event.

Board Configuration The Board Configuration web page is similar to the same page in the RIC-M and is used to set the basic configuration of the TKMD.



When entries are made on the Board Configuration web page, click the "Save" button at the bottom of the page, wait for the "Reset TKMD" button to change from light grey to dark grey and then click on the "Reset TKMD" button to apply the new information. The TKMD will reset and it will be necessary to re-access the web page to view the applied changes.

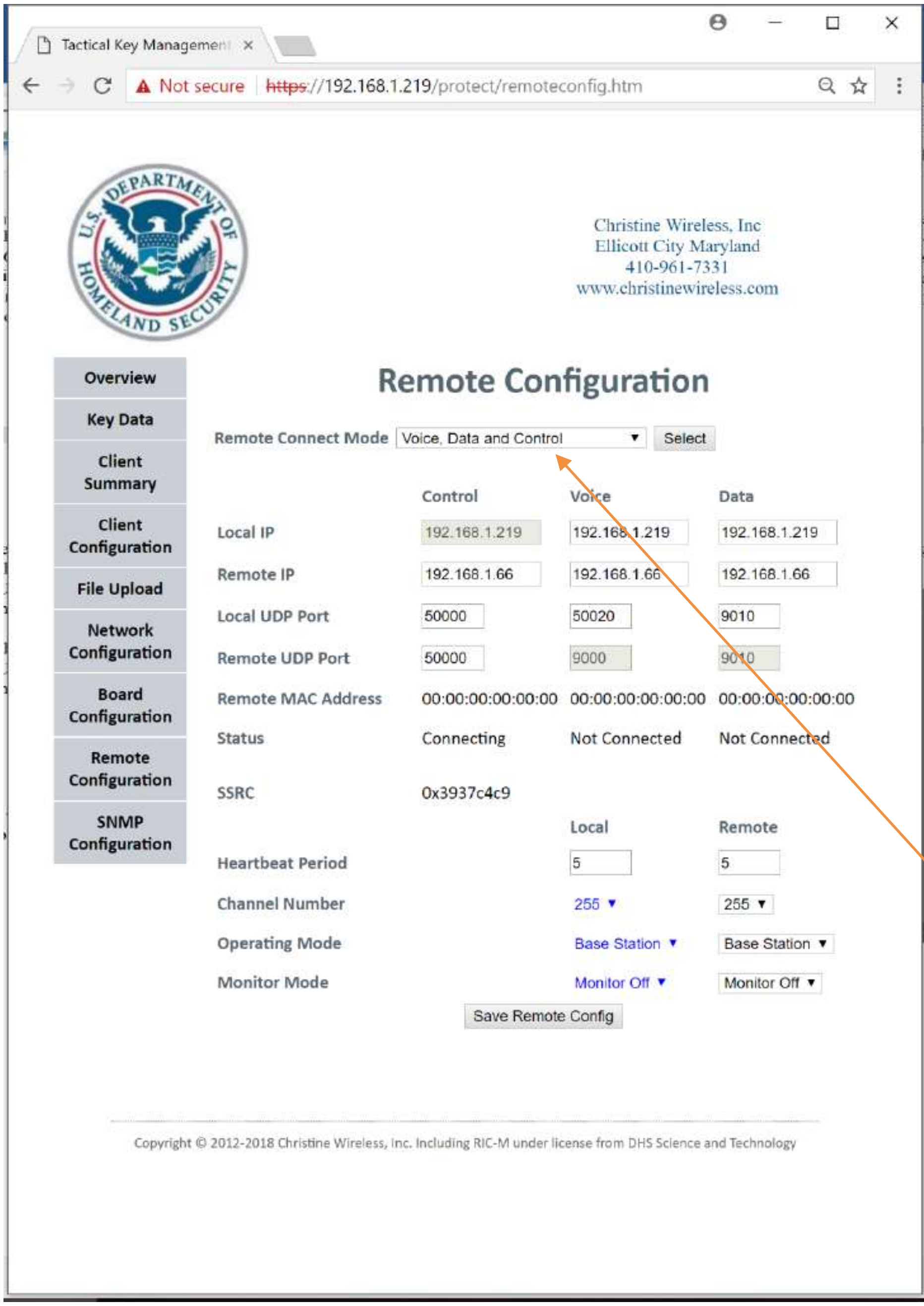
Each entry category is explained in the following paragraphs:

- **Crypto Officer** The User Name and User Password for the Crypto Officer are entered in these two text entry blocks. For production TKMDs this must be done on the first access of the TKMD and DHS strong password criteria is enforced on the Crypto Officer User Password.
- **Virtual COM Port** The TKMD has a Virtual COM Port feature that allows IP access (TLSv1.2 secure) from a PC application to the Radio Service Software RS-232 port on a Quantar™, PDR-3500™, DIU-3000™ or ATAC-3000. The setting options are:
    - **Option** To use the Virtual COM Port it must be enabled with the first pulldown menu.
    - **Port** This window is used to set the port used by the Virtual COM (1 to 65535). The default port is 23.
    - **User Name** The Virtual COM Port User Name can be changed with this text entry box. The default User Name is "admin".
    - **Password** The Virtual COM Port User Password can be changed with this text entry box. The default password is "microchip".
- **Debug Enable** These two pulldown menus select how the USB and RS-232 ports will be used.
    - **USB Options** Use of the USB port requires installation of an appropriate Microchip Driver on the PC and use of a terminal emulation program such as Teraterm. (http://www.microchip.com/Developmenttools/ProductDetails.aspx?PartNO=MCP2200EV-VCP).
        - **USB Disabled** This option still has the USB port active for external processor status inquiries/responses.
        - **Debug Enabled** This option routs the debug messages to the USB port.
        - **V.24 I/O Enabled** This option gives a formatted hexadecimal output of the V.24 messages in both directions including time stamps and CRC checks.
    - **RS-232 Options** The following options are available for use of the TKMD RS-232 port:
        - **Disabled** This will disable all output on the RS-232 port.
        - **Debug Enabled** This option enables output of debug messages from the TKMD at 115,200 baud.
        - **Virtual COM Enabled** This option enabled Virtual COM connections to an external RSS plug at 9600 baud.

        - **Async HDLC->IP** This option is for use with a TXM-2000™ Asynchronous HDLC connection at 19,200 baud. HDLC messages are converted to IP for transport.
        - **Async HDLC->V.24** This option is also used with the TXM-2000™ to convert from Asynchronous HDLC at 19,200 baud to Synchronous HDLC at 9600 baud (V.24).
        - **V.24 I/O Debug** This option provides both V.24 I/O messages and Debug message outputs interleaved at 115,200 baud.
        - **SLIP Radio Enable** This option is used to allow the TKMD to use a compatible portable radio as a Base Station using the SLIP protocol at 38,400 baud.
- **TKMD Start Up Options** These two entries setup what Operating Mode the TKMD will be in after a power cycle or reset including whether Automatic KMF is enabled. The usual setting is for one of the KMF modes to be enabled along with Automatic OTAR enabled to allow autonomous (unattended) OTAR operation.
- **TKMD Option** This pulldown menu enables/disables the sharing of the Client file records on startup to other IP addresses as enabled on the Network Configuration web page. The files are encrypted with a derived transport key (AES-256 Key Wrap File Encryption) and then transported on a TLSv1.2 encrypted connection (AES-256, Diffie-Hellman Ephemeral Key Establishment). Anew connection is established for each file and each IP address on the enable list.
- **Connection Option** The following options are available to define the interaction of V.24 and IP UDP connectivity:
    - **No Quantar** This option has no interaction between the V.24 connectivity state and the IP connectivity state. Both connections are independently established if possible.
    - **Require Quantar** This option will prevent an IP UDP connection is the V.24 connection is not established.
    - **Require IP** This option will prevent a V.24 connection if there is no IP UDP connection.
- **Behavior Option** This option sets whether the TKMD appears to be a DIU or a Station (Quantar) to external connected V.24 equipment.
- **Latency** This option sets the number of 20 millisecond voice frames that will be stored prior to beginning to output them on V.24. The latency should be set low (2-4 if an ATAC-3000™ is used in a true voting mode(selecting the best version of the same signal via different receive paths) and higher if using LTE or low reliability IP transport.
- **RTP Option** The Real Time Protocol (RTP) Option selects how the TKMD transports UDP packets. The options are:
    - **Standard RTP** This selects use of TIA Standard RTP formats.
    - **Enhanced RTP** This selects use of TIA Standard RTP formats with addition of data to enhance the fidelity of the V.24 messages for V.24 content that is not directly mapped to TIA Standard RTP messages. This mode is only intended for TKMD/TKMD-RIC-M connections.

  - **HDLC Server Tunnel** This mode makes use of a non-standard encapsulation of V.24 messages in a UDP Server operating mode.
  - **HDLC Client Tunnel** This mode makes use of a non-standard encapsulation of V.24 messages in a UDP Client operating mode.
- **Voice/Data Transport** This pulldown menu selects how the TKMD will transport voice and data messages. The options are:
  - **UDP** Each UDP voice/data packet will be transported over IP a single time.
  - **UDP Repeat 4X** In this mode, the latest UDP packet is sent with the previous 3 UDP packets being sent also. UDP packets are interleaved and spaced in time. Sequence numbers are used on the receiving end to recognize previously received packets and to discard them.
  - **UDP Repeat 8X** In this mode, the latest UDP packet is sent with the previous 7 UDP packets being sent also. UDP packets are interleaved and spaced in time. Sequence numbers are used on the receiving end to recognize previously received packets and to discard them.
- **Output Site Number** This allows setting of the Sits number (0-63) for non-tunnel modes for compatibility with ATAC-3000™, etc.
- **DFSI NAC** This decimal entry is used to set the NAC used in DFSI messages (1-4095).
- **V.24 Input Clock** The source of the clock for V.24 data into the TKMD is set by this pulldown menu.
- **V.24 Output Clock** The source of the clock for V.24 data out of the TKMD is set by this pulldown menu.
- **V.24 Connection** This setting should be “V.24 Board” since the TKMD does not support the ribbon connection to the Wireline Board.

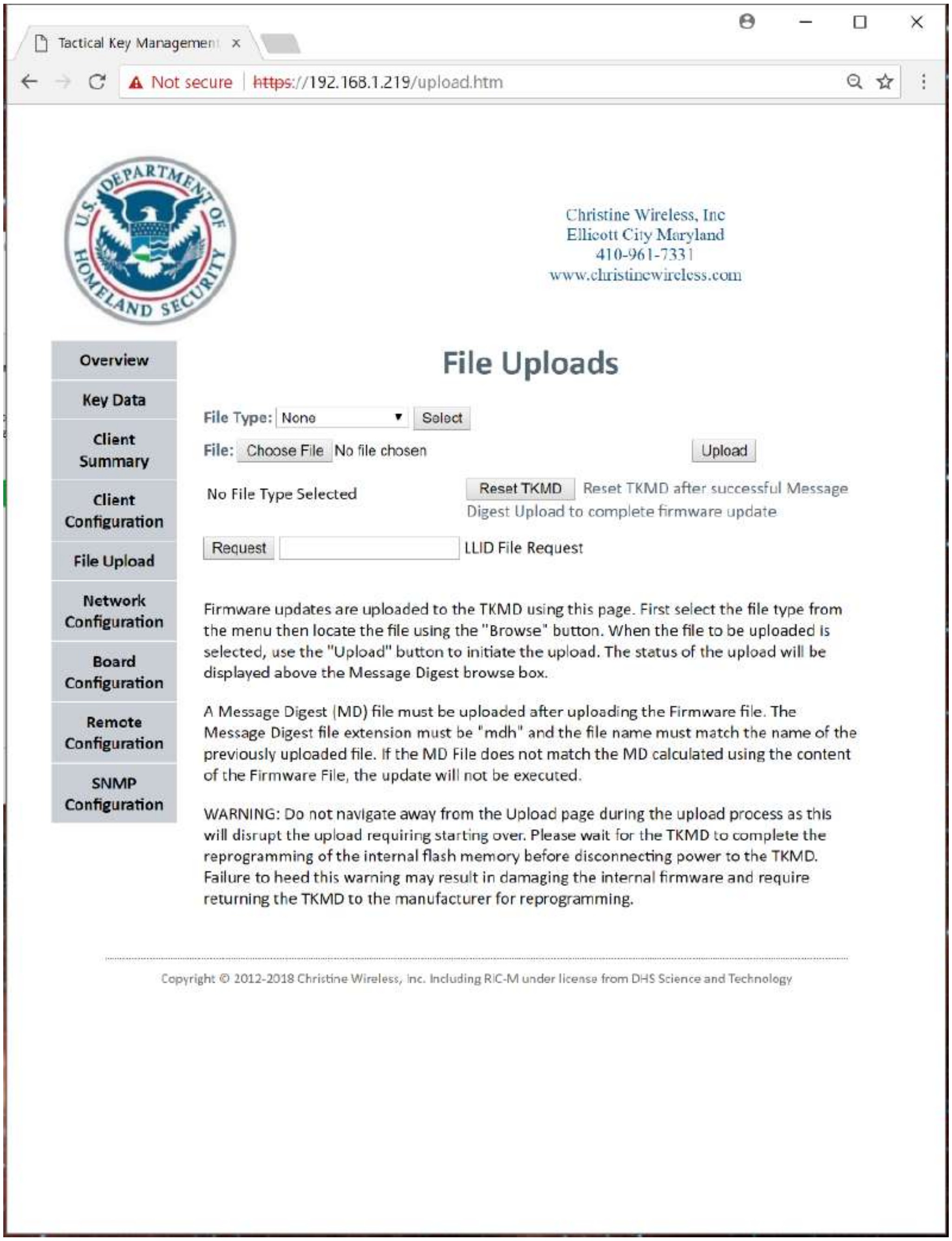
Remote Configuration The Remote Configuration web page is used to define how the TKMD connects with DFSI-Capable equipment over UDP.



When connecting to a DFSI Version 2 RF Resource (Codan, ICOM Eclipse or RIC-M), the Remote Configuration will generally be in the Voice, Data and Control mode as shown above.

File Upload The File Upload web page is used to modify the firmware on the TKMD. Google Chrome is the recommended browser for use with the TKMD.

Browser Circular Icon



Tactical Key Managemen
Not secure | https://192.168.1.219/upload.htm
Christine Wireless, Inc
Ellicott City Maryland
410-961-7331
www.christinewireless.com
Overview
Key Data
Client Summary
Client Configuration
File Upload
Network Configuration
Board Configuration
Remote Configuration
SNMP Configuration
File Uploads
File Type: None Select
File: Choose File No file chosen Upload
No File Type Selected
Reset TKMD Reset TKMD after successful Message Digest Upload to complete firmware update
Request LLID File Request
Firmware updates are uploaded to the TKMD using this page. First select the file type from the menu then locate the file using the "Browse" button. When the file to be uploaded is selected, use the "Upload" button to initiate the upload. The status of the upload will be displayed above the Message Digest browse box.
A Message Digest (MD) file must be uploaded after uploading the Firmware file. The Message Digest file extension must be "mdh" and the file name must match the name of the previously uploaded file. If the MD File does not match the MD calculated using the content of the Firmware File, the update will not be executed.
WARNING: Do not navigate away from the Upload page during the upload process as this will disrupt the upload requiring starting over. Please wait for the TKMD to complete the reprogramming of the internal flash memory before disconnecting power to the TKMD. Failure to heed this warning may result in damaging the internal firmware and require returning the TKMD to the manufacturer for reprogramming.
Copyright © 2012-2018 Christine Wireless, Inc. Including RIC-M under license from DHS Science and Technology

The steps to install a new firmware image are:

1. Use the File Type pulldown menu to select TKMD Firmware. Click Select
2. Use the Choose File button to locate the firmware file with the extension ".hex" and select it. The file name will appear next to the Choose File button.
3. Click Upload. It will take less than a minute for the file to upload. When the file is done uploading, the message "MD Calculated, Enter Correct MD" will appear.
4. Return to the File Type pulldown menu and select Message Digest and click Select. If the browser returns "501 Not Implemented: Only GET and POST supported" click the clockwise circular icon on the left of the browser address window (Google Chrome).
5. Click the Choose File button and navigate to the firmware file with the extension ".mdh" and select it.
6. Click Upload button and the message window will return "MD Checks, Update Enabled".
7. Click Reset TKMD. If the browser returns with the "501" message, again click the clockwise circular icon on the left of the browser window. The TKMD will reset and load the new firmware into the processor program memory.
8. Be patient and do not disconnect the TKMD. The application of the firmware update takes approximately 2-3 minutes and the TKMD yellow light will rapidly flicker when the process is complete.
9. Delete "?resetbtn=Reset+TKMD" from the browser address window since this will cause the TKMD to reset again when the browser connects to the TKMD.
10. Reconnect to the https site and navigate to the Home (Overview) page to verify the new date on the installed firmware.

Automatic OTAR KMF Sequence The following is a step-by-step description of what happens when a Subscriber Unit (Client) attempts to register on an OTAR channel serviced by the TKMD:

1. The Client sends a Registration Request on the OTAR channel.
2. The TKMD receives the request, sends a confirmed data response packet back to the Client and checks if the LLID of the requesting unit is in the local TKMD Client data base. If the Client is found, a Registration Grant message is sent to the Client. If the Client is not found, the TKMD sends a Client Query to the network asking for the Client File. If the Client file is found on the network, it is sent (double encrypted) to the requesting TKMD. The received file is decrypted and added to the TKMD local data base. The next time the Client requests OTAR Registration, it is granted.
3. The TKMD checks the Client record for currency and also checks if any of the referenced key material in the Client data base has been updated (KFD or Key Kettle File upload) since the Client record was last updated. Any indicated changes are made in the Client record.
4. The TKMD starts with the DES algorithm (if enabled).
5. The TKMD verifies that the Client Record has a KEK assigned and "provisioned" (verified to be loaded in the Client). A random number generator created a Warm Start key of the appropriate algorithm, encrypts it with the KEK known to be loaded in the Client and sends it in an outer layer unencrypted message to the Client.
6. The Client receives and acknowledges the message, decrypts the Warm Start key using the appropriate KEK and sends back a message encrypted with the Warm Start Key and also with a MAC calculated with the Warm Start Key.
7. The TKMD decrypts and verifies the message. The Client and TKMD now have a single-usage Warm Start key to start the transfer of "real" keys.
8. The TKMD selects a "real" TEK from the Client assigned keys, encrypts it with the KEK and incorporates it into a message encrypted with the Warm Start Key and also with a MAC calculated with the Warm Start Key and sends it to the Client.
9. The Client receives the message and acknowledges the Confirmed message. The Client decrypts the message with the Warm Start key, decrypts the "real" TEK with the appropriate KEK and sends back a response message encrypted with the 'real" key including a MAC calculated with the "real" key.
10. The TKMD now selects a keyset (key set 1 say) and encrypts each key with the appropriate KEK, encrypts the entire message with the "real' TEK, includes a MAC calculated with the "real" key and sends the rekey message to the Client.
11. The client receives the confirmed rekey message, decrypts the message and keys included and sends back a response message to the TKMD encrypted with the "real" key (including a MAC calculated with the "real" key) indicating success if the rekey works.
12. The TKMD receives, decrypts and verifies the response message. The TKMD now repeats the rekey process with key set 2 and then with key set 255 (KEKs) if any KEKs need updating.
13. After completing the first algorithm, the entire process starting with Warm Start is repeated until the list of rekey actions is complete.

14. If any action in this process fails it is repeated up to 3 times until it is successful or the step is skipped.
15. Once the Automatic OTAR process is complete, the TKMD updates the Client file including metadata, encrypts the file and sends it to any indicated TKMDs/Servers on the Network page that are flagged for sharing.

Key Fill Operation The TKMD has the capability to accept key material from a Project 25 KFD as well as to act as a KFD to load key material into any Project 25-compliant OTAR-Capable radio. In both cases a two wire connection to the TKMD is made through the 6 pin Hirosi Key Fill connector on the TKMD front panel.

Key Fill Receive The steps to accept key material from a KFD are:

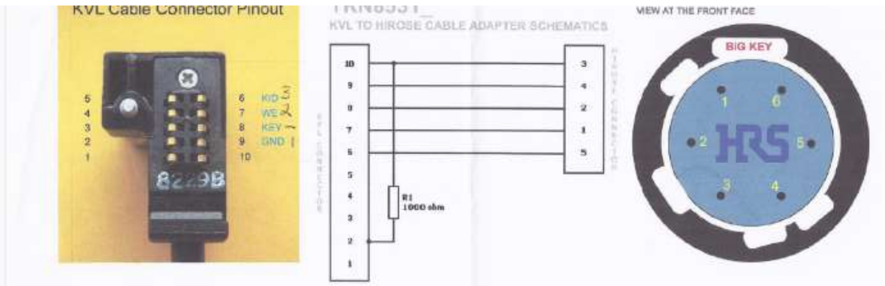
1. Log on to the TKMD as a Crypto Officer.
2. Go to the Client Configuration web page.
3. Enter Client number 0 to select the TKMD as the Client.
4. In the upper left corner of the Client Configuration web page, select KeyFill Receive.
5. Select the Key Summary web page at the right top of the Client Configuration to open that page as a separate window.
6. Open the Status page as a separate window.
7. Connect the KFD to the TKMD Key Fill connector.
8. Operate the KFD according to the manufacturer's instructions to load the selected key material into the TKMD (Client 0).
9. Observe the Status and Key Summary web pages to monitor the progress on loading key material.
10. Once key material has been loaded into the TKMD, go to the Key Data web page and select the TKMD as the key source. The TKMD Key material can now be assigned to Clients on the Client Configuration web page.

Key Fill Send The steps to load key material into a Project 25-compliant OTAR-capable radio are:

1. Log on to the TKMD as a Crypto Officer.
2. Go to the Client Configuration web page.
3. In the upper left corner of the Client Configuration web page, select KeyFill Send.
4. Enter the Client number of the intended Key Fill Target in the Client Selection window. If the Client Number is not known, enter the Client Number of ant configured client and perform a RSI inventory to find the programmed individual RSI for the radio.
5. Select the Key Summary web page at the right top of the Client Configuration to open that page as a separate window.
6. Open the Status page as a separate window.
7. Connect the target radio to the TKMD Key Fill connector.
8. Perform a RSI Inventory and view the result on the status web page to verify the RSI of the target radio.

9. Perform the intended key/radio management operation on the target radio.
10. Disconnect the Key Fill cable from the TKMD.

Key Fill Connections To connect a KFD or target radio to the TKMD remove the back shell on the 10 pin MX connector that would normally connect to the KFD. Drill a small hole in the back shell and feed two wires from a mating Hirosi connector (P/N HR10-7P-6P(73), Digikey HR1560-ND) through the back shell and solder the wire from Hirosi Pin 2 to Pin 8 on the MX connector and the wire from Pin 4 (Ground) on the Hirosi connector to Pin 9 on the MX connector. Reassemble the MX connector.



Pin cross of factory made TKN8531C:

KVL / HIROSE	1	2	3	4	5	6	7	8	9	10
1	—	—	—	—	—	—	+	—	—	—
2	—	—	—	—	—	—	—	+	—	—
3	—	1000 ohm	—	—	—	—	—	—	—	+
4	—	—	—	—	—	—	—	—	+	—
5	—	—	—	—	—	+	—	—	—	—
6	—	—	—	—	—	—	—	—	—	—

Legend:

Short circuit	+
No Connection	—
Some resistence	xxx ohm