Tactical Key Management Device (TKMD)

January 17, 2022

Introduction: The Tactical Key Management Device (TKMD) is a multi-purpose single box 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 2. 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), GGM-8000™, CGW-8000™, 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 RF Technology (Eclipse). The TKMD will also interoperate with a Christine Wireless, Inc. RIC-Mz using DFSI Version 2 which allows IP connection to V.24-capable equipment not collocated with the TKMD.

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 of one or more encrypted Key Kettle Files. Subscriber assignments can be done manually or by upload of encrypted Subscriber Files. Subscribers can also be configured by uploading an Excel Comma Separated Variable (CSV) file.

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 100'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 (Battery Access Cover Removed)

TKMD Epoxy Potting (Battery Access Cover, Support Foam and Battery Removed)

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

1. 2.0 mm 12 VDC input power jack
2. Zeroize switch with protective cover to erase cryptographic variables stored in volatile memory
3. Ethernet connection for https web connection and shared with UDP Base Station/network connection
4. USB connector for monitor
5. 4 Light Emitting Diode (LED) status indicators
6. RS-232 for monitoring or Asynchronous Base Station connection

7. V.24 connector for use with RF Resources with compatible connections
8. 6 Pin Hirosi connector for KFD or Subscriber Unit key fill use

TKMD Front Panel

TKMD File Sharing: If the feature is enabled, 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 60 keys.

Each Key Kettle File contains all Key Material and metadata for up to 40 keys. Each TKMD can store up to 8 Key Kettles. Keys in the Key Kettle are cross referenced 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.

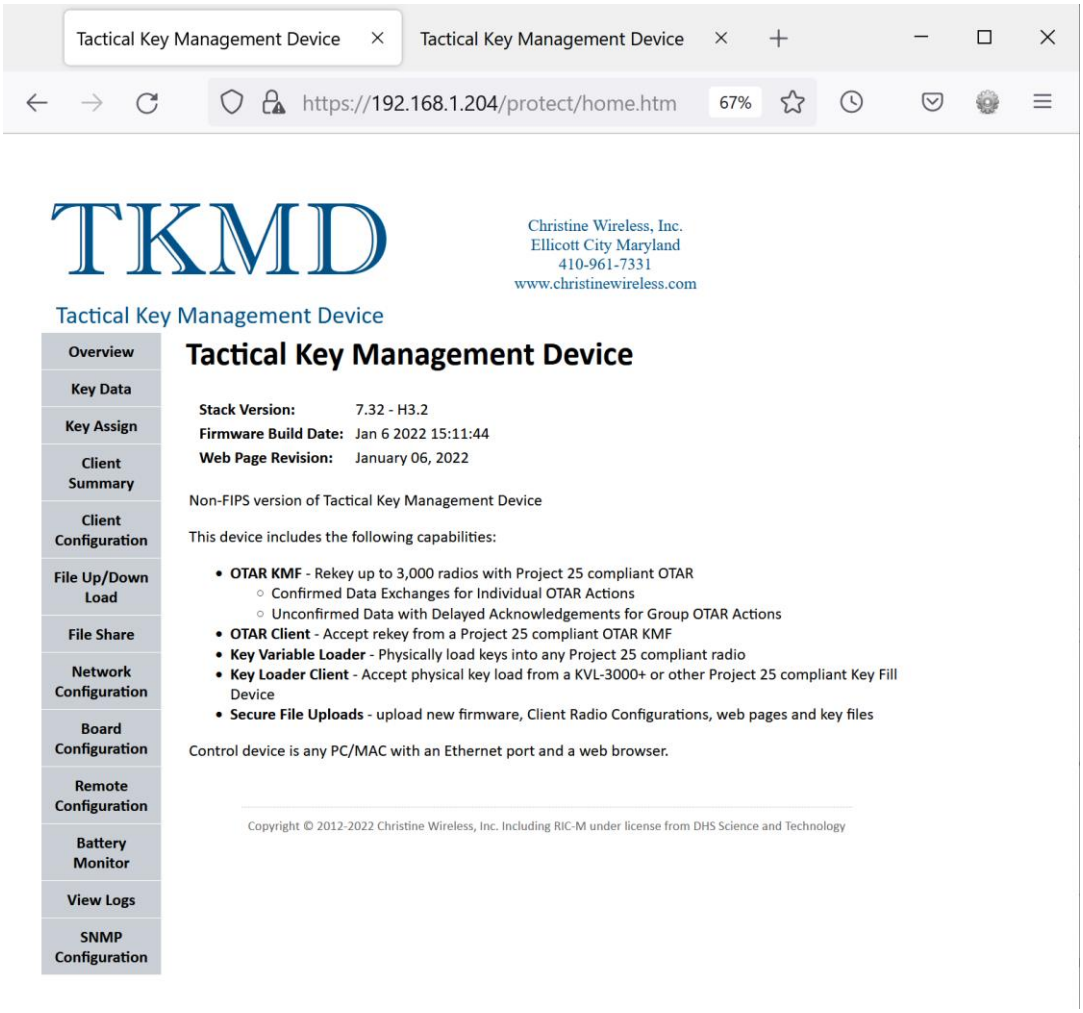
TKMD Configuration Setup

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.

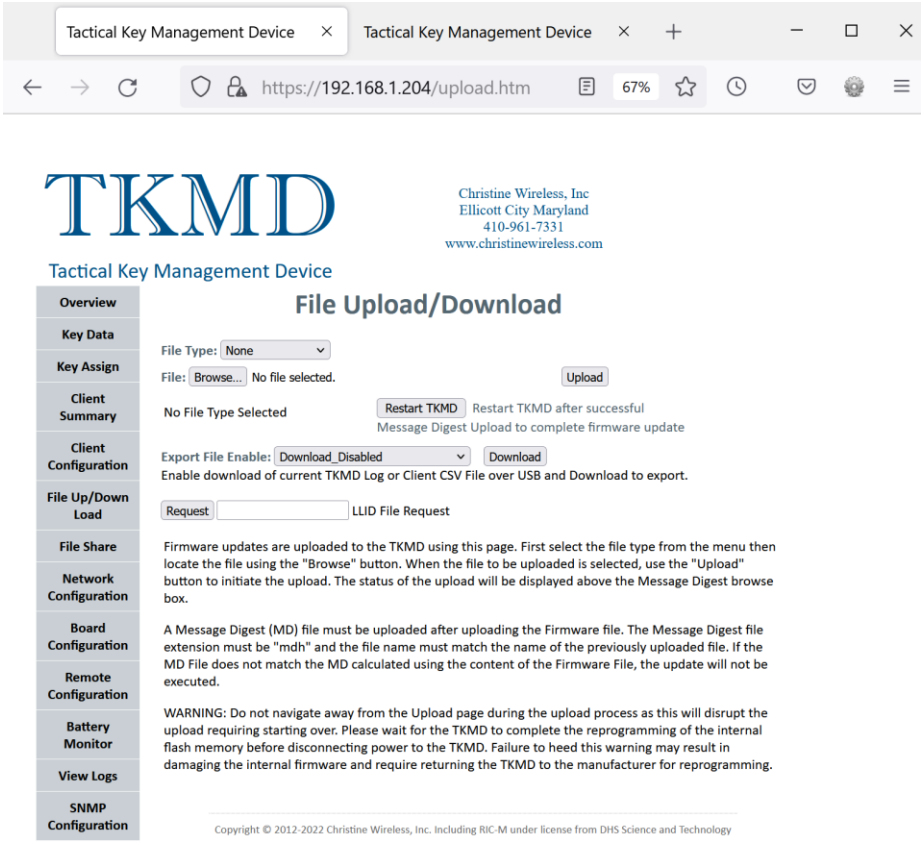
Web Page Access: The default IP address for the TKMD is 192.168.1.204. In a web browser (Google Chrome is the recommended web browser-make sure that you have a recently updated version of Chrome) enter https://192.168.1.204 in the browser address box. Chrome will attempt to connect and will produce a 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.

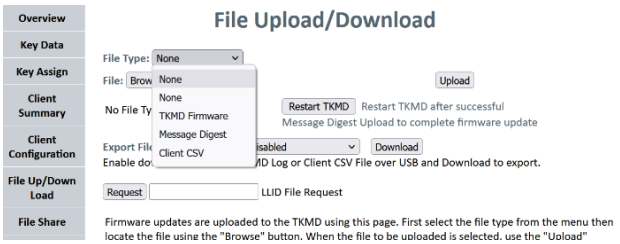
At the bottom of the warning web page, click Logon which will produce a window for the user name and password. The default user name is “admin” and the default password is “tkmdboard”. In production versions of the TKMD, it will be necessary to change the User Name and User Password to gain access to 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 Home web page. This page shows the firmware revision date for the TKMD and has a navigation tool bar to access other TKMD web pages.



The File UP/Down Load page is used to import new TKMD firmware and can also be used to import an Excel Comma Separated Variable (CSV) file to assist in initial configuration of the Radio Subscriber Units.





Tactical Key Management Device (TKMD)

CSV Import/Export

Introduction Christine Wireless, Inc. and ACG Systems have been continuing to advance the capabilities of the TKMD. With the introduction of TKMD Version 3, these capabilities include the ability to set up the required database for the Subscriber Radios Units (Clients) using an Excel Comma Separated Variable (CSV) tool. The Crypto Officer can create an Excel spreadsheet up to the maximum number of licensed Clients and import the CSV version of the spreadsheet into the TKMD. Upon the next startup of the TKMD, the CSV document is used by the TKMD to configure the Client database either in part or totally. The spreadsheet contains all Client-specific

data as well as references to which cryptographic keys are assigned to each Client. The key data bases (up to 8 "Key Kettles") can be setup either manually or up-loaded by the Crypto Officer as an encrypted file over the secure IP connection. Any keys contained in a key database that are referenced in the CSV record for each Client will be automatically copied into the corresponding Client record in the TKMD. All Key Kettles and keys contain a UTC time reference. Import of newer keys will cause the new key material to be distributed into the appropriate Client record.

Once configured, the TKMD also has the ability to export a CSV version of the Client Data Base. This can be used as a backup file of to configure another TKMD.

Excel Template The Excel template consists of a header row with 72 columns and a separate row with 72 columns for each Client unit. The first 12 columns are the Client-specific parameters and each of the following 60 columns each containing a reference to the Key Kettle and Key number in the referenced Key Kettle assigned to the Client. The reference is a 6 digit decimal number where the 4 most significant digits are the Key Kettle referenced and the least significant 2 digits are the specific key in the Key Kettle (up to 60). Thus, the key reference 700012 refers to key 12 in the Key Kettle identified with the Key Kettle ID 7000. Key Kettle IDs range from 1 to 9,999. Reference keys in the Key Kettle range from 1 to 60.

The Client-specific fields are:

1. **Client Number** The Client Number is the specific location to store the Client Record created by the CSV import file. Any other data located at that location will be over-written in the creation of the Client file.

2. Client RSI This is the Radio Set Identifier assigned to the specific Client. Care must be taken to avoid duplicate RSIs in the Client database.

3. Client Unit ID This is the Over-the-Air (Common Air Interface) ID assigned to the specific Client. Care must be taken to avoid duplicate Client Unit IDs in the Client database.

4. Client Name

5. Client Organization

6. Client Organization Group

7. Client File UTC This is the 10 digit Universal Time Code for the file.

8. Client KMF This is the 7 digit RSI for the KMF the Client is assigned to use.

9. KVL RSI This is the 7 digit RSI for the KVL the Client is assigned to use.

10. Client Group RSI This is the 7 digit RSI for the Group the Client is assigned to use.

11. Client Group This is then identification of the Group the Client I assigned to for Group OTAR operations if used.

12. Message Number Period This is the setting for the period assigned to manage OTAR Message Numbers.

CSV File Import To import a configuration from Excel, first save the Excel configuration file as a CSV file (.csv). Use the TKMD "File Up/Down Load" web page and select "Client CSV" in the File Type pull-down menu. Click Browse and navigate to the .csv file saved from Excel and select the file. Click Upload to upload the .csv file to the TKMD. The file will be saved in non-volatile memory and will be applied on the next restart of the TKMD. Once the file is imported, the TKMD will make the indicated entries in the designate Client file memory. The TKMD will also attempt to find the referenced key material in one of the 8 available Key Kettle storage locations. If a match of a Key Kettle ID and the referenced Key Kettle ID can be found, the TKMD will attempt to copy the key referenced into the appropriate Client Key location.

CSV File Export It is also possible to export the current or archived CSV configuration using the TKMD "File Up/Down Load" web page. To download the current configuration, connect a USB cable and use a terminal emulation program such as Tera Term to capture the USB output text. Select the Export File Enable setting Download Latest Client CSV. Click download and save the Terminal emulation file as a .csv file with the desired name. Depending on the start/stop history of the TKMD it may also be possible to download an earlier version of the Client CSV file. The Client CSV file storage can also be erased (without damaging the actual Client files) using the same pulldown menu.

Construction of a Key Kettle Once one or more Key Kettles are constructed, the Key Kettles can be use within the local TKMD or can be exported as encrypted files over a second level of encrypted Internet Protocol to other TKMDs. The basic construction of a Key Kettle is done with the Key Assign web page (See TKMD Web Page Description document).

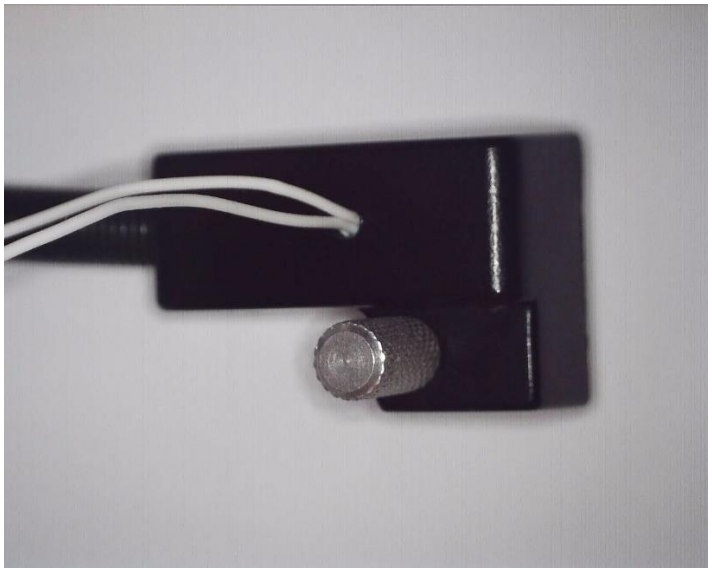
Creating Key Kettles The TKMD "Key Assign" or "Key Data" web pages can be used to create a Key Kettle. It is strongly recommended that at least two Key Kettles are created, one for the Key Encryption Keys (KEKs) and a second for the Traffic Encryption Keys (TEKs). This will allow periodic update of the TEKs without disturbing the KEKs which are essential for OTAR operations. If the KEKs are changed, it may not be possible to perform OTAR and it may become necessary to update the Client through a key fill operation prior to attempting OTAR.

Key Kettles are stored (encrypted) in one of 8 non-volatile memory locations designated as "Imported Keyset" 1 -> 8. Key Kettles created on one TKMD can be securely transferred to another TKMD over Internet Protocol using the TKMD "File Share" web page. If the key material is entered into the TKMD using a Key Fill Device the keys will be assigned to Client 0, the TKMD itself and it will be necessary to use the "Key Assign" web page to move the keys into the desired Key Kettle.

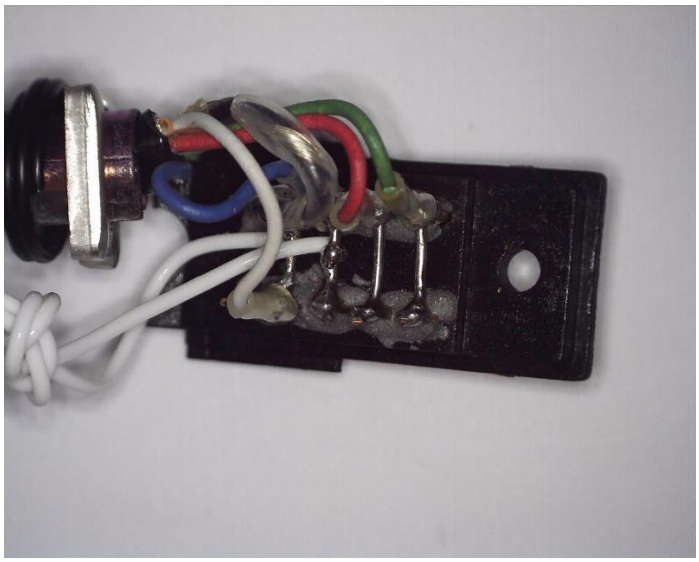
Key Fill Cable Modification for use with TKMD

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.



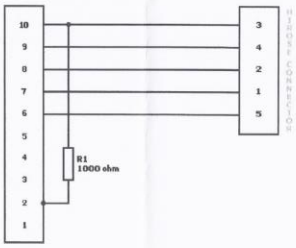
Remove the screw from the KVL connector to expose the 10 solder pins. Drill a small hole in the back of the Motorola (or other) key fill cable KVL connector. Run the two wires from the Hirosi 6 pin connector through the hole and tie a knot inside the connector back shell to prevent strain on the solder connections to be made below. Solder the ground wire (wire with a knot in it, connected to Hirosi connector pin 4) to the 4th pin away from the connector screw. Solder the key fill line (Hirosi Connector pin 2, wire without a knot) to the middle solder pin on the KVL 10 pin connector. On the KVL connector there should be 4 jumpers joining each of the first 4 pins to the pin on the opposite row as shown above.



KVL Cable Connector Pinout

TKN8531_

KVL TO HIROSE CABLE ADAPTER SCHEMATICS



HIROSE MALE 6 PIN CONNECTOR PINUOT
VIEW AT THE FRONT FACE

Pin cross of factory made TKN8531C:

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

Legend:

Short circuit	+
No Connection	—
Some resistance	xxx ohm