Tactical Key Management Device (TKMD)

The TKMD is a low-cost, single box, Project 25 Over-the-Air Rekey (OTAR) implementation for transportable, campus stand-alone or network applications

Stand-Alone Operation As a stand-alone Key Management Facility (KMF) the TKMD is connected directly or via an Internet Protocol connection to the RF Resource(s) used in the OTAR System. The TKMD in this mode will support OTAR in a campus environment (example: Airport, Embassy, etc.). As a standalone KMF, the TKMD can also support transportable field operations such a First-Responder Incidents, SWAT and other needs to quickly distribute interoperability keys.

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 RF Resource(s) assigned to that TKMD. 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 Operating Modes: *The TKMD can function in the following Modes:*

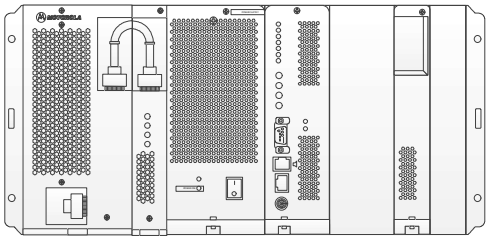
1. ***OTAR KMF*** *The TKMD can operate as a Key Management Facility (KMF) for a stand-alone or networked Project 25 OTAR System. An individual TKMD can support up to 500 (and optionally 3,000) subscriber radio units. A network of TKMDs with a central server can support a virtually unlimited number of subscriber radio units.*

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.*

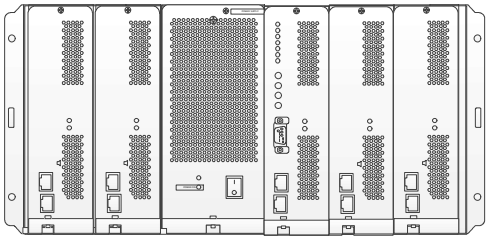
3. ***Key Fill Receive*** *The TKMD can operate as a Subscriber Unit and receive Key Material from Project 25-compliant Key Fill Device (KFD).*

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

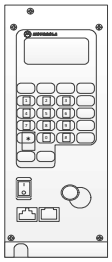
Compatible HDLC Equipment



Quantar™



ATAC-3000™



DIU-3000™

GTR-8000™ with V.24 Option

GGM-8000™

CGW-8000™

TXM-2000™ (HDLC Async.)

PDR-3500™

Compatible IP Base Station Equipment

ICOM/RFT Eclipse DFSI Base Station

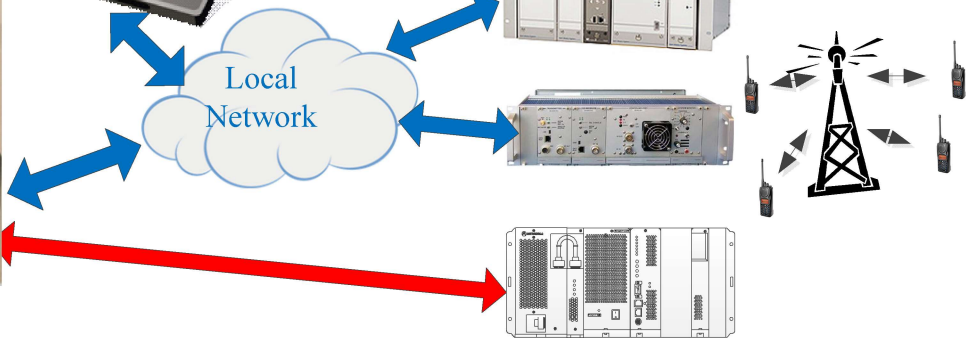
Codan DFSI Base Station

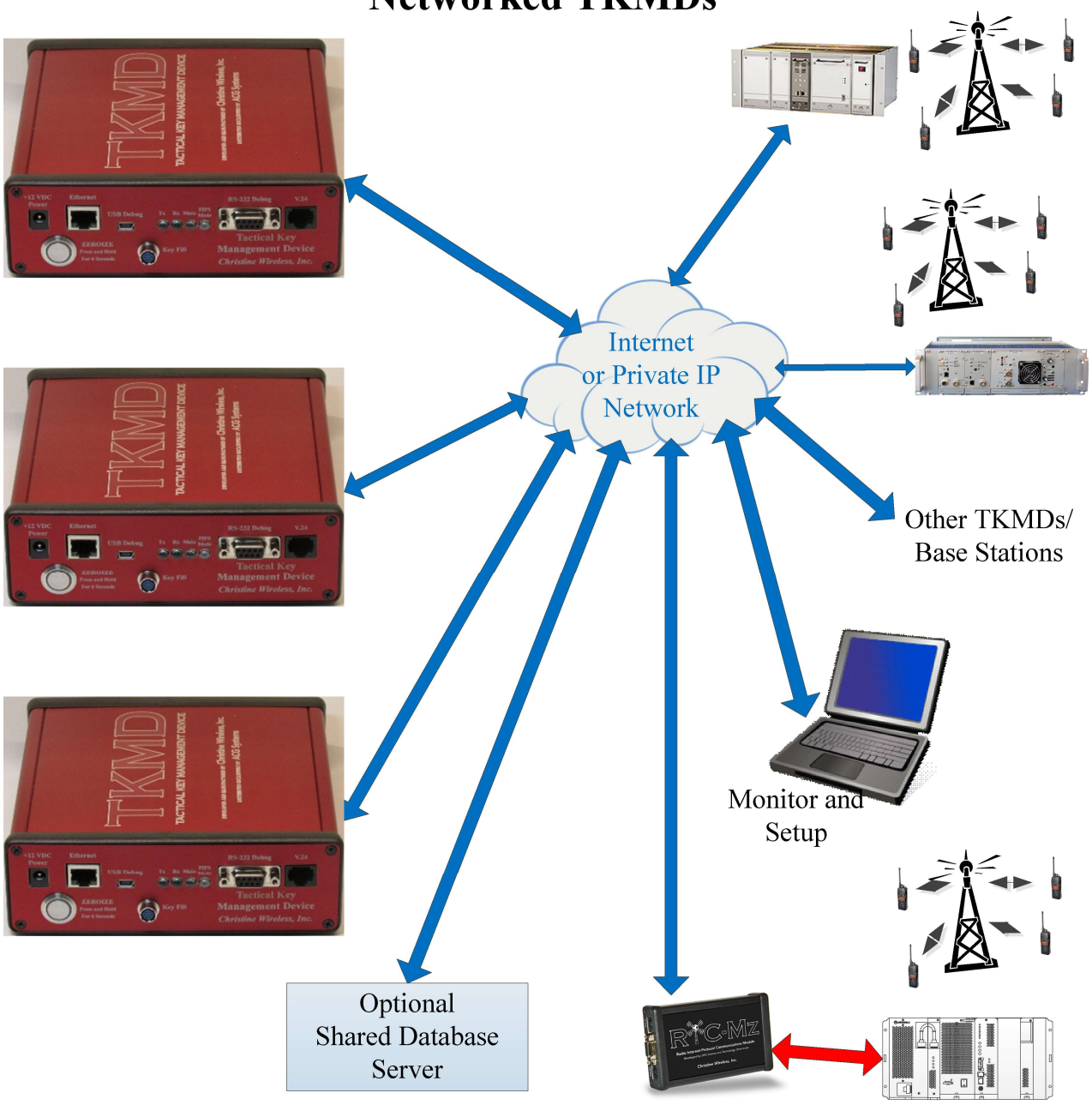
HDLC V.24 or Async

RIC-M in Fixed Station Mode

Standalone TKMD

Monitor and Setup





Networked TKMDs

- **Share Subscriber Status Files** On each OTAR subscriber radio update, the results of the update can be sent as an encrypted file to all TKMDs designated as sharing.
- **Updated Key File** An encrypted file containing updated key material can be distributed via IP to all networked TKMDs
- **Unknown Subscriber Unit** If a subscriber is not found in the locally stored subscriber database, a "Query" is sent to all networked TKMDs to see if the unknown subscriber is contained in any network TKMD database. If it is, the file is encrypted and sent to the requesting TKMD to permit OTAR operation for the unknown subscriber.
- **Optional Server** The Optional Server stores all encrypted subscriber files from the networked TKMDs. These files are only sent at the completion of an OTAR operation with the respective subscriber radio and therefore are the most recent file is the latest and most correct record. The file names contain the over-the-air ID for the subscriber radio. The server only needs to store the encrypted file and provide it on request to the requesting TKMD. Therefore this server need not decrypt the file and the server can be a simple Cloud Data Resource.

TKMD Connections

+12 VDC Power (approximately 2 Watts) Backup internal battery for retention of key material etc. while not powered

Ethernet Communication with RF Base Stations, other TKMDs, Central Server and access to TKMD web pages for setup and control.

USB Debug

V.24 Connection for Base Station

Zeroize Switch

Keyfill Connector Load from/to KVL Device aand load to Subscriber Radio

Status Indicator LEDs

RS-232 Connection for Debug, Asynchronous HDLC, RSS or SLIP connection to a portable radio used as a Base Station

TKMDs Features

- **Stand-Alone or Network Operation** The TKMD can be used in a stand-alone or campus environment or can be a part of an IP network with other TKMDs. In a network environment, encrypted subscriber and key files can be securely distributed to all TKMDs via separately encrypted IP.
- **Web Page Monitor and Setup** Secure web pages are used to access the TKMD. Pages are encrypted (https) and require the operator (Crypto Officer) to enter a valid User Name and Password to access the web pages. While logged into the TKMD web pages, the Crypto Officer can view the current operational and rekey status of all provisioned subscriber radios.
- **Autonomous Operation** Once the key and subscriber data bases are established (either manually by the Crypto Officer or by importing encrypted data files over secure IP) the TKMD operates automatically. In the KMF mode, when a subscriber radio unit attempts to register with the TKMD the respective data bases (subscriber and key material) will be checked and OTAR activities as required will automatically be performed by the TKMD.
- **Cryptographic Key Entry** Key Material can be entered into the TKMD in one of three ways:
  - **Manual Entry** The Crypto Officer can log into the TKMD and create key material either by entering the value or by using a built-in random key generator.
  - **Key Fill Device (KFD) Entry** A KVL-3000™, KVL-4000™ or (KVL-5000™) can be used to enter one or more keys into the TKMD.
  - **Key File Import** An encrypted file containing key material and associated data can be imported into the TKMD via encrypted IP. This file is imported automatically when it is received (if enabled) and the decrypted key material is used to update the corresponding keys in the TKMD internal database.
- **Manual Operation** If desired the Crypto Officer can initiate any supported OTAR operation with a subscriber radio unit and monitor the outcome.
- **Key Fill** The TKMD has a built-in Project 25 key fill device (KFD) which can be used for initial provisioning into subscriber radios of Key Encryption Keys (KEKs) required prior to initiating OTAR operations.
- **FIPS 140-2** The TKMD is currently in the process of obtaining NIST FIPS 140-2 certification.
- **AES/DES Support** TKMD supports AES as a FIPS mode and DES as a non-FIPS mode.

TKMD is available on Purchase/Credit Card or Federal Contracts (including GSA) exclusively from:
ACG Systems, Inc. 133 Defense Highway Annapolis Maryland 21401
(410) 224-0224 https://www.acgsys.com