Tactical Key Management Device (TKMD)

FIPS 140-2 Non-Proprietary Security Policy

Cryptographic module for use in Project 25 Over-the-Air Rekey systems

Version: R01:00:03

Date: September 29, 2021

Table of Contents

List of Tables

List of Figures

1. Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST), Canadian Centre for Cyber Security (CCCS) and Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

1.1. Scope

This is the non-proprietary Security Policy for the Tactical Key Management Device (TKMD). This Security Policy specifies the security rules under which the TKMD must operate. In addition to the security requirements derived from FIPS 140-2 are those imposed by Christine Wireless, Inc. These rules, in total, define the interrelationship between the:

- Module Operators,
- Module Services, and
- Critical Security Parameters (CSPs).

1.2. Overview

The TKMD provides Over-the-Air-Rekey (OTAR) services for Project 25 Radio Systems.

The TKMD can function in the following types of operation:

- 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 typically up to 500 (and optionally up to 3,000) radio Subscriber Units (SUs). A network of TKMDs with a central server can support a virtually unlimited number of radio SUs.
    - *KMF Stand-Alone Operation*: As a stand-alone KMF, the TKMD is connected directly or via an Internet Protocol connection to the RF Resource(s) used in the OTAR System. As a stand-alone KMF, the TKMD will support OTAR in a campus environment (example: Airport, Embassy, etc.). The TKMD can also support transportable field operations such a First-Responder Incidents, SWAT and other needs to quickly distribute interoperability keys.
    - *KMF 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 radio SU 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 radio SU Files after OTAR operations (if file sharing is enabled) or to request the SU File from the network if an unknown Subscriber Unit attempts to perform an OTAR Registration on the local node.

- OTAR Subscriber Unit: The TKMD can participate as a Project 25 OTAR Subscriber Unit and interact with another KMF to receive Key Material from that KMF. If desired, that Key Material can be redistributed to other SUs while the TKMD is operating as the OTAR KMF.
- Key Fill Receive: The TKMD can operate as a Subscriber Unit and receive Key Material from Project 25-compliant Key Fill Device (KFD).
- Key Fill Device: The TKMD can act as a Key Fill Device for any Project 25-compliant Subscriber Unit.

1.3. TKMD Implementation

The TKMD is implemented as a multi-chip standalone cryptographic module as defined by FIPS 140-2.

1.4. TKMD Hardware/Firmware Version Numbers

Table 1: FIPS Validated Version Numbers

FIPS Validated Cryptographic Module Hardware Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
TKMD Spin 3	TKMD_FIPS_FINAL_11_01_20

1.5. FIPS 140-2 Security Levels

The TKMD can be configured to operate at FIPS 140-2 overall Security Level 2. The table below shows the FIPS 140-2 security levels met for each of the eleven areas specified in the FIPS 140-2 security requirements.

Table 2: FIPS Validated Version Numbers

FIPS 140-2 Security Requirements Section	Validated Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.6. TKMD Cryptographic Boundary

The TKMD is housed in an aluminum case that has been filled with black hard epoxy. A single printed circuit board contained in the aluminum TKMD enclosure implements all TKMD functionality. The cryptographic boundary is the outer enclosure and the entire portion of the product that is encapsulated by epoxy. Due to the epoxy potting, the front and top aluminum covers cannot be removed, and the encapsulated printed circuit board cannot be accessed or removed.

Figure 1: TKMD Top and Front View

Figure 2: TKMD Front Panel

Figure 3: TKMD Top and Right Side View

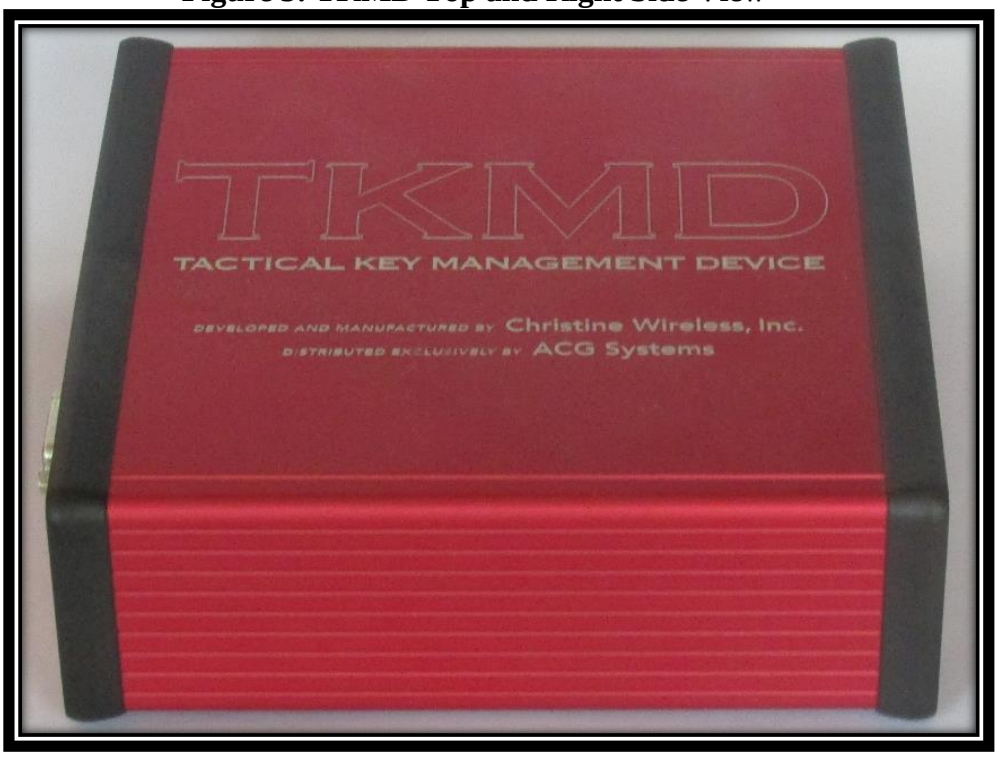


Figure 4: TKMD Top and Left Side View

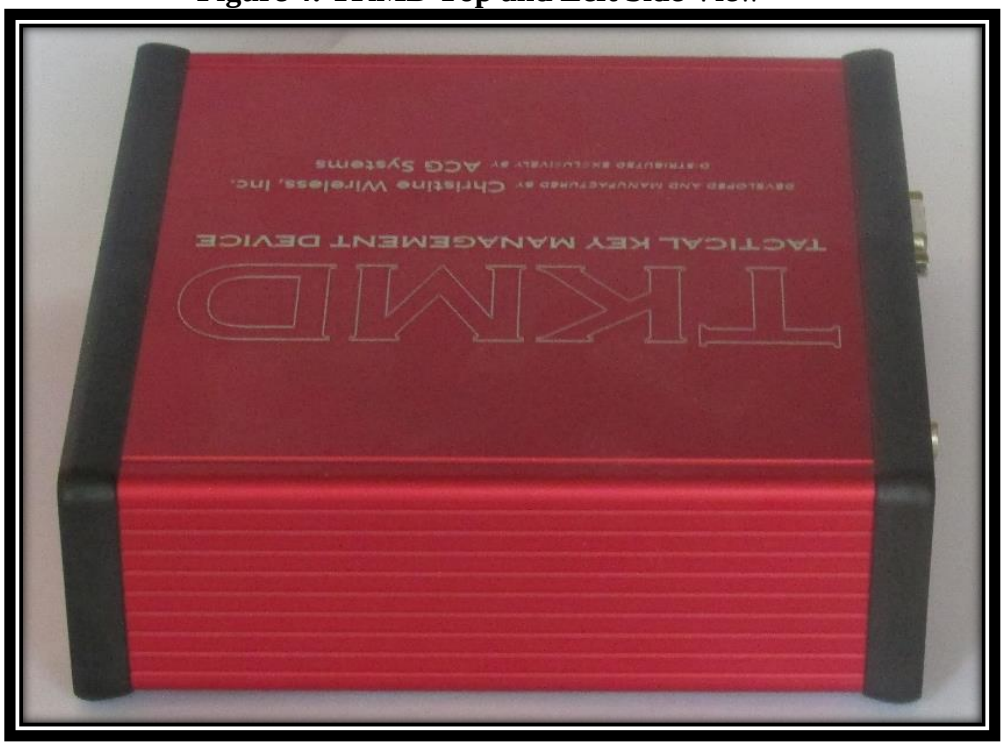
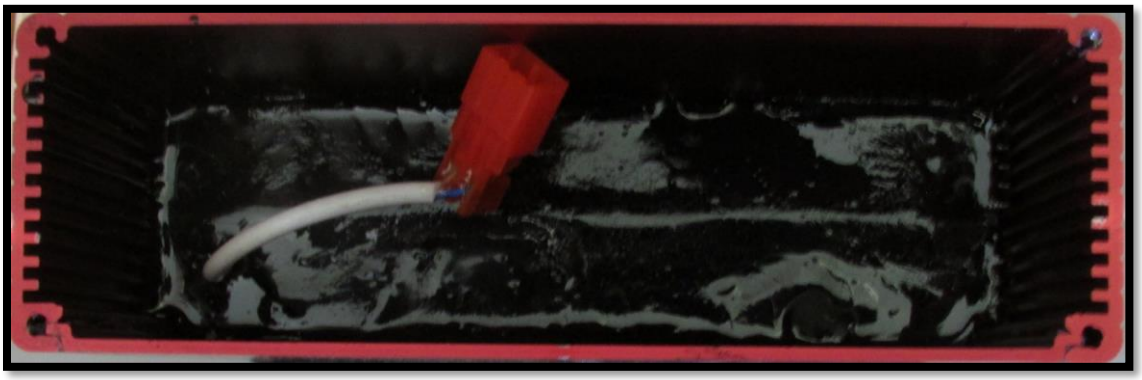


Figure 5: TKMD Rear View Showing Extent of Black Epoxy Potting and Battery Cable



1.7. Ports and Interfaces

The TKMD provides the following physical ports and logical interfaces:

Table 3: Ports and Interfaces

Physical Port	Qty	Logical Interface Definition	Description
Front of the Module			
+12 VDC Power	1	Power Input	+12VDC power into module
V.24	1	Data Input/ Data output (Base Station Interface)	Synchronous serial interface for Tx/Rx of encrypted OTAR data messages if a Quantar is used as a Base Station. V.24 is only used by Motorola "Astro" equipment such as the Quantar Base Station.
RS-232	1	Data Input. Data Output, Status Output (Base Station Interface)	Asynchronous serial interface for Tx/Rx of encrypted OTAR data messages if a SLIP radio is used as a Base Station. Can also be used to provide TKMD status information (no CSPs) during operation.
FIPS LED (Blue) (Right LED)	1	Status Output	Indicates FIPS Mode of Operation
Main LED (Yellow) (Right Center LED)	1	Status Output	Indicates firmware is operating normally
Rx LED (Green) (Left Center LED)	1	Status Output	Indicates incoming Base Station OTAR message
Tx LED (Red) (Left LED)	1	Status Output	Indicates outgoing Base Station OTAR message
USB	1	Status Output	Used only for monitoring V.24 messages. There is no access to CSPs
Ethernet Black	1	Data input/Data output, Status Output, Control Input (IP Base Station Connection)	Internet Protocol (UDP TIA 102.BAHA-A DFSI) interface for Tx/Rx of encrypted OTAR data messages
Ethernet Red (TLSv1.2 on shared physical port logically separated from black ethernet port)	(1) Shared with above physical port	Data input/Data output, Status Output, Control Input	• Crypto-Officer access for setup and monitoring • Crypto-Officer upload of new firmware • Automatic upload of encrypted radio SU and Key Kettle files containing new CSPs
Zeroize Switch	1	Control Input	Zeroization of all CSPs
Keyfill	1	Data input/Data output, Status Output, Control Input	Crypto-Officer upload of un-encrypted CSPs from a Key Fill Device or download to a radio SU
Back of the Module			
Backup Power cable	1	Power Input/Battery Charge Output	Battery Backup for volatile storage- Removal of both power sources zeroizes all CSPs

2. Modes of Operation

The TKMD can be configured to operate in a FIPS 140-2 Approved mode of operation (FIPS mode) and a non-FIPS 140-2 mode of operation (Non-FIPS mode). Documented below are the configuration settings that are required for the TKMD to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 2.

To support Legacy Project 25 Radio Systems, the TKMD is capable of performing OTAR operations using the DES Algorithm (non-FIPS Mode or non-Approved mode). Use of the DES algorithm is strongly discouraged as it provides virtually no security for SU voice operations.

The DES operations are separated from the AES (FIPS) operations and the presence of DES is indicated by the FIPS Blue LED indicator turning off on the TKMD front panel. FIPS operation is indicated by the illumination of the Blue LED. The option to allow the use of DES is selected by the Crypto-Officer using the Red Ethernet TLSv1.2 encrypted Control Interface. In the FIPS Approved mode, only AES OTAR operation is permitted. The module must be zeroized prior to entering the non-Approved mode of operation. Once any DES key has been entered into the TKMD the FIPS indicator will be extinguished and warning messages will appear on the Crypto-Officer Web pages. It is necessary to perform a front panel switch hardware Zeroization to enter the FIPS Approved mode again. This will remove all cryptographic CSPs, restore the illumination of the FIPS indicator and remove the DES warning messages.

In the Non-FIPS Mode, the TKMD can operate with the DES algorithm for OTAR interactions with radio SUs. The Non-FIPS Mode is provided to facilitate interoperability with older OTAR/Radio systems. All services in the non-Approved mode and the Approved mode are the same except for the use of DES keys.

Unless the Crypto-Officer is actively using the TKMD in another mode, the TKMD will be in the KMF OTAR mode and will operate autonomously without direction from the Crypto-Officer. In this mode the TKMD will automatically perform OTAR operations in response to OTAR Registration or Rekey Requests from Subscriber Units.

Upon receipt of a Registration Request or Rekey Request from a SU, the TKMD will verify that the SU Logical Link ID (over-the-air ID) and Radio Set Identifier (OTAR ID) are found in the SU Data Base. If the Subscriber Unit record indicates that the SU has a Key Encryption Key provisioned, the TKMD will determine if there are TEKs or KEKs that have not been sent to the SU that would necessitate an OTAR operation.

For either AES or DES operations the OTAR process proceeds as follows:

1. Send a Warm Start TEK to the SU. This key is generated by the Approved TKMD DRBG and is encrypted with one of the KEKs shown as provisioned. The SU must successfully decrypt the Warm Start Key and send back a response message encrypted with the Warm Start Key thus authenticating the identity of the SU by possession of the symmetric KEK.

2. The TKMD will now use the Warm Start Key to send additional keys to the SU. The Warm Start Key is restricted to a single use thus requiring additional TEKs be sent to the SU to support the balance of the OTAR exchange.
3. The TKMD will update the SU record based on the response messages received from the SU.

3. Identification and Authentication Policy

The TKMD supports a SU User Role, a Network User Role and a Crypto-Officer Role.

The Crypto-Officer Name and Crypto-Officer Password are set as factory default values at the manufacture (admin, tkmdboard). Prior to shipping each unit, these entries are set to non-default values which are securely communicated to the customer to allow initial set up of the unit when it is received. Before any setup or file/key loading is permitted, the Crypto-Officer must log into the TKMD with the as-shipped Crypto-Officer Name and Crypto-Officer Password and set the two entries to new values. Password criteria is enforced on the Crypto-Officer password (uppercase/lowercase/numerical/special character combination).

The Crypto-Officer Name and Crypto-Officer Password are stored in non-volatile memory as a HMAC SHA-256 hash using a HMAC key unique to the individual TKMD. To continue, the Crypto-Officer must log out and log back into the TKMD with the new credentials. The TKMD can now be configured and files uploaded as well as operated with a Key Fill Device.

In the event that the Crypto-Officer Name/Password are erased, the TKMD will be returned to a factory default condition which will result in the erasure of all key material as well as all Crypto-Officer entered setup/configuration data.

The SU User Role requires that each radio SU is provisioned in the TKMD by an authenticated Crypto-Officer. Security for the SU User role is provided by the requirement for each SU User radio and the TKMD to have the same AES-256 key (Key Encryption Key) to be able to encrypt/decrypt keys exchanged in the OTAR processes. The identity of the SU is verified by being able to successfully decrypt OTAR Key Messages with the symmetric KEK. In addition, the OTAR IDs (Radio Set Identifiers) for each individual User must be entered into the TKMD by the Crypto-Officer to permit OTAR operation

The Traffic Encryption Keys (TEKs) for the Project 25 OTAR are loaded as un-encrypted keys by a KFD process, generated by an Approved DRBG or are imported as an encrypted file (over a TLSv1.2 encrypted RED Ethernet interface).

The File Transport Base Key used in the Network User Role is entered by the Crypto-Officer using the encrypted TLSv1.2 IP connection. The File Transport Base Key is never used for encryption of a file. A derived key (HMAC SHA-256 based on the File Transport Base Key, the file name and a nonce) is used to derive each of the unique shared files encryption key which called the File Transport Key.

Table 4: Roles and Authentication

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
Crypto-Officer (Basic Operation, Firmware Update and KFD)	Identity	Username and 8-10 character ASCII password	The minimum password length is an 8-10 ASCII characters. There are 95 printable ASCII characters. Password restrictions force at least one upper case, one lower case, one number and one special character resulting in making the chance is guessing the correct 8 characters 1 in 1.7e+13 ($26*26*10*31*95^4$). The user interface limits password entry tries to 20 per minute resulting in a probability of guessing the password to 1 in 1.2e+12 per minute.
SU User Role	Identity	User ID, User RSI and 256-bit AES Key Encryption Key (KEK)	The probability of a successful random attempt is 1 in 2 ^ 256 (1.2e+77). OTAR channel bandwidth and message length considerations limit the number of attempts possible in one minute to less than 40 limiting the possibility of guessing the KEK to less than 1 in 3.5e+76.
Network User Role	Identity	256-bit AES File Transport Base Key	The probability of a successful random attempt is 1 in 2 ^ 256 (1.2e+77). TKMD limits the number of attempts possible in one minute to less than 100, limiting the possibility of guessing the AES Base File Transport Key in one minute to less than 1 in 8.6e+76.

4. Access Control Policy

4.1. TKMD Supported Roles

The TKMD supports three authenticated roles. These roles are defined to be:

- SU User Role (OTAR Client)
- Network User Role (Network File Share Client)
- Crypto-Officer Role.

4.2. TKMD Services Available to the Authenticated SU User Role.

- OTAR Operations (requires prior CO provisioning of User IDs and User radio SU possession of one or more symmetric AES-256 KEKs)
    - **Request Rekey:** A Subscriber Unit may optionally request a complete rekey. This will result in the TKMD sending all keys assigned to the Subscriber Unit via the OTAR Process.
    - **Warm Start Rekey:** An OTAR process generally includes sending the SU a one-time TEK encrypted with a KEK. The one-time key (Warm Start Key) is used to initiate a complete OTAR exchange with the TKMD.
    - **Rekey:** When the SU registers with the TKMD when first using an assigned OTAR RF channel, the TKMD will automatically initiate an OTAR process and send any keys that have been assigned to the SU, but have not been sent to the SU according to the TKMD individual SU data record.
    - **Zeroize:** Under the control of the CO, a SU can be completely erased of any Cryptographic Keys (zeroized) as part of the OTAR process. After zeroization it will be necessary to manually load at least one KEK into the SU with a KFD for the SU to be able to participate in any OTAR process with the TKMD.
    - **Inventory:** The TKMD can perform an inventory of an individual SU to determine the number of keys and other OTAR parameters contained in the SU.
    - **Change Message Number/RSI:** The CO can change the Radio Set Identifier (OTAR ID) of the SU if desired and can update the OTAR message numbers to reconcile the SU with the record kept by the TKMD.
    - **Change Active Key Set:** The TKMD can instruct the SU to change its active key set to facilitate operation in OTAR systems where both an active and inactive keyset are in use.

4.3 TKMD Services Available to the Authenticated Network User Role

- **Encrypted File Share** (requires Crypto-Officer entry of IP addresses for sharing and provisioning of AES-256 File Transfer Base Key used to derive the file dependent File Transport Key used to File Key Wrap the file to be transported)
    - Key Kettle File Share
    - OTAR radio SU File Share

4.4 TKMD Services Available to the Authenticated Crypto-Officer

- **Validate Crypto-Officer Name/Password**: Entry of a CO Name/ Password is required to access anything other than the "Home" page on the TKMD. The only function supported by the "Home" page is entry of the CO Name/Password. Time and retry restrictions are applied to minimize the success of automated attack.
- **Change Crypto-Officer Name/Password:** After entry of the valid Crypto-Officer Name/Password, the Crypto-Officer will be able to access a page which allows resetting of the Crypto-Officer Name/Password. Strong password criteria are applied, and inadequate passwords are rejected.
- **Erase Crypto-Officer:** Erases Crypto-Officer username and password and resets them back to the default username and password.
- **Firmware Update:** Update the module using a TLSv1.2 Red Ethernet encrypted connection and a browser file upload function. A second file containing the HMAC SHA-256 hash for the Firmware image must be uploaded to complete the firmware update process. If the hash value calculated by the TKMD does not match the hash value contained in the second file upload, the update fails.
- **Zeroize TKMD**: The Crypto-Officer can initiate a Zeroize of all key parameters.
- **Initiate Self-Test**: The Crypto-Officer can initiate Self-Test for the TKMD.
- **Reset TKMD:** Force a power-up reset of the TKMD.
- **Version Query:** The Crypto-Officer can access the revision information on the TKMD firmware from a web page.
- **Extract Error Log**: The Crypto-Officer can upload the current Error/History Log. No CSPs are contained in the log file.
- **Factory Default**: The Crypto-Officer can initiate a reset of the TKMD to factory defaults.
- **Base Station Configuration**: The Crypto-Officer can set up the Base Station/Configuration, IP address, ports etc. to be used by the TKMD.
- **IP Address**: The Crypto-Officer can set the IP address that will be used by the TKMD. TLSv1.2 and DTLSv1.2 parameters are factory configured and cannot be changed by the Crypto-Officer.
- **SU Configuration**: The Crypto-Officer can manually configure each OTAR radio SU including key assignments.
- **Delete SU**: The Crypto-Officer can delete an OTAR SU from the internal encrypted non-volatile data storage.
- **KFD Import:** The Crypto-Officer must select KFD Import and connect a KFD device to the KFD port to import key material from the KFD device. The use of the KFD requires the action of the Crypto-Officer and is disabled after the Crypto-Officer logs off the TKMD. The TKMD cannot be left in the KFD mode without continuing action from the Crypto-Officer.
- **KFD Export:** The Crypto-Officer must select KFD Export and connect a TKMD device to the KFD port to export key material from the TKMD to a User radio SU device. The use

of the KFD Export requires the action of the Crypto-Officer and is disabled after the Crypto-Officer logs off the TKMD. The TKMD cannot be left in the KFD Export mode without continuing action from the Crypto-Officer.

- **Configure Key Kettle File Import:** If configured by the Crypto-Officer, the TKMD can import to the SU updated Key Kettle files over a network. The sharing is done using Key Kettle File encrypted with a AES-256 the File Transport Key and is accomplished over the Red Ethernet TLSv1.2 encrypted Ethernet port. A separate and distinct TLSv1.2 encrypted connection is established for the transfer of each file. Once imported and decrypted, the new Key Kettle File information is automatically used to update the TEKs and KEKs for each radio SU using the referenced key material.
- **Configure SU File Sharing**: If configured by the Crypto-Officer, the TKMD can automatically share encrypted SU Configuration Files with a remote IP address using a TLSv1.2 encrypted Red Ethernet Connection. A separate and distinct encrypted IP connection is established for the transfer of each file. TKMD file sharing requires both TKMDs that file share have a provisioned AES-256 key File Transport Base Key from which to derive a common file encryption key (File Transport Key) unique to the individual file. The remote connection point can be another TKMD or a file server. In the case of a file server, the file server need not be able to decrypt the file, only to save the latest file and to provide it on a secure TLSv1.2 connection to the remote TKMD upon request.
- **Manually Initiate OTAR**: The Crypto-Officer can manually initiate all OTAR operations for a specific OTAR radio SU including Zeroization.
- **SU Status**: The Crypto-Officer can view status information on the connectivity and status of all configured OTAR radio SUs.
- **OTAR Operation**: Manually providing Project 25 OTAR service through a network or RF Base Station connection.
- **Enabling Automatic OTAR Operation:** The Crypto-Officer can enable the TKMD to automatically provide OTAR service to any Authenticated Subscriber Unit. This is the normal unattended operation mode of the TKMD.

4.5 TKMD Services Available Without a Role

- Zeroize using TKMD Zeroize button.
- Zeroize by removing both TKMD power sources.
- Reset TKMD by removing/restoring the main power connection (thus initiating self-tests)
- Monitor LED Status

5. Cryptographic Algorithms

5.1. Approved Algorithms

The TKMD supports the following Approved algorithms*:

Table 5: Approved Algorithms

CAVP Cert. #	Algorithm	Mode/Method	Standard	Description	Use/ Function
C1775	AES	CBC, ECB, OFB, GCM, KW	SP 800-38A SP 800-38D SP 800-38F	Key Size: 256	Encryption, Decryption, Authentication OFB and CBC modes are used in Project 25 OTAR messages. GCM and KW are used in TLSv1.2 and DTLSv1.2
Vendor Affirmed	CKG		SP 800-133	Key generation using unmodified output of the DRBG	Key Generation
C1775	CVL	TLS KDF	SP 800-135rev1	SHA-384	Key Derivation
C1775	DRBG	Hash_DRBG	SP 800-90Arev1	SHA-256	Random Bit Generation Used to generate key for internal storage encryption and to develop keys for OTAR usage when enabled
A881	ECDSA	Keypair Generation	FIPS PUB 186-4	P-521	Keypair Generation
C1775	HMAC	SHA-256	FIPS PUB 198-1	Key Size: 256	Message Authentication Used to verify integrity of Firmware Upload,

CAVP Cert. #	Algorithm	Mode/Method	Standard	Description	Use/ Function
					verify passwords and for TLSv1.2.
C1775	RSA	SigGenPKCS1.5 SigVerPKCS1.5	FIPS PUB 186-4	n=2048 (SHA-384)	Signature Generation, Signature Verification
C1775	SHS	SHA-256 SHA-384	FIPS PUB 180-4		Message Digest Generation
A862	SP 800-108 KDF	Feedback	SP800-108	HMAC-SHA2-256	Key Derivation
Vendor Affirmed	KAS-SSC	P-521	SP 800-56A rev 3	EC DH Key agreement methodology provides 256 bits of encryption	Key Agreement during TLS 1.2
N/A	KTS	AES Cert. #C1775 (GCM, KW)	SP800-38F	Key establishment methodology provides 256 bits of encryption strength	Key Encryption

*There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

5.2. Non-Approved but Allowed Algorithms

Table 6: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use/ Function
AES MAC	AES Cert. #C1775, vendor affirmed; P25 AES OTAR	OTAR
NDRNG	N/A	Derived from PIC32 Thermal Noise Source to seed the SP800-90A Hash_DRBG (256 bits)

5.3. Non-Approved Algorithms

The module supports DES, which shall not be used in the Approved mode.

5.4. Critical Security Parameters (CSPs) and Public Keys

Table 7: CSP Definition

CSP Identifier	Description/Usage
Traffic Encryption Key (TEK)	TEKs for OTAR are AES OFB 256-bit keys and are entered from a KFD in plaintext format or are imported as part of an encrypted OTAR radio SU file or Key Kettle file uploaded through the TLSv1.2 encrypted Red Ethernet interface. TEKs are stored encrypted in individual radio SU files in non-volatile memory. The radio SU files are encrypted with the File Storage Key.
Key Encryption Key (KEK)	KEKs are AES-256-bit keys used for SU authentication in OTAR are entered from a KFD in plaintext format or are imported as part of an encrypted OTAR radio SU file or Key Kettle file uploaded through the TLSv1.2 encrypted Red Ethernet interface. KEKs are stored encrypted in individual radio SU files in non-volatile memory. The radio SU files are encrypted with the File Storage Key.
File Storage Key	The AES-256 key used to store radio SU files and Key Kettle files is generated by the DRBG and is stored in tamper-protected volatile memory when generated. If this key is erased, the stored radio SU or Key Kettle files cannot be successfully decrypted. Failure to decrypt when reading these

CSP Identifier	Description/Usage
	files causes the entire file to be erased from Non-volatile memory
File Transport Base Key	This AES-256 key is loaded in an encrypted format as part of the Firmware Update process. This key is never output from the TKMD and further is never used to encrypt/decrypt a file. This base key is used along with the file name and a file type specific nonce to derive (HMAC SHA-256) an encrypt/decrypt key used with the file transfer. The key is stored in tamper-protected volatile memory. If erased, the File Transfer process cannot take place.
File Transport Key	The File Transport key is a derived key based on the File Transfer Base Key, the file name and a nonce. An HMAC SHA-256 is used to derive this key. The Key Derivation conforms to SP 800-108.
DRBG_Seed	Entropy input derived from PIC32 Thermal Noise Source and nonce.
DRBG_State	Hash_DRBG (SHA-256) state V (440-bit) and C (440-bit).
Crypto-Officer Password	8-10-character ASCII value
Password Storage Key	HMAC-SHA-256 key used to store Crypto-Officer passwords
Firmware Load Key	HMAC-SHA-256 key used to authenticate firmware images loaded by the module.
TLSv1.2/DTLSv1.2 Volatile/Temporal CSPs (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bit keys)	
TKMD Server Private Key	RSA private key for authenticating the TLSv1.2 handshake for TKMD server connections

CSP Identifier	Description/Usage
TKMD Client Private Key	RSA private key for authenticating the TLSv1.2 handshake for TKMD client connections
KAS_Private	Private component of an ECC (P-521) key pair provided by the local participant, used for EC Diffie-Hellman shared secret generation.
KAS_SS (TLS Pre-master Secret)	The EC Diffie-Hellman shared secret. ECC: (security strength 256-bits).
TLS Master Secret	Derived from the TLS Pre-master Secret.
IP Session Key	IP Session key is a 256-bit AES-GCM Key generated by an ephemeral Diffie-Hellman key negotiation. It is not output from the module, is not stored in non-volatile memory and is erased once the IP session tunnel is closed.

Table 8: Public Keys

Public Key	Description / Usage
TKMD Server Public Key	RSA Public Key for initiating TLSv1.2 handshake for TKMD server connections
TKMD Client Public Key	RSA Public Key for initiating TLSv1.2 handshake for TKMD client connections
KAS_Public	ECC (P-521) key pair received from the remote participant, used for EC Diffie-Hellman shared secret generation.

Key Zeroization

When the TKMD is zeroized all plain text private and secret keys are erased. Key material contained in encrypted radio SU or Key Kettle Files is no longer accessible due to the erasure of

the AES 256-bit File Storage Key (stored in Volatile Memory) used to encrypt these files. The TKMD can be zeroized in one of the following ways:

a) Removing both power sources.

b) Pressing the Zeroize switch on the front of the TKMD.

AES GCM IG A.5 Compliance

AES GCM is used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52 Section 3.3.1. The construction of the 64-bit nonce_explicit part of the IV is deterministic via a monotonically increasing counter. The module ensures that that when the deterministic part of the IV uses the maximum number of possible values, a new session key is established. The module generates new AES-GCM keys if the module loses power.

5.5. CSP Access Types

Table 9: CSP Access Types

CSP Access Type	Description
D – Decrypt CSP	• Decrypts radio SU and Key Kettle files which include KEKs and TEKs retrieved from non-volatile memory using the File Storage Key • Decrypts radio SU and Key Kettle files which include KEKs and TEKs received via the Red Ethernet Interface using the File Transport Key
E – Encrypt CSP	• Encrypts radio SU and Key Kettle files which include KEKs and TEKs for storage in non-volatile memory using the File Storage Key • Encrypts TEKs and KEKs for OTAR using other KEKs • Encrypts radio SU and Key Kettle files which include KEKs and TEKs prior to sending via the Red Ethernet Interface using the File Transport Key
G – Generate CSP	• Generate CSP using the SP 800-90A DRBG
S – Store CSP	• Stores the encrypted radio SU File or Key Kettle File (including TEKs and KEKs) in non-volatile memory • Stores File Storage Key or File Transport Key in tamper-protected volatile memory.
U – Use CSP	Uses the CSP internally for encryption/decryption services
Z – Zeroize CSP	Zeroizes CSP

Table 10: CSP versus CSP Access

Service	CSP											Role			
	Traffic Encryption Key (TEK)	Key Encryption Key (KEK)	File Storage Key	File Transport Base Key	File Transport Key	DRBG_Seed	DRBG_State	Crypto-Officer Password	Password Storage Key	Firmware Load Key	TLS\DTLS CSPs	SU User Role	Network User Role	Crypto-Officer Role	No Role Required
Validate Crypto-Officer								U	U		G, U, Z			✓	
Change Crypto-Officer								G, U	U					✓	
Erase Crypto-Officer											G, U, Z			✓	
Firmware Update			Z, G		Z, D, S						G, U, Z			✓	
Zeroize TKMD	Z	Z			Z						G, U, Z	✓		✓	✓
Initiate Self Test											G, U, Z			✓	✓
Reset TKMD											G, U, Z			✓	✓
Version Query											G, U, Z			✓	
Extract Error Log			Z, G											✓	
Factory Default	Z	Z			Z						G, U, Z			✓	✓
Base Station Configuration											G, U, Z			✓	
IP Address											G, U, Z			✓	
SU Configuration	G, S	G, S									G, U, Z			✓	
Delete SU	Z	Z	U, D, E								G, U, Z			✓	
KFD Import/Export	D, S	D, S									G, U, Z			✓	
Configure Key Kettle Import	G, S	G, S	U, D, E		U, D, E						G, U, Z			✓	
Configure SU File Sharing														✓	
Manually Initiate OTAR	U, Z	U, Z									G, U, Z			✓	
Enabling Automatic OTAR Operation			U, D, E											✓	
SU Status														✓	
OTAR Operation	U, Z	U, Z										✓		✓	

Service	CSP											Role			
	Traffic Encryption Key (TEK)	Key Encryption Key (KEK)	File Storage Key	File Transport Base Key	File Transport Key	DRBG_Seed	DRBG_State	Crypto-Officer Password	Password Storage Key	Firmware Load Key	TLS\DTLS CSPs	SU User Role	Network User Role	Crypto-Officer Role	No Role Required
Encrypted File Share				U	U								✓		

6. Physical Security

The TKMD is a production grade, multi-chip standalone cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 Physical Security requirements.

The TKMD is entirely contained within an aluminum production grade enclosure that has been filled with hard, black, opaque epoxy potting. The potting extends from the front panel to 2 inches short of the rear edge of the aluminum enclosure. A lithium-ion rechargeable battery is mounted at the rear of the enclosure and can be accessed by removing the rear cover. The cryptographic boundary for the TKMD extends from the front panel to the rear extent of the epoxy potting. The rear cover and battery are not part of the module boundary. The rear cover only provides access to the replaceable backup battery and not to any part of the TKMD.

The front panel and top aluminum cover cannot be removed since they are permanently bonded to the aluminum wrap around case by the epoxy potting. The TKMD printed circuit board cannot be removed or accessed due to the epoxy potting.

Anti-Tamper protection includes:

- Over Voltage Sensing
- Under Voltage Sensing
- Over Temperature Sensing
- Under Temperature Sensing
- (Optional) Physical Tamper Sensing of all critical storage locations with file trace anti-tamper films.

Sensing of a tamper condition erases all CSPs from volatile memory.

No maintenance access interface is available.

7. Self-Tests

The TKMD performs the following self-tests:

a) Power up and On-Demand tests:
   - Firmware Integrity Test (HMAC SHA-256)
   - AES-256 ECB encrypt/decrypt KATs
   - AES-256 GCM encrypt/decrypt KATs
   - HMAC SHA-256 KAT
   - Hash_DRBG KAT
   - SHA-256 KAT
   - SHA-384 KAT
   - RSA Sign/Verify KATs
   - TLS KDF KAT
   - SP800-108 KDF KAT

   If a self-test fails, the module will enter a critical error state and cannot be recovered. The module must be returned to the manufacturer for service.

b) Conditional Tests:
   - Firmware load test using HMAC SHA-256
   - NDRNG Continuous test

c) Critical Functions Test
   SP 800-90A DRBG Section 11.3 Health Checks

8. Mitigation of Other Attacks Policy

The TKMD is not designed to mitigate any specific attacks outside those required by FIPS 140-2.

9. Security Rules and Guidance

The TKMD enforces the following security rules:

9.1. FIPS 140-2 Imposed Security Rules

The following security rules are imposed by FIPS 140-2 requirements:

1) The TKMD inhibits all input and output data paths whenever an error state exists or during self-tests.

2) The TKMD inhibits all input and output data paths during key loading via the KFD Interface excluding the KFD Interface.

3) Authentication data is not output during entry.

4) Secret cryptographic keys are entered in one of the following ways:

a) In a plaintext manner via the separate KFD Interface under the direct control of an authenticated Crypto-Officer.

b) As part of an encrypted file uploaded automatically on the TLSv1.2 encrypted Red Ethernet Interface.

c) Generated by an Approved DRBG under the direction of the Crypto-Officer.

5) The TKMD enforces Identity-Based authentication.

6) The TKMD supports a Crypto-Officer Identity and a User Identities.

a) The Crypto-Officer Identity is authenticated by entry of a CO Name and an 8 to 10 character ASCII Password on the TLSv1.2 encrypted Red Ethernet interface.

b) The User Identity requires prior provisioning (IDs and IP addresses) entered by the Crypto-Officer and possession of the symmetric AES-256 key used to encrypt the OTAR or file upload. File upload is done over the TLSv1.2 encrypted Red Ethernet interface with a new ephemeral key establishment for each file exchange. OTAR exchanges are accomplished over one of the black Base Station interfaces with AES-256 encrypted messages. All key material transferred on the OTAR function is AES Key Wrap encrypted with a symmetric AES-256 Key Encryption Key (KEK).

7) When the TKMD is powered off, an IP session times out due to inactivity or after the Crypto-Officer logs off and attempts to log back in to the TKMD, the Crypto-Officer must reauthenticate.

8) The TKMD implements all firmware using a “C” high-level language. The firmware is loaded as a single non-modifiable executable image running on an infinite loop “bare metal” processor without an operating system.

9) The TKMD stores all files containing secret and private keys in an encrypted form. Keys are read and decrypted only as needed to support TKMD operation. No external access is provided to any encrypted or decrypted secret or private keys. The AES-256 key used to encrypt stored keys is locally generated by the TKMD using an Approved DRBG and is never output from the TKMD.

10) The TKMD provides a means to ensure that each key entered into or stored within the module is associated with the correct entities to which the key is assigned.

11) The TKMD denies external access to plaintext or encrypted keys contained within the module.

12) The TKMD conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A requirements.

13) The TKMD enters a Critical Error state if the Cryptographic Algorithm Test or the NDRNG test fails.

14) The TKMD enters a firmware failure state if the Firmware Load test fails.

15) If all power up self-tests pass, the yellow Main LED will begin to flash at a 25 per second rate.

16) The TKMD will not perform any cryptographic operations while in an error state.

17) Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

9.2. Christine Wireless Inc. Imposed Security Rules

The following security rules are established by Christine Wireless, Inc. for the TKMD;

1. All connections to the TKMD web server must be through https TLSv1.2.
2. Only one https connection at a time is permitted.
3. The only key exchange supported is Elliptic Curve Diffie-Hellman P-521.
4. All web pages with sensitive content can only be accessed after entering the Crypto-Officer Username and Password.

9.3. Crypto-Officer and User Guidance

Administration of the TKMD in a secure manner (Crypto-Officer)

The TKMD requires no special administration for secure use after it is setup for use in a FIPS Approved manner.

Assumptions regarding User Behavior

The TKMD has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

Approved Security Function, Ports and Interfaces available to Users

The TKMD services available to the User Role are listed in section 4.2.

User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the TKMD.

10. Definitions

AES	Advanced Encryption Standard
ALGID	Algorithm Identifier
CBC	Cipher Block Chain
CSP	Critical Security Parameter
DTLS	Datagram Transport Layer Security
DES	Digital Encryption Standard
ECB	Electronic Code Book
GCM	Galois Counter Mode
HMAC	Keyed Message Authentication Code
IV	Initialization Vector
KEK	Key Encryption Key
KFD	Key Fill Device
KID	Key Identifier
LED	Light Emitting Diode
DRBG	Deterministic Random Bit Generator
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feed Back encryption
OTAR	Over the Air Rekey
RAM	Random Access Memory
TEK	Traffic Encryption Key
TKMD	Tactical Key Management Device
TLS	Transport Layer Security