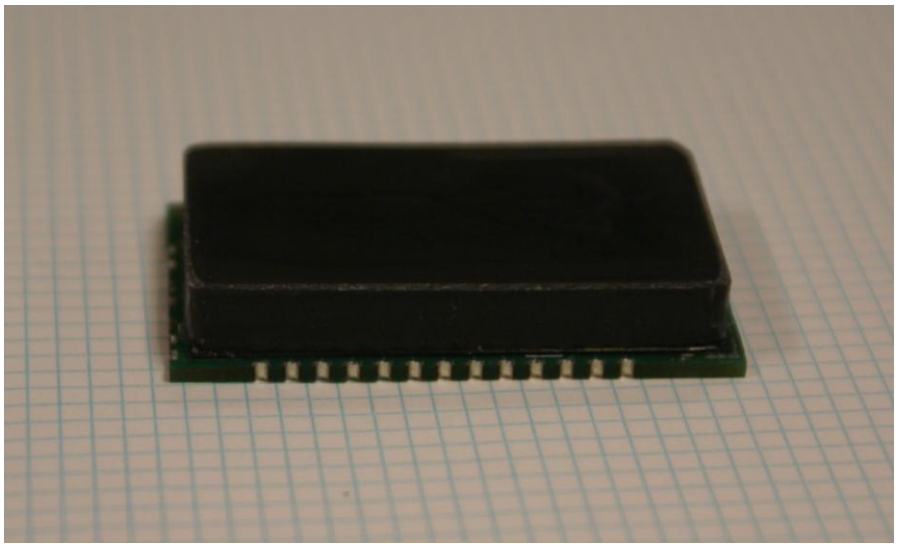
Comtech Mobile Datacom Corporation
Transceiver Cryptographic Module (TCM)

(Firmware Version: 0.1.L)
(Hardware Part/Version: C80101 Rev. 2)



FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.1

Prepared by:

Comtech Mobile Datacom Corporation
20430 Century Boulevard
Germantown, MD 20874
Phone: (240) 686-3300
Fax: (240) 686-3301
http://www.comtechmobile.com/

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2009-06-29	David Wenzel	Initial draft.
0.2	2009-07-28	David Wenzel	Updated images of module. Added details for Crypto-Officer setup and management of device.
0.3	2009-08-04	David Wenzel	Changed from single-chip to multi-chip embedded module; Added Software Erase service;
0.4	2009-09-01	David Wenzel	Added Authenticated User role;
0.5	2009-09-14	David Wenzel	Added hardware part/version info; Added information on the epoxy covering;
0.6	2009-10-07	David Wenzel	Updated firmware version number;
0.7	2009-11-07	David Wenzel	Added Set Password services;
0.8	2009-11-18	David Wenzel	Updates from Lab Comments
0.9	2010-01-14	David Wenzel	Updated firmware version number;
1.0	2016-03-23	Chris Thorne	Updated for changes in NIST requirements.
1.1	2016-04-18	Chris Thorne	Addressed name and formatting issues.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Transceiver Cryptographic Module (TCM) from Comtech Mobile Datacom Corporation. This Security Policy describes how the Transceiver Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/cmvp/

The Transceiver Cryptographic Module is referred to in this document as the Crypto Module, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Comtech website (http://www.comtechmobile.com) contains information on the full line of products from Comtech.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Comtech and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Comtech.

2 Transceiver Cryptographic Module (TCM)

2.1 Overview

Comtech Mobile Datacom offers secure, real-time packet data messaging and position reporting services using L-Band satellite networks. Comtech's technology allows government agencies to communicate accurately, securely, and in a timely manner with vehicles through mobile satellite communications. This end-to-end satellite-based solution includes earth stations located strategically around the world, leased satellite capacity, mobile terminals, and tailored software solutions that meet and support Comtech's clients' critical needs.

The Transceiver Cryptographic Module (TCM) is a compact hardware module with a firmware component for implementation of cryptographic algorithms. The Crypto Module, in connection with Comtech's ASDR Transceiver, enables secure over-the-air communications. The module provides a serial interface for communication over a pair of SPI ports.

2.2 Module Specification

The Crypto Module hardware consists of a 32-bit ARM processor and supporting components. A block diagram of the module and interfaces is given in Figure 1 below, and the cryptographic boundary is depicted in this diagram.

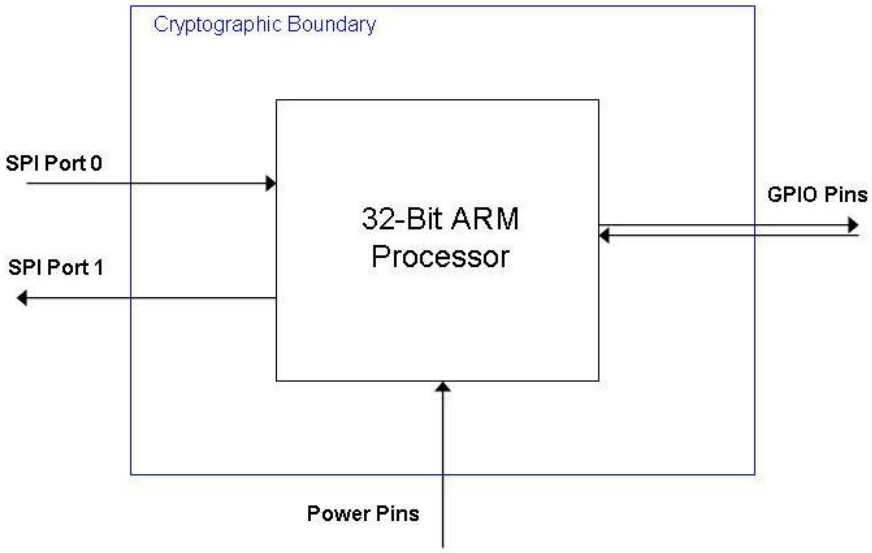


Figure 1 – Transceiver Cryptographic Module Block Diagram

The module contains a single Printed Circuit Board (PCB) encased in epoxy. The following is a list of the key circuit components and interfaces:

1. 32-bit ARM Processor: the processor contains firmware to control communication with external devices and perform cryptographic functions.

2. SPI Ports: the Serial Peripheral Interface ports provide an interface with the Crypto Module for passing data and control information.

3. GPIO Pins: the GPIO pins provide an interface for hand-shaking between the Crypto Module and external devices.

The Transceiver Cryptographic Module is a multi-chip embedded module that meets overall level 2 FIPS 140-2 requirements. The module is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference (EMI)/ Electromagnetic Compatibility (EMC)	3
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.3 Module Interfaces

The module provides a serial interface to external devices over a pair of SPI buses. Application Programming Interface (API) commands can be provided to the module using the serial interface. The interface consists of two single direction SPI ports:

- SPI Port 0 provides a path for data to be sent to the Crypto Module
- SPI Port 1 provides a path to receive data from the Crypto Module

The module also provides access to a set of GPIO pins. These pins are primarily intended for hand-shaking with external devices.

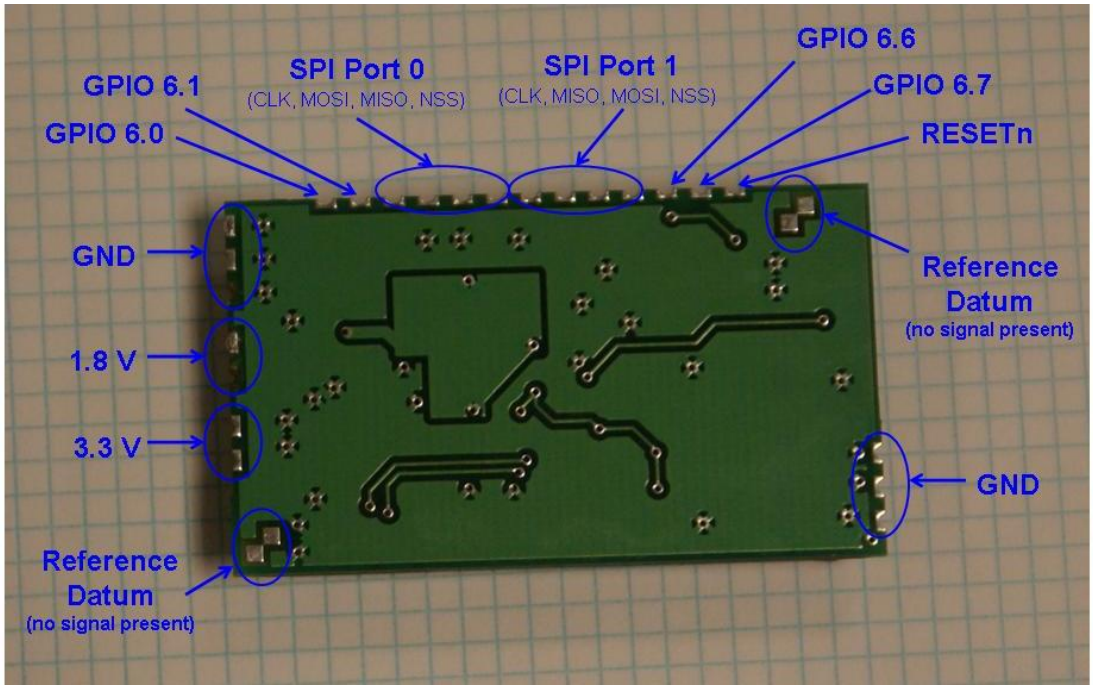


Figure 2 - Transceiver Cryptographic Module Interface Pads

The module's physical interfaces are composed of connector pin pads, as shown in Figure 2. A subset of the connector pins is used for providing data/control input or data/status output. The remaining pins are used to interface with an external power source. Functions of active pins are listed in Table 2.

Table 2 – Transceiver Cryptographic Module Pin-out

Pin	Pin Description
1	3.3 V
2	3.3 V
3	1.8 V
4	1.8 V
5	Ground (GND)
6	GND
7	GND
8	GPIO 0
9	GPIO 1
10	SPI 0 CLK
11	SPI 0 MOSI
12	SPI 0 MISO
13	SPI 0 NSS
14	SPI 1 CLK
15	SPI 1 MISO
16	SPI 1 MOSI
17	SPI 1 NSS
18	GPIO 6 (not currently used)
19	GPIO 7 (not currently used)
20	CRYPTO RESET
21	GND
22	GND
23	GND

All of the physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 3 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Transceiver Cryptographic Module Port/Interface
Data Input	Pin 10, Pin 11, Pin 12, Pin 13
Data Output	Pin 14, Pin 15, Pin 16, Pin 17
Control Input	Pin 8, Pin 10, Pin 11, Pin 12, Pin 13, Pin 20
Status Output	Pin 9, Pin 14, Pin 15, Pin 16, Pin 17
Power	Pins 1, 2, 3, 4, 5, 6, 7, 21, 22, 23

The module exposes pads for interface connections along the edges of the PCB, as shown in Figure 2. Several non-sensitive signals are also exposed on the bottom and top edges of the PCB board. These exposed connections already reference to pins and mappings discussed above. These include power interfaces (+1.8V, +3.3V and GND). Additionally, connections do not have any signal present at all. All of these connections are not relevant to the cryptographic module's security since they are do not perform data input or data output. There are also no traces that indicated the interconnection of parts of the module.

2.4 Roles and Services

The module supports role-based authentication. There are three roles in the module that operators may assume: Normal User role, Authenticated User role, and Crypto-Officer (CO) role. The Normal User role is an unauthenticated role assumed by the end users for general device services. The Authenticated User role is an authenticated role used for performing approved security functions, including encryption, decryption, and FIPS algorithm testing. The Crypto-Officer role is an authenticated role used to perform administrative services on the cryptographic key table. All users access the module via the SPI interfaces provided on the module. Locally, an operator connects to the module as a Normal User first, and then enters a password to log in as an Authenticated User or a Crypto-Officer.

2.4.1 Normal User Role

The Normal level user is an unauthenticated role which has access to the following services:

Table 4 – Mapping of Normal User Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
General Information	Retrieves status information, hardware and firmware version information as well as the Crypto Module serial number	Command	Status output	--
Authentication	Current level of authentication; if password, change access level to an authenticated role	Command and password	Authentication status; Change in access level;	Password – Execute
Software Erase	Erases application code image from FLASH and reboots module	Command	Acknowledgment output	--

Service	Description	Input	Output	CSP and Type of Access
Self-Test	Perform a series of self-tests including firmware integrity and cryptographic Known Answer Tests	Power off / Power on	Status results	--

2.4.2 Authenticated User Role

The Authenticated User is an authenticated role which has access to the following services:

Table 5 – Mapping of Authenticated User Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
General Information	Retrieves status information, hardware and firmware version information as well as the Crypto Module serial number	Command	Status output	--
Encryption	Encrypts packet data	Command and data	Encrypted packet	Traffic Keys – Execute
Decryption	Decrypts packet data	Command and data	Decrypted plaintext	Traffic Keys – Execute
FIPS test algorithms	Perform FIPS tests	Command and data	Test result data	--
Authentication	Current level of authentication; if password, change access level to an authenticated role	Command and password	Authentication status; Change in access level;	Password – Execute
Set Password	Changes Authenticated User password	Command and password	Set Password result	Password – Read/Write
Software Erase	Erases application code image from FLASH and reboots module	Command	Acknowledgment output	--
Self-Test	Perform a series of self-tests including firmware integrity and cryptographic Known Answer Tests	Power off / Power on	Status results	--

2.4.3 Crypto-Officer Role

Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Table 6 – Mapping of Crypto-Officer Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
General Information	Retrieves status information, hardware and firmware version information as well as the Crypto Module serial number	Command	Status output	--

Service	Description	Input	Output	CSP and Type of Access
Encryption	Encrypts packet data	Command and data	Encrypted packet	Traffic Keys – Execute
Decryption	Decrypts packet data	Command and data	Decrypted plaintext	Traffic Keys – Execute
FIPS test algorithms	Perform FIPS tests	Command and data	Test results	--
Authentication	Current level of authentication; if password, change access level to an authenticated role	Command and password	Authentication status; Change in access level	Password – Execute
Set Password	Changes Authenticated User or Crypto-Officer password	Command and password	Set Password result	Password – Read/Write
Software Erase	Erases application code image from FLASH and reboots module	Command	Acknowledgment output	--
Self-Test	Perform a series of self-tests including firmware integrity and cryptographic Known Answer Tests	Power off / Power on	Status results	--
Key Management	Add or delete keys from the table of cryptographic keys	Command and data	Acknowledgement	Security Keys – Execute Traffic Keys – Execute Traffic Keys – Write

2.4.4 Authentication Mechanism

All users access the module through directly connected SPI ports. Authenticated Users and Crypto-Officers authenticate themselves using passwords.

Table 7 – Authentication Mechanisms

Authentication Type	Strength
Passwords	The minimum length of the password is six alphanumeric characters with any printable symbols. Assuming only 94 characters with repetition, the chance of a random attempt falsely succeeding is 1 in (94^6 =) 689,869,781,056. Due to the interface speed of the module (115,200 bps), less than 144,000 authentication attempts could be performed within one-minute. This means there would still be a less than 1 in 4.79 x 10^6 chance of such an attack working if repeated over one-minute.

2.5 Physical Security

The Transceiver Cryptographic Module is a multi-chip embedded cryptographic module. The module is contained on a single PCB, whose top half is encased in epoxy. The module's epoxy cover is resistant to probing and is opaque within the visible spectrum. More information on the epoxy characteristics can be found in the Technical Data sheet for the 3M Epoxy Potting Compound DP270. The tamper-evident epoxy is applied by Comtech before providing the module to the Crypto-Officer. The module has been designed to satisfy level 2 physical security requirements.

The cryptographic boundary is defined as encompassing the "top," "front," "left," "right," "rear," and "bottom" surfaces of module. Figures 5, 6, and 7 show top, side, and bottom views of an epoxy encased Crypto Module.

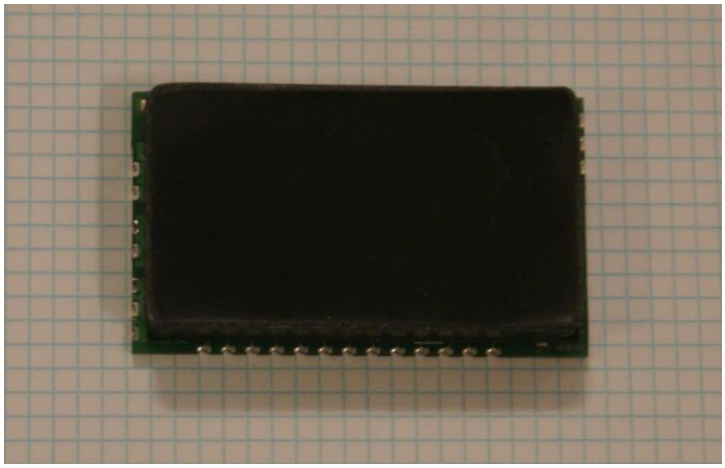


Figure 3 – Transceiver Cryptographic Module Top View

Figure 4 – Transceiver Cryptographic Module Side View

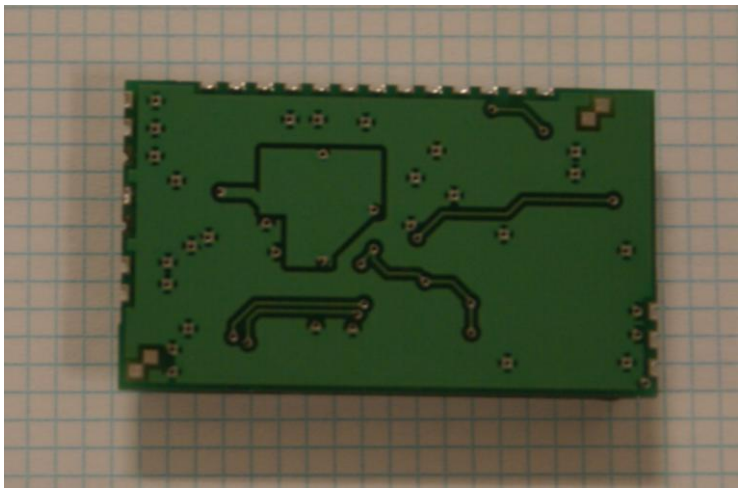


Figure 5 – Transceiver Cryptographic Module Bottom View

The module conforms to the Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC) requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, and Class B (for home use).

2.6 Operational Environment

The operational environment requirements do not apply to the Transceiver Cryptographic Module, because the module does not provide a general-purpose operating system (OS) to the user. The OS is not externally accessible and only the module's custom written firmware provides a logical interface into the module. The module provides a method to update the firmware in the module only while operating in a non-FIPS mode.

2.7 Cryptographic Key Management

The cryptographic module implements the following FIPS-approved algorithms:

- AES – CBC; 128, 192, and 256
- AES – CFB; 128, 192, and 256
- Triple-DES – CBC; Keying option 1, encrypt/decrypt
- SHA-1 Byte oriented
- SHA-256 Byte oriented
- HMAC SHA-1[1]
- HMAC SHA-256

AES Certificate #1201; Triple-DES Certificate #869; SHS Certificate #1106 & HMAC Certificate #698.

The cryptographic module implements the following non-FIPS-approved algorithms:

- Digital Encryption Standard (DES)
- Triple DES – CBC, Keying option 2 (2-key Triple DES)
- Towitoko MAC algorithm

The module supports the critical security parameters found in Table 8.

[1] Key lengths that are less than 112 bits (14 bytes) in length cannot be used for HMAC SHA-1 in FIPS mode, except for legacy-use HMAC-SHA-1 verification.

Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DES Traffic Keys	Triple-DES 192-bit CBC key	Generated externally; input in plaintext[2]	Never output from module	Stored in RAM in plaintext	Erasing from RAM	Encrypts/decrypts traffic data
AES Traffic Keys	AES 128, 192, and 256-bit CBC and CFB keys	Generated externally; input in plaintext[2]	Never output from module	Stored in RAM in plaintext	Erasing from RAM	Encrypts/decrypts traffic data
Security Keys	AES 256-bit CFB keys	Generated externally; hardcoded in application	Never output from module	Stored in Flash in plaintext	Erasing flash image	Decrypts traffic keys
Passwords	Authenticated User and Crypto-Officer passwords	Generated externally; defaults hardcoded in application; new values input in plaintext	Never output from module	Stored in Flash in plaintext	Erasing flash image	Authenticates users

[2] *The methods used for key wrapping (AES CBC or CFB) are not compliant with the NIST key transport standards, and are only allowed for usage in the approved mode through December 31, 2017 as per FIPS 140-2 IG D.9. After December 31, 2017, the keys are considered to be entered into the module in plaintext.*

2.7.1.1 Key Generation

All keys are generated externally to the module.

2.7.1.2 Key Storage

All Traffic keys are stored in RAM in plaintext along with pre-computed subkeys. Security keys and the authentication passwords are stored in Flash in plaintext.

2.7.1.3 Key Entry and Output

Security Keys and the default passwords are hardcoded in the application firmware. Traffic Keys are loaded into the module's RAM electronically over the SPI interface. Traffic keys are sent in plaintext[2]. The module does not support the output of cryptographic keys or CSPs.

2.7.1.4 Key Zeroization

Traffic Keys are zeroized by erasing from RAM. All other keys and CSPs are zeroized by erasing the Flash image.

2.8 Self-Tests

The Transceiver Cryptographic Module performs the following self-tests at power-up:

- Software integrity check using Cyclic Redundancy Check (CRC)-32 checksum
- Known Answer Tests (KATs)
    - Triple-DES-CBC encrypt/decrypt KAT
    - AES-CBC encrypt/decrypt KAT
    - AES-CFB encrypt/decrypt KAT
    - SHA-1 HMAC KAT
    - SHA-256 HMAC KAT

If any of the above self-tests fail, the module sends a failure response on the serial port and the module locks down. Otherwise, a success indicator message is posted on the serial port.

2.9 Design Assurance

The source code is primarily written in C. Comtech uses Borland StarTeam to perform source code versioning and management.

2.10 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Secure Operation

The Transceiver Cryptographic Module meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

The module is available directly from Comtech Mobile Datacom Corporation and is shipped via a third party shipping company, such as FedEx or UPS. The module, sealed with an anti-static bag, is provided in a carton. The Crypto-Officer must inspect the box, packing materials, and module for signs of tamper, including damage to the box, packing materials, or the module itself. If any signs of tamper are evident, the module should not be utilized and instead should be returned to Comtech Mobile Datacom Corporation. The Crypto-Officer (CO) is responsible for key management and maintenance in the FIPS mode of operation.

3.1.1 Key Management

After physically installing the module on the Host, the Crypto-Officer must initialize the module with cryptographic key data. The Crypto Module comes preloaded with all necessary firmware components, and when powered on, the module will jump to the main application code and enter FIPS mode. The Crypto-Officer should confirm successful boot-up by verifying the Power-Up message sent back to the Host from the module.

The module does not initially contain any traffic key data. To load traffic keys, the CO must first authenticate using the Crypto-Officer password. After authentication, the CO will be able to load traffic keys to the Crypto Module key table using API commands. When all necessary keys have been loaded, the Crypto-Officer should terminate the authenticated session.

3.1.2 Management

The Crypto-Officer manages the traffic keys in the Crypto Module key table. The CO should add and remove keys as required of the device. To manage the key table, the CO must begin an authenticated session using the Crypto-Officer password. Care should be taken to protect all sensitive key and password information.

The module operates within FIPS mode whenever it enters the main application firmware. To clear the module into a non-FIPS device, the main application code must be erased using the appropriate API command. New application firmware can only be loaded to the module from a boot loader in this non-FIPS state.

3.2 Authenticated User Guidance

Authenticated Users have access to approved security functions but do not have the ability to configure sensitive information on the module. Authenticated Users should be careful not to provide traffic key information to other parties.

The module operates within FIPS mode whenever it enters the main application firmware. Once an operator has performed the Software Erase command, the module is no longer operating in a FIPS mode.

3.3 General User Guidance

Normal Users do not have the ability to perform approved security functions or configure sensitive information on the module. All users should be careful, however, not to provide sensitive device information to other parties.

The module operates within FIPS mode whenever it enters the main application firmware and the operator only uses FIPS approved algorithms, meaning the use of DES, 2-Key Triple-DES or Towitoko MAC is not allowed in the approved mode of operation. To clear the module into a non-FIPS device, the main application code must be erased using the appropriate API command. New application firmware can only be loaded to the module from a boot loader in this non-FIPS state.

4 Acronyms

Table 9 – Acronyms

Acronym	Definition
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
OS	Operating System
PCB	Printed Circuit Board
RF	Radio Frequency