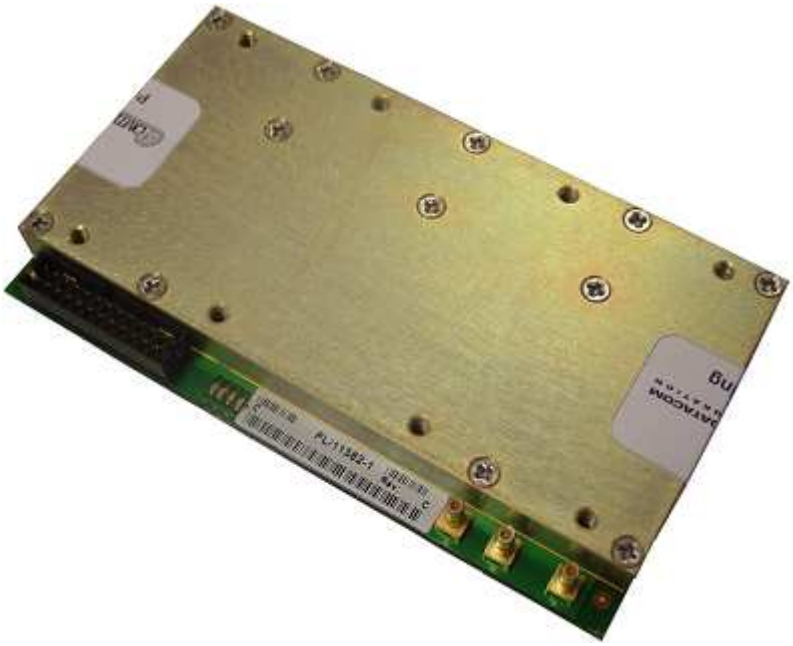
Comtech Mobile Datacom Corporation
MTM-203 Satellite Mobile Transceiver

(Commercial Firmware Version: C.3.7.Y, with Boot Code 2.3.E)



FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.7

Comtech Mobile Datacom Corporation
20430 Century Boulevard
Germantown, MD 20874
Phone: (240) 686-3300
Fax: (240) 686-3301

Revision History

Version	Modification Date	Description of Changes
0.1	2006-04-21	Initial draft.
0.2	2006-07-21	Updated section two and section three.
0.3	2006-07-26	Incorporated Quality Review feedback on document. Contents
0.4	2006-09-07	Minor updates.
0.5	2006-10-12	Updated the list of cryptographic keys, cryptographic key components, and Critical Security Parameters
0.6	2006-12-08	Added PRNG information
0.7	2006-12-20	Added role descriptions for Softload-user and Remote Administrator
0.8	2007-01-10	Added Softload Secret authentication information.
0.9	2007-01-12	Added algorithm certificate numbers.
1.0	2007-05-18	Added KEK functionality
1.1	2007-08-13	Added AES
1.2	2007-08-27	Clarified KEK operation and size of SK-2/SK-3.
1.3	2007_09_05	Clarification of clamshells. Specify which CSPs are exclusively Military and Commercial. Clarify that KEK is authentication,
1.4	2007-09-11	Removed Military references to return document to Commercial only.
1.5	2007-09-18	Clarified key entry formats, replaced ‘Ab Initialization’ with ‘Ab Initio’.
1.6	2007-11-05	Changed software version to 3.7.Y, added boot version and boot code functionality.
1.7	2008-02-05	Changed Table 11 from “124-bit” to “128-bit” AES keys, changed figure 2 to remove the word 'three' when describing LEDs and changed description of Pin 20 from “Internal LED” to “LED D”. Also updated CMVP website to new address and shrank size of photos to reduce document’s file size.

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 MTM-203 Satellite Mobile Transceiver from Comtech Mobile Datacom Corporation. This Security Policy describes how the MTM-203 Satellite Mobile Transceiver meets the security requirements of Federal Information Processing Standards (FIPS) 140-2 and describes 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/index.html

The MTM-203 Satellite Mobile Transceiver is referred to in this document as: the MTM-203 transceiver, the transceiver, 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/index.html) 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 the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine document
- 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 MTM-203 Satellite Mobile Transceiver

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.

Comtech Mobile Datacom has developed miniature L-band transceivers for streamlined messaging and real-time tracking systems. The miniature transceivers open doors to many new applications, such as covert devices and handheld units for the dismounted soldier - applications where weight and size limits are very important. The MTM-203 transceiver module represents a new generation in small-size, low power consumption transceivers for use in weight-restrictive environments.

The MTM-203 is designed for easy integration into systems that benefit from secure, near real-time, over-the-air communications. Low power consumption and efficient satellite communications technology make for a long-battery-life product under field conditions. This device allows dismounted users to maintain situational awareness and messaging connectivity worldwide with other mobile and terrestrial connected users. The miniature module operates over MSAT, INMARSAT, Thuraya, Artemis, ACeS, and OPTUS L-band satellite systems without reconfiguration.

2.2 Module Specification

The transceiver is a hardware module with hard metal covers, which compromise the cryptographic boundary. A block diagram of the internal components of the cryptographic module is given in Figure 1 below, and the cryptographic boundary is depicted in this diagram.

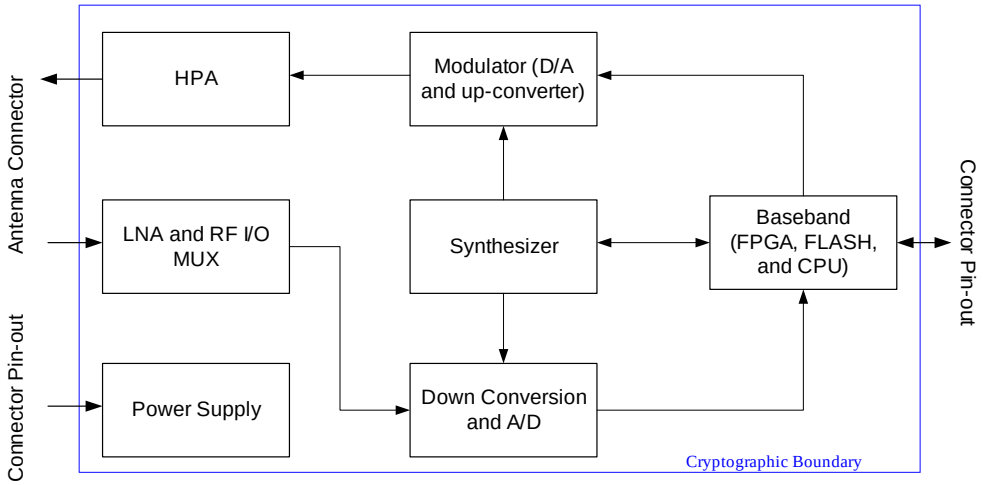


Figure 1 – MTM-203 Mobile Satellite Transceiver Block Diagram

The module contains a single Printed Circuit Board (PCB) with metal covers. The following is a list of the key circuit components for the PCB:

1. High Power Amplifier (HPA) – HPA amplifies Radio Frequency (RF) signals for output traffic. It is active only when the module is transmitting data.

2. Modulator: Modulator receives outgoing data from Baseband and converts it into a RF signal during data transmission.

3. Baseband: Baseband contains the FLASH memory and the Central Processing Unit (CPU) of the module. This component of the PCB controls the module and performs transceiver functionalities.

4. Synthesizer: Synthesizer controls signal frequency of Down Conversion or Modulator for incoming or outgoing RF signals, respectively. This component communicates with Baseband to decide on frequency.

5. Low Noise Amplifier (LNA) and RF I/O Multiplexer (MUX): Receives RF signal from the Antenna Connector.

6. Down Conversion and Analog-to-Digital (A/D) Converter: Down conversion and A/D converts RF signal to Baseband signal.

The MTM-203 Satellite Mobile Transceiver is a multi-chip standalone 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)	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.3 Module Interfaces

The MTM-203 Transceiver module provides a single serial interface at Transistor-Transistor Logic (TTL) levels. Application Programming Interface (API) commands can be provided to the module using the serial interface or the antenna interfaces. The antenna interface consists of three coaxial connectors,

- Left Hand circularly polarized (LHCP) antenna
- Right Hand circularly polarized (RHCP) antenna
- Global Positioning System (GPS) connection

Two of these connectors deliver the received signal from either a left hand (LH) or right hand (RH) circularly polarized antenna to the corresponding LNA circuitry. All three interfaces only operate in half duplex mode and use the High Power Amplifier (HPA) to send the signal to the antenna. Only the transmit or the receive signal is present on this interface at any given time. The third connector is used to connect to the on-board Global Positioning

System (GPS) device. The transceiver may be configured to automatically switch from LH to RH (or vice versa) by issuing the appropriate API command.

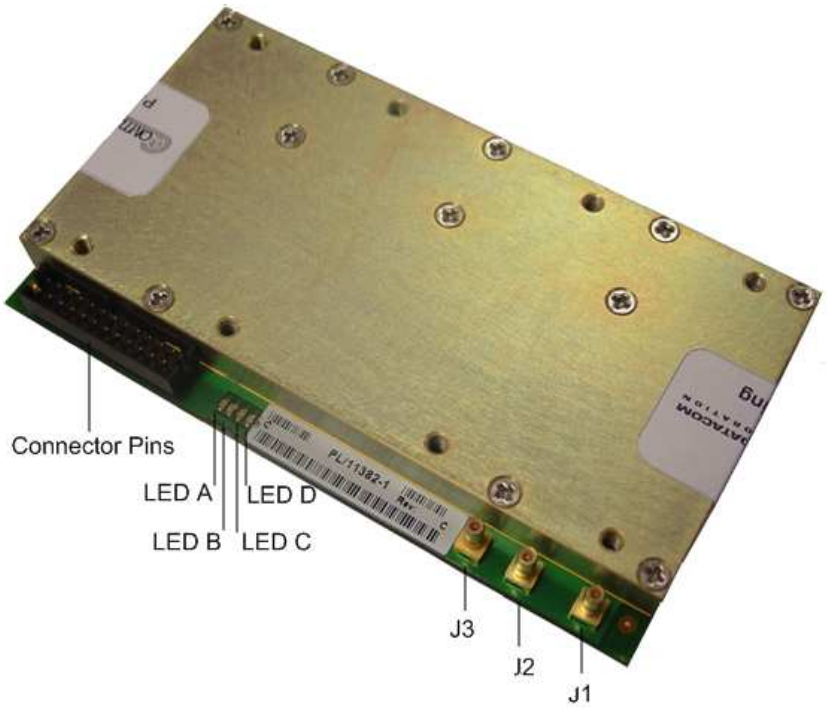


Figure 2 - MTM-203 Mobile Satellite Transceiver Interfaces

The module's physical interfaces are composed of Connector pins, Antenna Connectors, and Light Emitting Diodes (LEDs). Some of the Connector pins are used to provide serial data/control input and data/status output. The remaining active Connector pins are used to interface with an external power source. Functions of all active Connector pins are listed in Table 2. Antenna connectors are also used for data/control input or data/status output. The LEDs that are present on the module provide status concerning transmit or receive mode.

Table 2 – Connector Pin Functionality

Pin	Pin Description
1	GND
2	Voltage from Battery (VBATT) 6.5 – 15 V
3	Ground (GND)
4	VBATT (6.5 – 15 V)
5	LED C
6	LED A
7	LED B
8	AUX_PWR CNTL
9	IGN_SENSE
10	MAIN CNTL (ON/OFF) – Must be pulled high (3.3V) for the module to turn on.
11	User Defined: 0–3 V, 8 mA, max, 3 V logic,
12	User Defined: 0–3 V, 8 mA, max, 3 V logic,
13	User Defined: 0–3 V, 8 mA, max, 3 V logic,
14	User Defined: 0–3 V, 8 mA, max, 3 V logic,

Pin	Pin Description
17	SER DAT IN
18	SER DAT OUT
20	LED D
21	Power for GPS – 1.95-3.6V (40 μA max. at 3.3 V)

The Antenna interfaces on the MTM-203 Transceiver consists of three coaxial connectors: two connectors for external CP antennas (J2 and J3 in Figure 2), and a third connector (J1 in Figure 2) for an external GPS antenna.

- Antenna-LHCP (J3): Connector J3 feeds the LHCP LNA circuitry when in receive mode, and connects to the LHCP HPA circuitry when the unit is in transmit mode.
- Antenna-RHCP (J2): Connector J2 feeds the RHCP LNA circuitry in the receive mode, and connects to the RHCP HPA circuitry when the module is in transmit mode. The RHCP LNA also feeds the internal GPS module as well as the J1 connector.
- The third coaxial connector, J1, feeds the GPS signal to an external GPS module. The signal output from this connector is only available when the unit is in the receive mode.

All of these 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	MTM-203 Satellite Mobile Transceiver Port/Interface
Data Input	Pin 17, J2, J3
Data Output	Pin18, J1, J2, J3
Control Input	Pin 9, pin 10, pin11, pin 12, pin13, pin14, pin 17, J2, J3
Status Output	Pin 8, pin11, pin 12, pin13, pin14, pin 18, LEDs
Power	Pin 1, pin 2, pin 3, pin 4, pin 21

2.4 Roles and Services

The module supports role-based authentication. There are six roles in the module that operators may assume:

Table 4 - List of Roles

Role	Interface	Authentication
Normal Level User	Serial port	Not authenticated.
Super-User	Serial port	Super-User password.
Crypto-Officer	Serial port	Crypto-Officer password.
User	Satellite connection	Possession of correct identity and traffic TDES keys.
Remote Administrator	Satellite connection	Possession of identity and traffic keys.
Solftload User	Satellite connection	Possession of correct “softload secret” (9 bytes of random value used to derive a 192-bit TDES softload user key)

The User role is assumed by operators who utilize the module’s data transmitting functionalities. The Crypto-Officer, Super-user, Softload-user, and Remote Administrator roles are used to perform administrative services on the module, such as initialization, configuration, and monitoring of the module. The Normal level user is an unauthorized role who can perform only non-security relevant operation on the module. Normal level users cannot

modify or view any Critical Security Parameters (CSPs). Users and Remote Administrators only access the module via the Antenna interface, whereas other roles access the module locally via the serial port. To access the module as Crypto-Officer or a Super-user, the operator must first access the module locally as a Normal level user, and then enter a password to log in as a Crypto-Officer or a Super-user.

All roles except for the Softload User can 'Execute' the Traffic and Identity keys to encrypt and decrypt messages. The Softload User and Remote Administrator can 'Read' keys from and 'Write' keys to the transceiver. 'Execute' means that the role can use a key to encrypt or decrypt a message, but the ability to 'Execute' does not provide access to the raw key material. 'Read' means that the role can view the raw key material. 'Write' means that the role can add, or replace, the raw key material.

2.4.1 Normal Level User Role

The Normal level user is an unauthorized role which has access to the following non-security relevant services:

Table 5 – Mapping of Normal Level user Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSPs and Module's Access Level
API Modes	Controls display of command provided to the module over serial port	Command	Status output	--
General Information	Shows module status	Command	Status output	--
Identities and Nodes	Shows identity list and associated data	Command and identity name	Status output	--
Viewing Messages	Monitors message transaction	Command	Status output	--
Formatting a Message Payload	Formats payload data	Command	Status output	--
Message Formats	Formats incoming or outgoing messages	Command and data	Status output	--
Sending a Message	Transmits a message	Command and data	Status output	--
DSP	Configures and monitors DSP setting	Command	DSP configured and status output	--
Host Processor	Configures and monitors Host configuration to the EEPROM.	Command	Status output	--
GPS	Configures and monitors GPS setting	Command	DSP configured and status output	--
Digital I/O	Sets up antenna configuration	Command	Antenna configured and status output	--
Power	Sets up auxiliary power and 'powersave' mode	Command and power	Status output	--
Emergency Mode	Sets emergency mode	Command	Status output	--
LED	Tests LEDs	Command	Status output	--

Service	Description	Input	Output	CSPs and Module's Access Level
Provisioning	Provisions the module	Command	Module ready for service	--
Diagnostics	Diagnostic operations on the module	Command	Status output	--
Send message	Sends a message	Network packet with data	Data transmitted	Identity Key – Execute Traffic Key – Execute
Receive message	Receives a message	Network packet with data	Data received	Identity Key – Execute Traffic Key – Execute
Erase firmware holding area	Used by boot code protocols prior to upload of new firmware to holding areas in non-volatile memory	Commands	Status responses	--
Write firmware holding area	Used by boot code protocols to upload new firmware to holding areas in non-volatile memory	Commands and firmware image data	Status responses	--
Verify firmware holding area	Used by boot code protocols prior to request checksum test of holding areas in non-volatile memory	Commands and checksum data	Status responses	--

2.4.2 Super-user Role

The Super-user is an authorized role with following privileges:

Table 6 – Mapping of Super-user's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSPs and Module's Access Level
General Setup	Shows module status	Command	Status output	--
Access Levels	Changes access level to Crypto-Officer or Super user level	Command and password	Change in access level	Password – Read
Nodes and Identities	Monitors and sets identity list and associated data	Command and identity name	Status output	--
Sending a Message	Transmits a message	Command and data	Status output	--
DSP	Configures and monitors DSP setting	Command	DSP configured and status output	--
GPS	Configures and monitors GPS setting	Command	DSP configured and status output	--

Service	Description	Input	Output	CSPs and Module's Access Level
Power	Sets up auxiliary power and 'powersave' modes	Command and power	Status output	--
Send message	Sends a message	Network packet with data	Data transmitted	Identity Key – Execute Traffic Key – Execute
Receive message	Receives a message	Network packet with data	Data received	Identity Key – Execute Traffic Key – Execute

2.4.3 Crypto-Officer Role

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

Table 7 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSPs and Module's Access Level
Node and Identities	Monitors and sets identity list and associated data	Command and identity name	Status output	--
Access Levels	Changes access level to Crypto-Officer or Super user level	Command and password	Change in access level	Password – Read
Enable Internal GPS	Configures and monitors GPS setting	Command	DSP configured and status output	--
Monitor Maps	Manages and monitors inbound and outbound network maps.	Command	Status output	--
Process CMDC	Changes the transceiver packet display mode.	Command	Status output	--
Set Transmit	Adjusts the module's transmit power level and DSP setting.	Command	Status output	--
Test cryptographic algorithm	Tests TDES encryption/decryption algorithm	Command	Status output	--
Send message	Sends a message	Network packet with data	Data transmitted	Identity Key – Execute Traffic Key – Execute

Service	Description	Input	Output	CSPs and Module's Access Level
Receive message	Receives a message	Network packet with data	Data received	Identity Key – Execute Traffic Key – Execute

2.4.4 Softload-user and Remote Administrator Roles

Softload-user and Remote Administrator users are authorized roles whose privileges are listed in Table 8. These two roles can also access all module management related commands defined for Crypto-Officer and Super user roles.

Table 8 - Mapping of Softload-user and Remote Administrator's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSPs and Module's Access Level
NC_ESTABLISH_KEYSET	Adds keyset to the keyset tables	Command and key data	Keyset table changes	Traffic key – Read/Write AB Initialization Key – Read/Write
NC_ESTABLISH_ENCRYPTED_KEYSET	Adds the keyset to the keyset tables	Command and key data	Keyset table changes	Traffic key – Read/Write Ab Initio Key – Read/Write
NC_ESTABLISH_NODE	Builds incoming and outgoing maps in non-volatile memory.	Command and node name	Status output	--
NC_ADD_IDENTITY	Establishes the maps to add a node as a destination identity within the transceiver.	Command and data	Status output	--
NC_SET_DEFAULT_TO	Sets a node as the active default destination node.	Command	Status output	--
NC_SET_DEFAULT_FROM	Sets a node as the active default source node.	Command	Status output	--
NC_SET_DEFAULT_TO_AND_FROM	Sets the active source and destination nodes appropriately	Command	Status output	--
NC_REMOVE_KEYSET	Removes a keyset	Command	Status output	--
NC_REMOVE_NODE	Removes a node from the maps	Command	Status output	--
NC_REMOVE_IDENTITY	Removes a node from the identities within the transceiver.	Command	Status output	--
NC_SET_ALL_RADIO_PARAMETERS	Configures and monitors channel	Command	DSP configured and status output	--

Service	Description	Input	Output	CSPs and Module's Access Level
NC_SET_OUTPUT_GAIN_FACTOR	Sets the transmit gain value to the value of the included parameter	Command	Status output	--
NC_SET_TX_AUTHORIZATION_MASK	Sets the transceiver transmit authorization mask to the value of the included parameter	Command	Status output	--
NC_SET_CURRENT_AUTHORIZATION_MASK	Sets the current beam transmit authorization mask to the value of the included parameter	Command	Status output	--
NC_USE_CONFIGURATION	Configures and monitors DSP setting	Command	DSP configured and status output	--
NC_REMOVE_AB_INITIO	Removes Ab Initio keys, maps and identities from memory.	Command	Ab Initio Key removed	Ab Initio Key – Read/Write
NC_WRITE_DSP_FLASH	Writes the data to the appropriate location in Flash memory	Command and data	Status output	--
NC_MT2011_COMPATIBILITY	Sets the compatibility flags to the value	Command	Status output	--
Send message (Remote Administrator only)	Sends a message	Network packet with data	Data transmitted	Identity Key – Execute Traffic Key – Execute

2.4.5 User Role

The User role has the ability to utilize the module's data transmitting functionalities via Antenna interface only. Descriptions of the services available to the Users are provided in the table below.

Table 9 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSPs and Module's Access Level
Send message	Sends a message	Network packet with data	Data transmitted	Identity Key – Execute Traffic Key – Execute
Receive message	Receives a message	Network packet with data	Data received	Identity Key – Execute Traffic Key – Execute

2.4.6 Authentication Mechanism

The Crypto-Officers, Super-users, and Softload-users are able to access the module through directly connected console port. Users and Remote Administrators access the module only via the Antenna interface network and authenticate themselves with Traffic keys (AES or TDES keys). Crypto-Officer and Super-user authenticate themselves using passwords. Softload-users authenticate with a 192-bit TDES key derived from Softload Secret. Softload Secret is a 9 byte random value.

Table 10 – Authentication Mechanisms

Authentication Type	Strength	Strength Within One Minute
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.	Because of the serial interface speed, the module can accept only 69,120 password attempts in a minute. So the chance of random success is 1 in (94^6/69,120) or 1 in about 9,980,754.
TDES Keys	The Softload-user authentication keys are 192 bit TDES keys with 112 bits of security. Users and Remotes Administrators can also authenticate with 192 bit TDES keys. The chance of a random attempt falsely succeeding is 1 in (2^{112} =) 5.192296858 x10^{33}.	The processor speed means the module can go through $4.5*10^9$ cycles per minute. If each authentication attempt took only one minute, the chance of random success would be 1 in (2^{112}/$4.5*10^9$) or 1 in 1.15 * 10^24.
AES Keys	Users and Remote Administrators can authenticate with 128, 192 or 256 bit AES keys. The chance of a random attempt falsely succeeding is 1 in (2^{128} =) 3.402823669 x 10^{38}, 1 in (2^{192} =) 6.277101735 x 10^{57}, and 1 in (2^{256} =) 1.157920892 x 10^{77}, respectively.	Due to the processor speed cite above, the minimum chance of a random success in one minute would be 1 in (2^{128}/$4.5*10^9$) or about 1 in 7 * 10^{28}.
Softload Secret	Softload Secret is a 9 byte random value, the chance of a random attempt falsely succeeding is 1 in (2^{72} =) 4,722,366,482,869,645,213,696.	Again, due to processor speed, the chance of random success in a minute would be a most 1 in (2^{72}/$4.5*10^9$) or $1.04*10^{12}$.

2.5 Physical Security

The MTM-203 Satellite Mobile Transceiver is a multi-chip standalone cryptographic module. The module is contained within a hard metal clamshell. The module's cover is resistant to probing and is opaque within the visible spectrum. Tamper-evident seals are placed on the cryptographic module so that the seal must be broken to attain physical access

The cryptographic boundary is defined as encompassing the "top," "front," "left," "right," "rear," and "bottom" surfaces of two clamshell metal housing that are firmly held together with twelve screws. The metal housing exposes interfaces for the Control Connector, Antenna Connectors, and LEDs at front side.

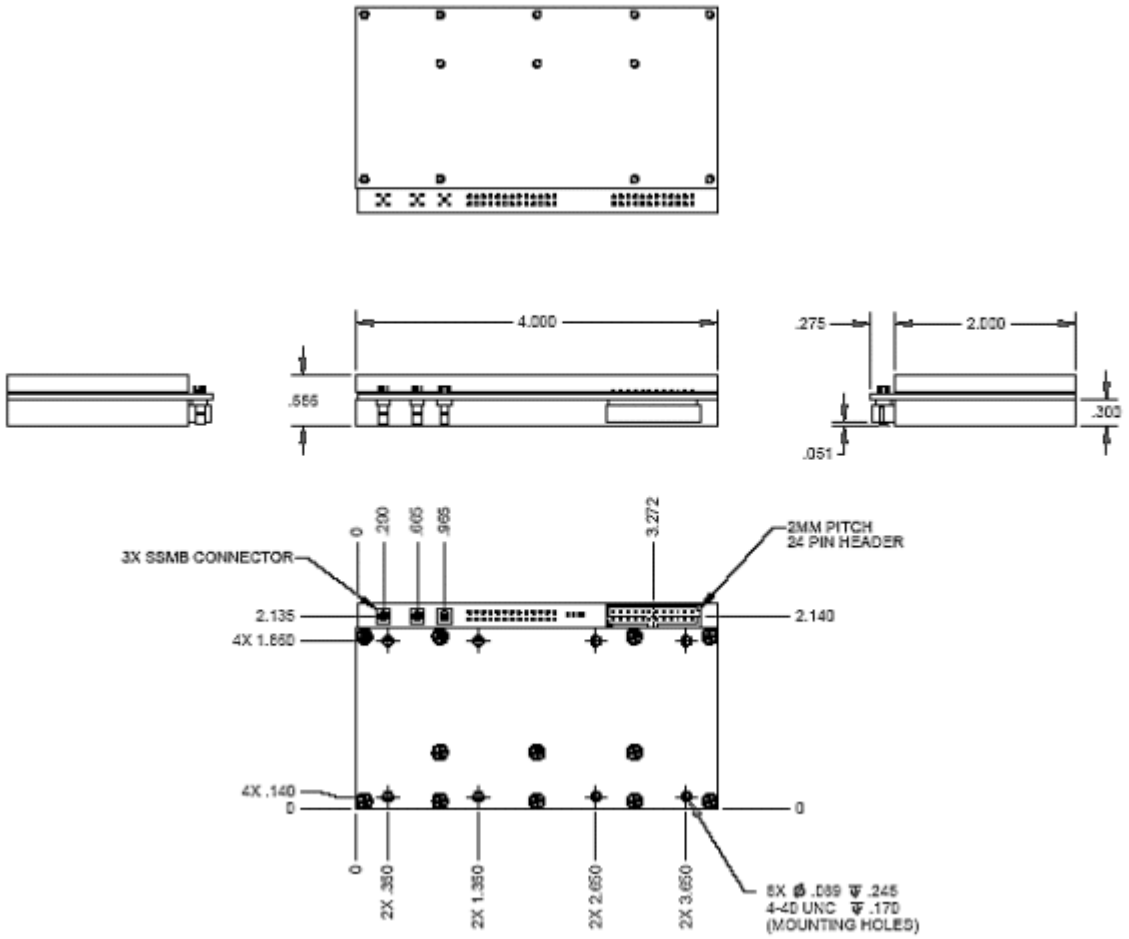


Figure 3 – MTM-203 Satellite Transceiver Mechanical View

The metal covers do not have any openings or ventilation holes. This module employs tamper-evident labels to detect the opening of the covers. The tamper-evident labels are applied by Comtech before providing the module to the Crypto-Officer, and the description of where these labels are located is described in the "Secure Operation" section of this document.

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 A (for business use).

2.6 Operational Environment

The operational environment requirements do not apply to the MTM-203 Satellite Mobile Transceiver, 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 with a new version. A HMAC-SHA-1 keyed hash is verified over the firmware update to ensure its integrity.

2.7 Cryptographic Key Management

The cryptographic module implements the following FIPS-approved algorithms:

- Triple DES – CBC; 1 and 2 keying option; encrypt/decrypt (certificate #502)
- SHA-1 Byte oriented (certificate #561)
- HMAC SHA-1 – (certificate #245)
- ANSI X9.31 Appendix A.2.4 PRNG – (certificate #271)
- AES – 128, 192 and 256 bit keying, CBC, encrypt/decrypt (certificate #626)

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

- Digital Encryption Standard (DES)
- Non-FIPS-approved RNG used to seed the FIPS approved PRNG

The module supports the following critical security parameters:

Table 11 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Identity Key	TDES 192-bit CBC key, or AES 128, 192 or 256 bit CDB key	Generated externally; input in plaintext or ciphertext, depending upon user role	Output in plaintext	Stored in Flash in plaintext	Erasing flash image	Encrypts and decrypts session data
Traffic Key	TDES 192-bit CBC key, or AES 128, 192 or 256 bit CDB key	Generated externally; input in plaintext or ciphertext, depending upon user role	Output in plaintext	Stored in Flash in plaintext	Erasing flash image	Encrypts and decrypts session data
Ab Initio Keys	TDES 192-bit CBC key	Generated externally; hardcoded in application	Output in plaintext	Stored in Flash in Plaintext or hardcoded in application	Erasing flash image	Encrypts and decrypts session data for unit recovery.
Softload Secret (Note: communication encrypted with the Softload Key is considered plaintext for FIPS purposes.)	9 bytes of random data	Generated externally; hardcoded in application	Never output from module	Hard coded in application firmware in plaintext	Erasing flash image	Derives key to encrypt and decrypt Softload session data. Derived keys are considered as authentication for softload user.
Password	Crypto-Officer or Super-user password	Generated externally	Never output from module	Stored in Flash in plaintext	Erasing flash image	Authenticates Crypto-Officer and Super-user
Firmware Upgrade key	20 bytes HMAC key	Generated externally; hardcoded in application	Never output from module	Hard coded in application firmware in plaintext	Erasing flash image	Perform Integrity check for firmware upgrade
PRNG seed	8 bytes of seed	Generated internally	Never output from module	Resides in volatile memory	Power cycle	Seeds the FIPS approved PRNG

2.7.1.1 Key Generation

The module has a nonapproved RNG to gather entropy and seed the FIPS approved PRNG. The module does not generate any cryptographic keys internally.

2.7.1.2 Key Storage

The Firmware Upgrade Key is held in volatile memory only in plaintext during firmware upgrade. The Softload Secret and passwords are stored in flash memory in plaintext. The Ab Initio key is stored in Flash memory in plaintext form. The Identity keys and Traffic keys are stored in flash memory, in plaintext form.

2.7.1.3 Key Entry and Output

All keys and CSPs that are entered into the module are electronically entered. Identity Keys, Traffic Keys, and Ab Initio Keys exit module in plaintext, no other keys or CSPs exit the module. Ab Initialization Keys are hardcoded in application. Identity Key and Traffic Keys can enter the module plaintext or in encrypted form.

2.7.1.4 Key Zeroization

All keys and CSPs can be zeroized by erasing the flash image. The user can erase the flash image by either engaging a zeroize mechanism via the serial user interface, or by commands sent to the unit over the satellite connection.

2.8 Self-Tests

The MTM-203 Satellite Mobile Transceiver performs the following self-tests at power-up:

- Software integrity check using Cyclic Redundancy Check (CRC)-32 checksum, on both Boot code and Host application code.
- Known Answer Tests (KATs)
    - Triple-DES KAT
    - HMAC-SHA-1 KAT
    - PRNG KAT
    - AES KAT

If any of the above self-tests fail, the module prints a failure indicator message on the serial port. Otherwise, a success indicator message is posted on the serial port. Failure of the Boot code software integrity check is indicated by a flashing pattern on the LEDs, as the serial interface has not been activated at that point.

The MTM-203 Satellite Mobile Transceiver performs the following conditional self-tests:

- Software update test using HMAC SHA-1
- Continuous RNG Test for FIPS approved PRNG and non-approved RNG

Upon failing conditional self-tests, the module posts a message on the serial port.

2.9 Design Assurance

The source code is primarily written in C. Some portions are written in assembler for performance reasons. Comtech uses Code Co-op version 4.6e to perform source code versioning and management and stores release notes within for versions of the firmware.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the MTM-203 Satellite Mobile Transceiver's FIPS documentation. This software provides access control, versioning, and logging.

2.10 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Secure Operation

The MTM-203 Satellite Mobile Transceiver 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.

The Crypto-Officer (CO) is responsible for initial setup and maintenance to the FIPS mode of operation of the module.

3.1.1 Initial Setup

The MTM-203 Satellite Mobile Transceiver comes to the CO in a compact, rugged, solid-state device with no moving parts. The following materials are needed to run the MTM-203 Satellite Mobile Transceiver:

1. Antenna
2. RS-422 serial cable
3. Interface from the Connector pin-outs to serial port
4. External Power Supply (40 uA max, 3.3V)
5. 20AWG wiring gauge

Crypto-Officer receives the module with tamper evident labels on. The module requires two (2) a labels to detect any tampering.

1. One label is at the seam covering top and bottom surface of the clamshells at left side.

Figure 4 - Left Label Top View

Figure 5 - Left Label Bottom View

2. Another label is applied at the seam covering top and bottom surface of the clamshells at right side.

Figure 6 - Right Label Top View

Figure 7 - Right Label Bottom View

Tamper evident labels usually become torn upon an attempt to remove them, and always either break into small pieces or become noticeably warped whenever a successful removal attempt is made. Thus, attempts at removal always show evidence of tampering. After confirming that there is no evidence of label damage that would indicate tampering with the module, the Crypto-Officer should run the power-on test. This procedure requires a terminal or computer running terminal emulation software set for 9600 baud with 8 bits, no parity, 1 stop bit, and no flow

control. Initialization messages should appear on console port when an RS-422 serial cable with an RJ-45 male connector is connected to the terminal and with power turned on.

Comtech ships the module fully provisioned. Provisioning establishes the profile of configuration commands inherent to the module.

3.1.2 Management

The Crypto-Officer must ensure that the module is always operating in a FIPS-approved mode of operation. This can be achieved by ensuring the following:

- Ensure via the "show version" command that the FIPS-Approved versions of the Boot Code and Commercial Firmware are loaded on the transceiver (see pg.1 of this document for the applicable version numbers).
- Passwords must be at least six characters long.
- To login over serial port as a Crypto-Officer or Superuser role, 'superuser' command needs to be issued followed by a 'enter' key, then password needs to be entered.
- The module logs must be monitored. If suspicious log entries are noted, the Crypto-Officer should take the module off-line and investigate.
- The tamper-evident labels must be regularly examined for signs of tampering (Figure 4, Figure 5, Figure 6, and Figure 7) to detect any opening of the covers.
- 'softload' should be used only via serial port.
- The Crypto-Officer must ensure that only AES or Triple-DES keys are loaded into the module and used for encryption/decryption. DES keys must be explicitly disallowed.

3.2 User Guidance

The end Users do not have the ability to configure sensitive information on the module. The User should be careful not to provide Traffic key information to other parties.

4 Acronyms

Table 12 – Acronyms

Acronym	Definition
A/D	Analog to Digital Converter
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
GPS	Global Positioning System
HMAC	(Keyed-) Hash Message Authentication Code
HPA	High Power Amplifier
KAT	Known Answer Test
LED	Light Emitting Diode
LH	Left Hand
LHCP	Left-Hand Circularly Polarized
LNA	Low Noise Amplifier
MUX	Multiplexer
NIST	National Institute of Standards and Technology
OS	Operating System
PCB	Printed Circuit Board
RF	Radio Frequency
RH	Right Hand
RHCP	Right-Hand Circularly Polarized
TTL	Transistor-Transistor Logic
VBATT	Voltage from Battery
VSS	Visual Source Safe