Comtech EF Data Corporation

DMD2050E TRANSEC Module

Hardware Version: PL-0000192-1, Revision A; Firmware Version: 1.2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.6

Prepared for:

Comtech EF Data Corporation
2114 West 7th Street
Tempe, Arizona 85281
United States of America

Phone: +1 (480) 333-2200
http://www.comtechefdata.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, Virginia 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Comtech EF Data Corporation's DMD2050E TRANSEC Module (Hardware Version: PL-0000192-1, Revision A; Firmware Version: 1.2.1). This Security Policy describes how the DMD2050E TRANSEC Module meets the security requirements of 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. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/index.html.

The DMD2050E TRANSEC Module is referred to in this document as 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 EF Data website (http://www.comtechefdata.com/) contains information on the full line of products from Comtech EF Data.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) 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
- Submission Summary
- Finite State Model
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Comtech EF Data. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Comtech EF Data and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Comtech EF Data.

2 DMD2050E TRANSEC Module

2.1 Overview

Comtech EF Data Corporation designs, develops, and markets satellite communication products for commercial and government customers internationally. The company's product lines include satellite modems, modem accessories, performance enhancement proxies, satellite network gateways, bandwidth and capacity management products, encapsulators and receivers, converters, transceivers, amplifiers, terminals, block up converters, high-speed trunking modems, and legacy products. Its products are deployed in various applications by satellite operators, cellular service providers, broadcast and satellite news gathering organizations, government agencies, educational institutions, offshore oil and gas companies, and maritime enterprises. Comtech EF Data Corporation is based in Tempe, Arizona and operates as a subsidiary of Comtech Telecommunications Corp. Comtech's satellite modem solution, called the DMD2050E, is an IP[1] satellite modem designed to provide efficient and reliable data transmission over complex satellite connections. Figure 1 below shows a satellite modem sending and receiving traffic in a typical deployment. A typical deployment requires a satellite modem to be at both the transmitting and receiving ends of the communication to perform the encryption and decryption, respectively.

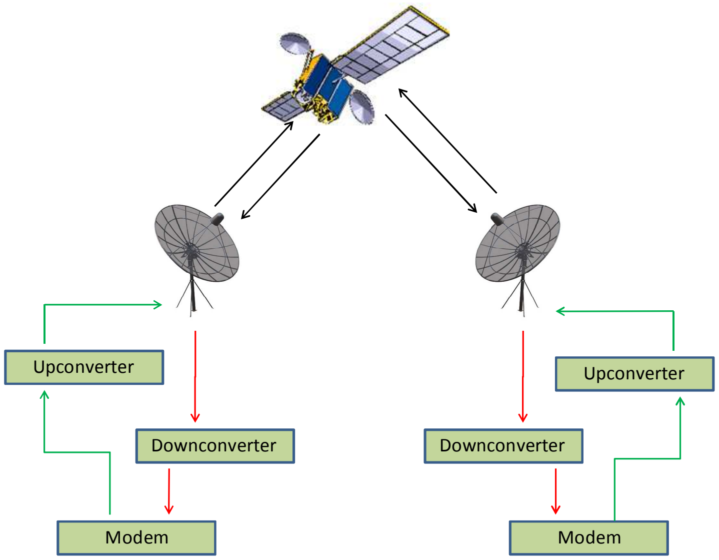

Figure 1 – Typical Deployment of Satellite Modems

The DMD2050E satellite modem includes a single FIPS card called the DMD2050E TRANSEC Module that will perform bulk encryption of all packets for transmission over the satellite regardless of the protocol, the format of data, or existing encryption on the incoming data. The DMD2050E TRANSEC Module uses 256-bit AES[2] in CTR[3] mode for bulk encryption of all data requiring encryption. The module is managed using an HTTPS[4] over TLS[5] interface to provide a graphical user interface (GUI) for management (referred as Management & Control Console), a command line management interface over SSH[6], as well as

[1] Internet Protocol
[2] AES – Advanced Encryption Standard
[3] CTR – Counter
[4] HTTPS – Secure Hypertext Transfer Protocol
[5] TLS – Transport Layer Security
[6] SSH – Secure Shell

supporting key imports through a handheld key loader. The DMD2050E TRANSEC Module only supports the N37B Modular Rugged Handheld Computer (key loader) by Newport Digital Technologies running Comtech's key loader software.

The DMD2050E TRANSEC 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	EMI/EMC[7]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The DMD2050E TRANSEC Module is a hardware module with a multi-chip embedded embodiment that meets overall level 2 FIPS 140-2 requirements. Figure 2 and Figure 3 below show the top and bottom side of the multi-chip embedded cryptographic module respectively. Figure 4 below shows the block diagram of the hardware module; the blue dotted line surrounding the module components represents the cryptographic boundary.

[7] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

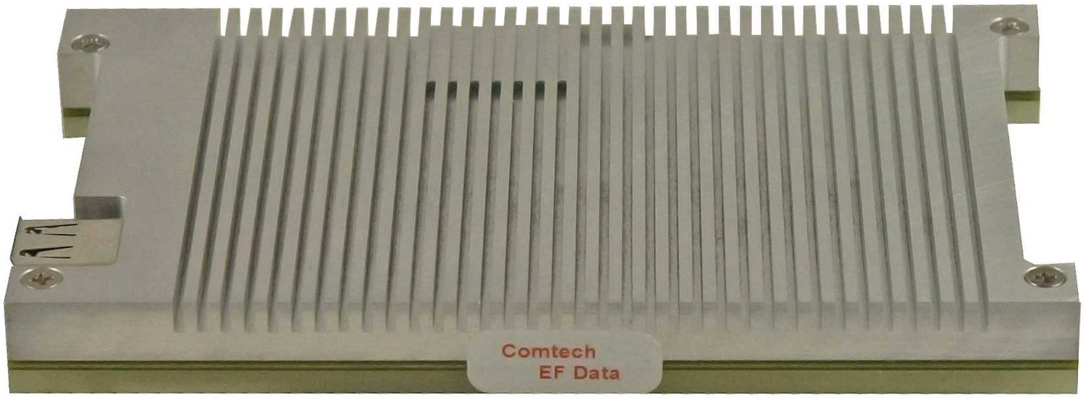

Figure 2 – DMD2050E TRANSEC Module (Top)

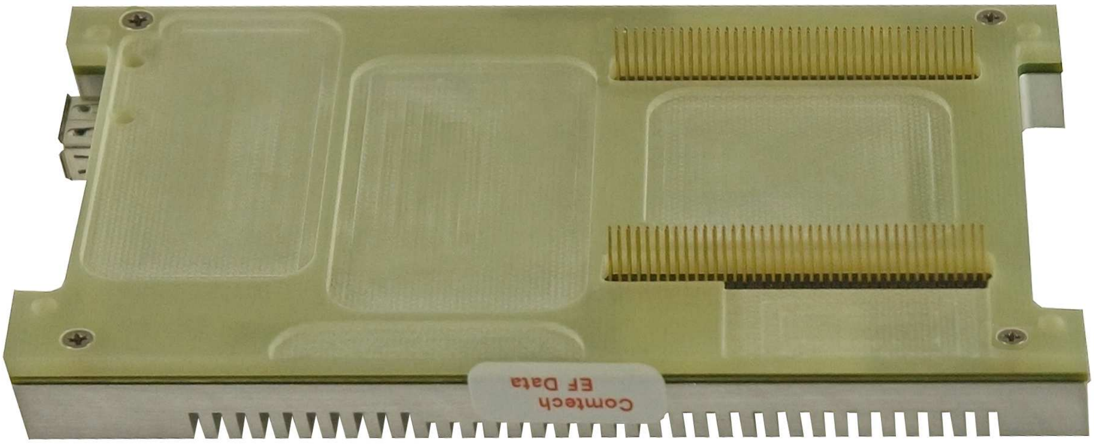

Figure 3 – DMD2050E TRANSEC Module (Bottom)

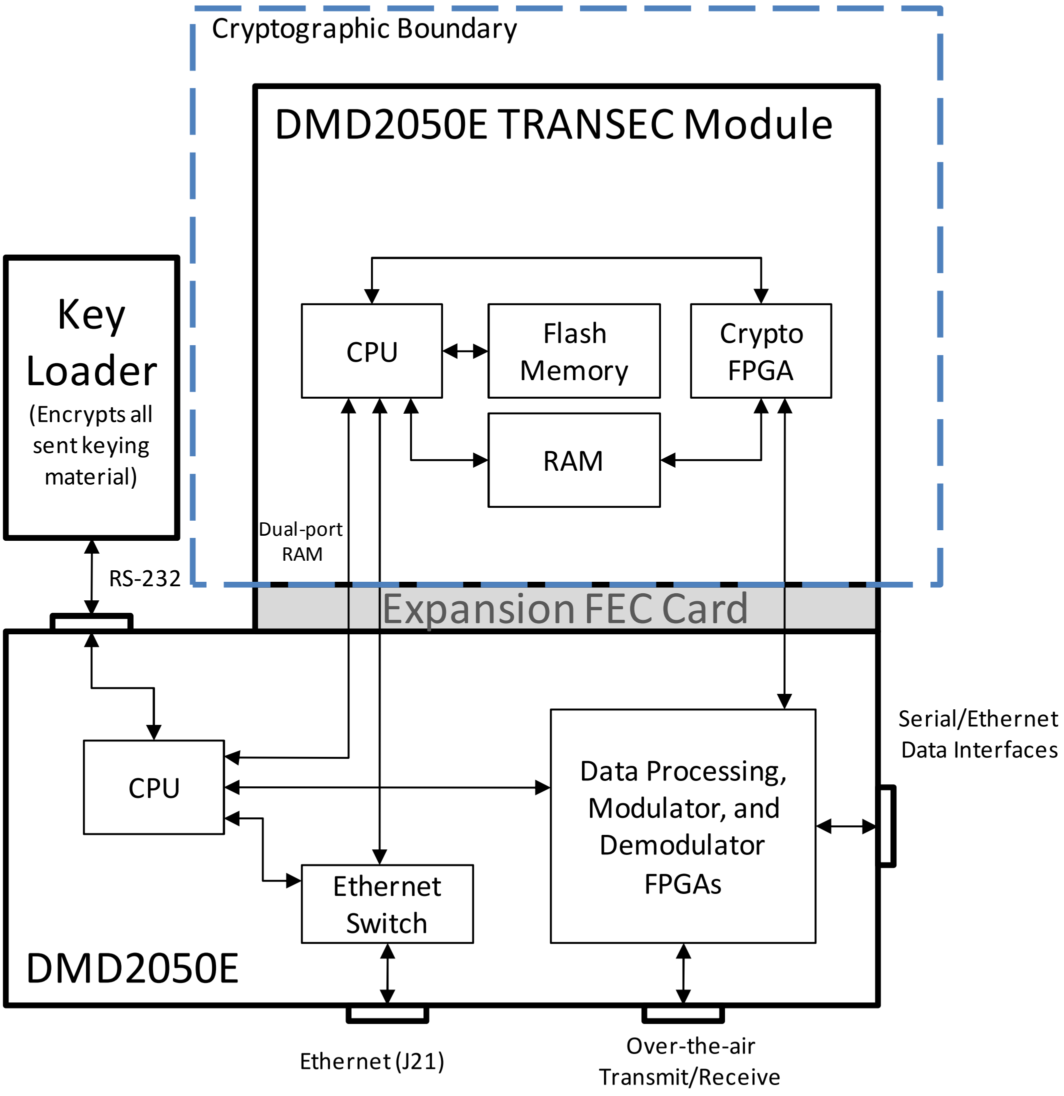

Figure 4 – DMD2050E TRANSEC Module Block Diagram

2.3 Module Interfaces

The DMD2050E TRANSEC Module is a multi-chip embedded cryptographic module that meets overall level 2 FIPS 140-2 requirements. Interfaces on the module can be categorized into the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

The module features the physical interfaces of the system depicted in Figure 4. The following is a list of the physical interfaces available for the module in the FIPS mode of operation:

- System Clock Interface
- Receiver (Rx) FPGA Interface
- Transmitter (Tx) FPGA Interface
- Encoder/Modulator Interface
- Decoder/Demodulator Interface
- Ethernet Interface
- Mailbox Interface
- Power Interface
- USB[8] Interface (Disabled)

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

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	DMD2050E TRANSEC Module Interface
Data Input	Transmitter (Tx) FPGA Interface, Decoder/Demodulator Interface, Ethernet Interface, Mailbox Interface
Data Output	Receiver (Rx) FPGA Interface, Encoder/Modulator Interface, Ethernet Interface, Mailbox Interface
Control Input	System Clock Interface, Ethernet Interface, Mailbox Interface
Status Output	Mailbox Interface, Ethernet Interface
Power Input	Power Interface

2.4 Roles and Services

The module supports the following authorized roles: the Crypto Officer (CO) role and the User role. The CO role is responsible for the management of the module. The User role performs the actual data protection services of encryption and decryption.

In addition to the authenticated roles, the module also supports an unauthenticated operator role called Unauthenticated User.

Please note that the keys and CSPs[9] listed in the table use the following notation to indicate the type of access required:

- Read: The CSP is read
- Write: The CSP is established, generated, modified, or zeroized
- Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism

2.4.1 Crypto Officer Role

The CO role performs services such as initialization and installation, configuration, management, monitoring, zeroization and upgrading the cryptographic module. Descriptions of the services available to the Crypto Officer role are provided in the Table 3 below.

[8] USB – Universal Serial Bus

[9] CSP – Critical Security Parameter

Table 3 – Mapping of Crypto Officer Role's Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Initialize and install	Initialize and install the FIPS DMD2050E TRANSEC Module	None
Configure the FIPS DMD2050E TRANSEC Module	Allows the operator to configure security-sensitive parameters	X9.31 PRNG Seed, Shared Modem Access Token (SMAT), Password - Read, Write, Execute
Configure Network Parameters	Allows the operator to configure network parameters of the module	None
Configure Operator Credential Parameters	Allows the operator to configure operator credential parameters of the module	Password - Read, Write, Execute
Access the Module via GUI	Access the module using TLS protocol	TLS Public/Private Keys, SMAT, TLS Session authentication key, TLS Session key, X9.31 PRNG Seed Key, X9.31 PRNG Seed, Password - Read, Write, Execute
Access the Module via CLI	Access the module using SSH protocol	SSH Public/Private Keys, SMAT, SSH Session authentication key, SSH Session key, Diffie-Hellman Parameters, X9.31 PRNG Seed Key, X9.31 PRNG Seed, Password - Read, Write, Execute
Access the module via Key Loader	Access the module using the handheld key loader	SMAT, X9.31 PRNG Seed, Key Encryption Key (KEK), Password, Key Loader HMAC Key – Read, Write, Execute
Upgrade Parameters	Configure upgrade parameters of the module	ECDSA Public Key - Execute
Cryptographic Module Status	Check the current status of the FIPS module	None
Perform Self-Tests	Performs the required self-test on the module	None
Zeroization	Zeroize all the cryptographic keys and key components	All keys and CSPs -Read, Write

2.4.2 User Role

The User role has access to encryption/decryption service in the cryptographic module over the Encoder/Modulator and Decoder/Demodulator Interface. Descriptions of the service(s) available to the User role are provided in Table 4 below.

Table 4 – Mapping of User Role's Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Encryption/decryption	Perform encryption and/or decryption of data	TEKs[10], TDKs[11], SMAT, Elliptic Curve Diffie-Hellman (ECDH) Parameters - Read, Write, Execute

2.4.3 Unauthenticated Operator Role

Unauthenticated User Role services are accessible through the Mailbox interface. The Unauthenticated Operator role has access to the services listed in Table 5 below for which the operator is not required to assume an authorized role. None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module. See Table 5 below for a list and description of the associated services.

Table 5 – Mapping of Unauthenticated Operator Role Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Change IP address and Subnet	Change the module's IP address and subnet	None
Change network default gateway	Change the module's IP network default gateway	None
Zeroization	Zeroize all the cryptographic keys and key components	All keys and CSPs -Read, Write

2.4.4 Authentication Mechanism

Table 6 below describes the authentication method employed by the module to authenticate the Crypto Officer and User.

[10] TEK – Transmission Encryption Key

[11] TDK – Transmission Decryption Key

Table 6 – Authentication Mechanism Employed by the Module

Role	Authentication Type	Authentication Strength
Crypto Officer	Password	The Crypto Officer authenticates with a username and password over a TLS, SSH, or Key Loader connection. Passwords are required to be at least 7 characters long. All printable ASCII characters can be used for the password, which gives a total of 95 characters to choose from. With the possibility of repeating characters, the probability of a random attempt falsely succeeding is 1:95^7, or 1:69,833,729,600,000. This would require 698,337,296 attempts in one minute to lower the random attempt success rate to less than 1:100,000. The fastest connection supported by the module is 155 Mbps. Hence, at most 9,300,000,000 bits of data (155 × 10^6 × 60 seconds, or 9.3 x 10^9) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 166,071,428 attempts can be transmitted over the connection in one minute.
User or Crypto Officer	Shared Secret (HMAC SHA-1)	The User authenticates by proving knowledge of a shared secret, the SMAT HMAC key. The SMAT is a 40-character secret specified by the User. All printable ASCII except for <, >, ", and ~ can be used, which gives a total of 90 characters to choose from. With the possibility of repeating characters, the probability of a random attempt falsely succeeding is 1:90^{40}, which is less than the required 1:1,000,000. The Crypto Officer also authenticates by proving knowledge of a shared secret, the Key Loader HMAC key, which is 160-bits in length. The probability of a random attempt falsely succeeding is 1:2^{160}, which is less than the required 1:1,000,000. The fastest connection supported by the module is 155 Mbps. Hence, at most 9,300,000,000 bits of data (155 × 10^6 × 60 seconds, or 9.3 x 10^9) can be transmitted in one minute. At that rate and assuming no overhead, a maximum of 166,071,428 attempts can be transmitted over the connection in one minute, which results in a probability of less than 1:100,000 that a brute force attack will be successful within a given minute for this authentication method.

2.5 Physical Security

The DMD2050E TRANSEC Module is a multi-chip embedded cryptographic module. The entire contents of each module, including all hardware, firmware, and data, are protected by a metal cover on the top and all sides and a hard plastic material on the bottom of the module. The metal cover and hard plastic material are opaque and sealed using preinstalled tamper-evident labels, which prevent the cover or plastic material from being removed without signs of tampering. All components are made of production-grade materials, and all ICs[12] in the module are coated with commercial standard passivation.

It is the Crypto Officer's responsibility to ensure that the physical security posture of the module is maintained. The proper maintenance of physical security of the module is detailed in the "Secure Operation" section of this document.

2.6 Operational Environment

The operational environment requirements do not apply to the DMD2050E TRANSEC Module, as the module employs a limited operating environment that requires a digital signature to be verified over any firmware updates.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 7 below.

Table 7 – FIPS-Approved Algorithm Implementations

Approved or Allowed Security Function	Certificate Number
Symmetric Key Algorithm	
AES – 128, 192 and 256-bit in ECB[13] and CBC[14] mode	2025
AES – 256-bit in ECB and CTR[15] mode (Helion FPGA)	2026
Triple-DES[16] – 112-bit in CBC mode (Encryption: Acceptable through 2010. Restricted use from 2011 through 2015. Disallowed after 2015 Decryption: Acceptable through 2010. Legacy-use after 2010.)	1309
Secure Hashing Algorithm (SHA)	
SHA-1, SHA-512	1775
Message Authentication Code (MAC) Function	
HMAC using SHA-1, SHA-512	1228
Random Number Generator (RNG)	
ANSI X9.31 Appendix A.2.4 (Acceptable through 2010. Deprecated from 2011 through 2015. Disallowed after 2015.)	1061
Asymmetric Key Algorithm	
RSA PKCS#1v1.5 sign/verify – 2048 bit	1053
ECDSA verify – P-521 curve	296

[12] ICs – Integrated Circuits
[13] ECB – Electronic Codebook
[14] CBC – Cipher-Block Chaining
[15] CTR – Counter
[16] DES – Data Encryption Standard

The module implements the following non-Approved algorithms, which are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology provides 80 to 112 bits of encryption strength)
- Non-Compliant EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256-bits of encryption strength)
- 2048-bit RSA[17] (key transport; key establishment methodology provides 112 bits of encryption strength)
- Message Digest 5 (MD5)

[17] RSA – Rivest Shamir Adleman

The module supports the keys and critical security parameters listed in Table 8 below.

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

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
TRANSEC Encryption keys	AES-CTR – 256-bit key	256-bit	Established during the ECDH handshake	ECDH	Never exits the module	Stored in volatile memory	By Zeroize command or power cycling the module	Encrypt the data
TRANSEC Decryption keys	AES-CTR – 256-bit key	256-bit	Established during the ECDH handshake	ECDH	Never exits the module	Stored in volatile memory	By Zeroize command or power cycling the module	Decrypt the data
SSH private key	RSA 2048-bit key	112-bit	Internally generated using the ANSI X9.31 PRNG	Electronic Distribution/Electronic Entry (ED/EE)	Never exits the module	Stored in non-volatile memory	By Zeroize command	Facilitates SSH sessions
TLS private Key	RSA 2048-bit key	112-bit	Factory default until externally generated and imported in encrypted form by TLS Session Key	ED/EE	Never exits the module	Stored in non-volatile memory	By Zeroize command	Facilitates TLS sessions
SSH public key	RSA 2048-bit key	112-bit	Internally generated using the ANSI X9.31 PRNG	ED/EE	Public key exported electronically in plaintext ; private component not output	Stored in non-volatile memory	By Zeroize command	Facilitates SSH sessions

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
TLS public key	RSA 2048-bit key	112-bit	Factory default until externally generated and imported in encrypted form by TLS Session Key	Electronic Distribution/Electronic Entry (ED/EE)	Public key exported electronically in plaintext ; private component not output	Stored in non-volatile memory	By Zeroize command	Facilitates TLS sessions
Peer public key	RSA 2048-bit key	112-bit	Imported electronically during handshake protocol	ED/EE	Never exits the module	Stored in volatile memory	None	Facilitates SSH/TLS sessions
TLS Session Authentication key	HMAC SHA-1	80-bit	Established during the TLS handshake	TLS	Never exits the module	Stored in volatile memory	Power cycle or session termination	Data authentication for TLS sessions
TLS Session key	• TDES-CBC key • AES-CBC 128-, 256-bit key	• 80-bit • 128, 256-bit	Established during the TLS handshake	TLS	Never exits the module	Stored in volatile memory	Power cycle or session termination	Data encryption/decryption for TLS sessions
SSH Session Authentication key	HMAC SHA-1	80-bit	Established during the SSH handshake	SSH	Never exists the module	Stored in volatile memory	Power cycle or session termination	Data authentication for SSH sessions
SSH Session key	• TDES-CBC key • AES-CBC 128-, 192-, 256-bit key	• 80-bit • 128, 192, 256-bit	Established during the SSH handshake	SSH	Never exists the module	Stored in volatile memory	Power cycle or session termination	Data encryption/decryption for SSH sessions

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
Diffie-Hellman Parameters	Diffie-Hellman 1024 or 2048-bit key	80 or 112-bit	Internally generated using the ANSI X9.31 PRNG	Not applicable	Public exponent electronically in plaintext, private component not output	Stored in volatile memory	Power cycle or session termination	Key exchange/agreement for SSH sessions
ECDH Parameters	ECDH 521-bit key	256-bit	Internally generated using the ANSI X9.31 PRNG	Not applicable	Public exponent electronically in plaintext, private component not output	Stored in volatile memory	Power cycle or session termination	Key exchange/agreement for over-the-air data encrypted sessions with peer devices
Operator password	Password	See Section 2.4.4	Input internally by the CO during initialization	Not applicable	Never exits the module	Stored in non-volatile memory	By Zeroize command	Operator authentication
Firmware update ECDSA public key	ECDSA 521-bit	256-bit	Externally generated	Not applicable	Never exits the module	Stored in non-volatile memory	N/A	To Verify firmware update
X9.31 RNG Seed Key	AES 256-bit key	256-bit	Internally generated	Not applicable	Never exits the module	Stored in volatile memory	Power cycle	Generates FIPS-Approved random number

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
X9.31 RNG Seed	128 or 256-bits of Seed value	128 or 256-bit	Internally generated. Additional entropy material may be input through TLS, SSH, or the Key Loader	Not applicable	Never exits the module	Stored in volatile memory	Power cycle	Generates FIPS-Approved random number
Key Encryption Key	AES-256 CBC	256-bit	Established using Password-Based Key Derivation Function 2 (PBKDF2)	PBKDF2	Never exits the module	Stored in volatile memory	Power cycle	Encrypts the SMAT and X9.31 PRNG Seed during entry
Key Loader HMAC Key	HMAC-SHA1	160-bit	Internally derived using a proprietary scheme	ED/EE	Never exits the module	Stored in volatile memory	Power cycle	Authenticates the Crypto Officer
SMAT	HMAC-SHA512	320-bit	Generated externally and entered into the module electronically over TLS, SSH, or through the Key Loader	ED/EE	Never exits the module	Stored in non-volatile memory	By Zeroize command	Authenticate the User and over-the-air data transmitted and received packets

2.7.1 Key Generation

The module uses a FIPS-Approved ANSI X9.31 Appendix A.2.4 algorithm to generate keys.

2.7.2 Key Entry and Output

The cryptographic module implements key entry with keys electronically imported into the module. The module does not provide a means to output private keys or CSPs from its physical boundary.

2.7.3 CSP Storage and Zeroization

All the keys and CSPs are stored in either the non-volatile or volatile memory in plaintext and can be zeroized by using the Zeroization command and then power cycling the cryptographic module.

2.8 EMI/EMC

The DMD2050E TRANSEC Module was tested and found to be conformant to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by Federal Communications Commission 47 Code of Federal Regulations (CFR), Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self -Tests

The DMD2050E TRANSEC Module performs the following self-tests at power-up:

- Firmware integrity test using CRC-32
- Cryptographic algorithm tests
  - Firmware AES Known Answer Test (KAT)
  - Helion AES KAT
  - Triple-DES KAT
  - SHA-1 KAT
  - SHA-512 KAT, tested as a part of the HMAC SHA-512 KAT
  - HMAC SHA-1, SHA-512 KAT
  - RSA Encrypt/Decrypt KAT
  - RSA Sign/Verify KAT
  - ECDSA Verify KAT
  - ECDH KAT
  - ANSI X9.31 Appendix A.2.4 RNG KAT

The DMD2050E TRANSEC Module also performs the following conditional self-tests:

- Continuous RNG Test for the ANSI X9.31 RNG
- Continuous RNG Test for NDRNG[18] used for seed generation
- Pairwise Consistency Test for RSA and ECDH
- Firmware load test (ECDSA digital signature verification)

If the firmware integrity test fails, the system will not boot up. Upon firmware integrity test failure, the module reinitializes itself by loading a redundant, standby firmware image (this is initially a factory-installed copy of the primary firmware image, which is stored in a second firmware slot). The newly-loaded image then undergoes the firmware integrity test. If there is no standby firmware or it is corrupt, the module must be serviced by Comtech EF Data Corporation.

If any of the power-up self-tests or conditional self-tests fail, the module disables data transmission, shows a fault indication on the modem's front panel, and writes the fault information to the modem event log. No

[18] NDRNG – Non-deterministic Random Number Generator

data output or cryptographic operations are possible when the module enters the critical error state. The CO can clear this error by power-cycling the module.

2.10 Design Assurance

Comtech EF Data uses Concurrent Versions System (CVS) and Polytron Version Control System (PVCS) Professional as the configuration management system.

Concurrent Versions System (CVS) records the history of the source files. It stores all the versions of a file in a single file in a clever way that only stores the differences between versions. It also helps individuals on a team to make changes without interrupting other team members. Every person works in his own directory, and CVS merges the work when each person is done.

PVCS follows the "locking" approach to concurrency control; it has no built-in merge operation. PVCS can be configured to allow several users to simultaneously edit files. With this configuration, subsequent editors create their own branches, ensuring that modifications create parallel histories for the same file.

Additionally, Microsoft Visual SourceSafe (VSS) version 6.0 is used to provide configuration management for the DMD2050E TRANSEC Module's FIPS documentation. This software provides access control, versioning, and logging.

2.11 Mitigation of Other Attacks

The module does not claim to mitigate any additional attacks in an approved FIPS mode of operation.

3 Secure Operation

The DMD2050E TRANSEC 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 Crypto Officer role is responsible for initializing and managing the module.

3.1.1 Installation and Configuration

The cryptographic module is designed to be embedded in a DMD2050 satellite modem as a single FIPS card called the DMD2050E TRANSEC Module. The cryptographic module will perform bulk encryption of all packets for transmission over the satellite regardless of the protocol, format of data, or existing encryption on the incoming data. The following steps provide rules for secure installation and configuration of the cryptographic module.

Installation:

- Turn off modem power
- Put on Electrostatic Discharge (ESD) protection
- Remove top cover of DMD2050E
- Install DMD2050E TRANSEC Module card onto Forward Error Correction (FEC) board
- Install FEC board into modem
- Close DMD2050E
- Turn on modem power

Configuration:

- Configure IP Address
- Log into the web as Crypto Officer for first time access
- Change SMAT from the factory-default value
- Change default Crypto Officer Password

3.1.2 Management

The module can run only in the FIPS-Approved mode of operation. The Crypto Officer is able to monitor and configure the module via the web GUI (HTTPS over TLS) and SSH.

3.1.3 Delivery

The Crypto Officer can receive the module from the vendor via trusted delivery couriers including UPS, FedEx, and DHL. Upon receipt of the module, the Crypto Officer should check the package for any irregular tears or openings. If the Crypto Officer suspects any tampering, he/she should immediately contact Comtech EF Data Corporation.

3.1.4 Maintenance of the Physical Security

The module employs tamper-evident labels to ensure that no one can tamper with the components of the module without leaving some form of evidence. These labels are installed by Comtech EF Data prior to delivery; however, it is the Crypto Officer’s responsibility to ensure that the physical security posture of the module is maintained. To accomplish this, the CO has the following responsibilities:

- The CO must visually inspect the module for the secure placement of tamper-evident labels. The tamper-evident labels ensure that no one can tamper with the components of the module without leaving some form of evidence. The module requires two labels to be placed on it to meet FIPS requirements. Figure 5 and Figure 6 show the required label placement.

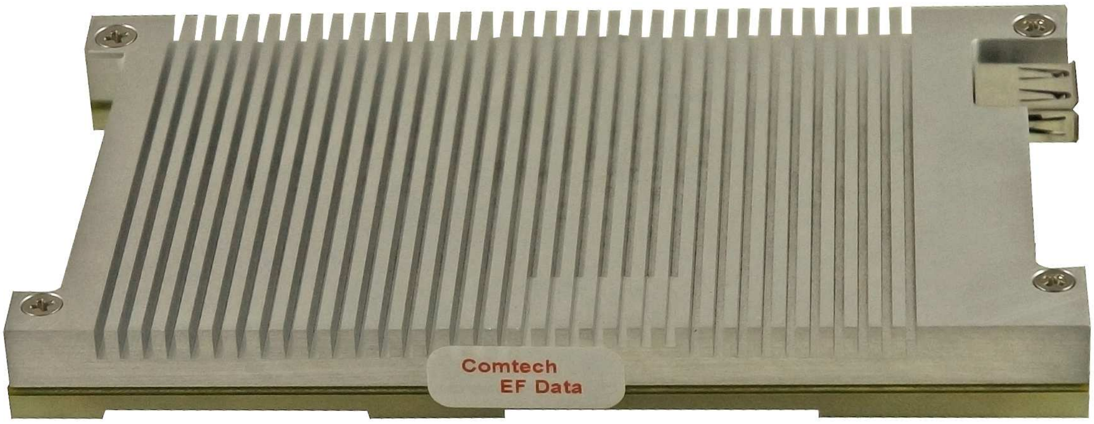

Figure 5 – Tamper-Evident Label Placement (Left Side View)

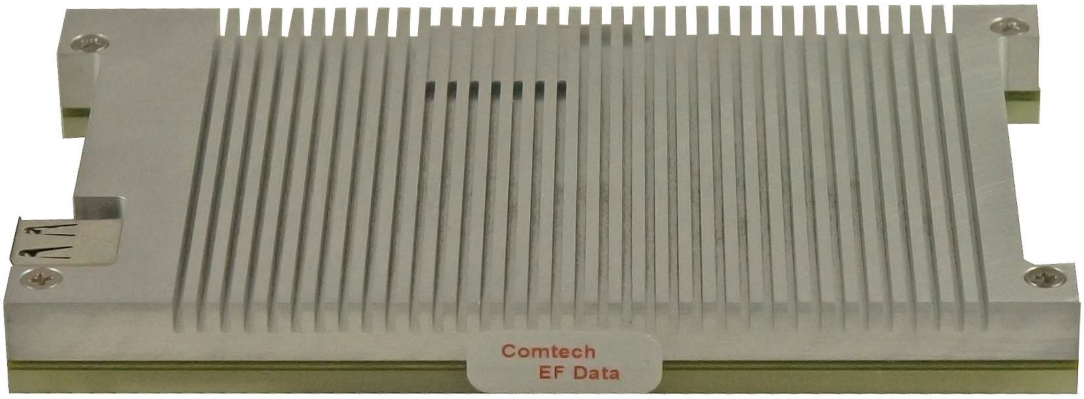

Figure 6 – Tamper-Evident Label Placement (Right Side View)

- The CO must visually inspect the module periodically for signs of tampering (including labels that have been voided, peeled off, or damaged in any way). If signs of tampering are noticed, the CO should remove the module from service and contact Comtech EF Data Corporation.

3.1.5 Zeroization

To perform zeroization of private keys and CSPs and bring the module back to the factory default setting, the CO will navigate to the “Configure” webpage via HTTPS or SSH and click on the “Zeroize All Keying Material” button. After clicking the button, the CO must do a power cycle on the module to clear all other keying material contained in volatile memory and being used by the module.

Unauthenticated users can also send a zeroization command to the module through the Mailbox interface. When the module receives the appropriate zeroization command, it will proceed to zeroize all cryptographic secret keys and CSPs.

3.2 User Guidance

The User role uses 256-bit AES in CTR mode for bulk encryption of all data requiring encryption.

4 Acronyms

This section defines the acronyms used throughout the Security Policy.

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CTR	Counter
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DES	Data Encryption Standard
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Standard
ED/EE	Electronic Distribution/Electronic Entry
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
ICs	Integrated Circuits
KAT	Known Answer Test
KEK	Key Encryption Key
MAC	Message Authentication Code
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
PVCS	Polytron Version Control System
RSA	Rivest Shamir Adleman
SMAT	Shared Modem Access Token
SSH	Secure Shell

Acronym	Definition
SSL	Secure Socket Layer
TDK	TRANSEC Decryption Key
TEK	TRANSEC Encryption Key
TLS	Transport Layer Security
TRANSEC	Transmission Security
USB	Universal Serial Bus
VSS	Visual Source Safe

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, Virginia 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com