Unified Crypto Module

Hardware Version: PL-0000235-2; Firmware Version: 2.2.4
FIPS 140-2 Non-Proprietary Security Policy
FIPS Security Level: 2
Document Version: 1.9

Prepared For:
Comtech EF Data Corporation

2114 West 7th Street
Tempe, Arizona 85281
United States of America
Phone: +1 (480) 333-2200
www.comtechefdata.com

Prepared by:
CGI Information Management Consultants Inc.
1410 Blair Place, 6th Floor
Ottawa, Ontario, K1J 9B9
Canada

www.cgi.com

This page intentionally left blank.

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Contents

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figures

Tables

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Comtech EF Data Corporation's Unified Crypto Module (Hardware Version: PL-0000235-2; Firmware Version: 2.2.4). This Security Policy describes how the Unified Crypto 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 (CSE): http://csrc.nist.gov/groups/STM/cmvp/index.html

The Unified Crypto 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

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 Unified Crypto 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 solutions, called the

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SLM-5650A and the DMD2050E, are IP[1] satellite modems designed to provide efficient and reliable data transmission over complex satellite connections.

The SLM-5650A and DMD2050E Satellite Modems include a single FIPS module called the Unified Crypto 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 Unified Crypto Module uses 256-bit AES[2] for bulk encryption of all data requiring encryption. The module is managed using a graphical user interface (GUI) via HTTPS[3] over TLS[4] (referred as Management & Control Console) and a command line interface (CLI) over SSH[5].

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 shows a satellite modem sending and receiving traffic in a typical deployment.

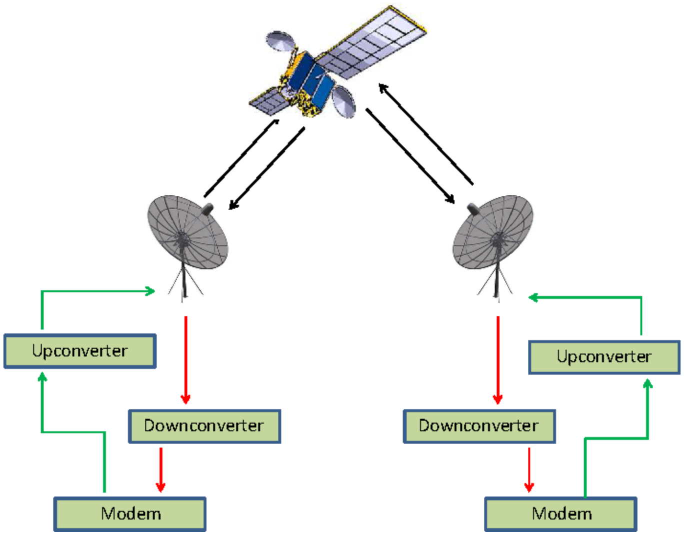

Figure 1 - Typical Deployment of Satellite Modems

The Unified Crypto Module is validated at the FIPS 140-2 Section levels shown in Table 1.

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

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 1 - FIPS 140-2 Section & Level

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[6]	2
9	Self tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Unified Crypto Module is a multi-chip embedded hardware cryptographic module (Hardware Version: PL-0000235-2; Firmware Version: 2.2.4) that provides bulk encryption and decryption, and secure communication protocols to the SLM-5650A and DMD2050E Satellite Modems. The modules operate in a mixed mode, meaning that Approved security functions are available alongside non-Approved security functions. Exercising cryptographic functions and services designated by this security policy as being FIPS Approved, means that the module is operating in the FIPS Approved mode. Those which are not listed as an Approved or allowed security function are considered to be non-FIPS Approved. The module will be operating in the non-Approved mode while non-Approved security functions are in use.

- The SLM-5650A Mixed Mode operates when the Unified Crypto Module is within the SLM-5650A Satellite Modem.
- The DMD2050E Mixed Mode operates when the Unified Crypto Module is embedded within the DMD2050E Satellite Modem.

Each mode provides its own cryptographic services, cryptographic algorithms, and cryptographic self-tests. Any differences between the modes will be highlighted in the sections below.

2.2.1 Unified Crypto Module Physical Representation

The Unified Crypto Module consists of a hardware platform composed of a Power Performance Computing (Power PC) based host processor and an FPGA[7] which performs the bulk encryption and decryption services for the module. The entire contents of the module, including all hardware, firmware, and data are protected by a metal cover on the top side and a hard plastic material on the bottom side of the module.

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

[7] FPGA – Field Programmable Gate Array

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 2 and Figure 3 below show the top and bottom side of the multi-chip embedded cryptographic module, respectively.

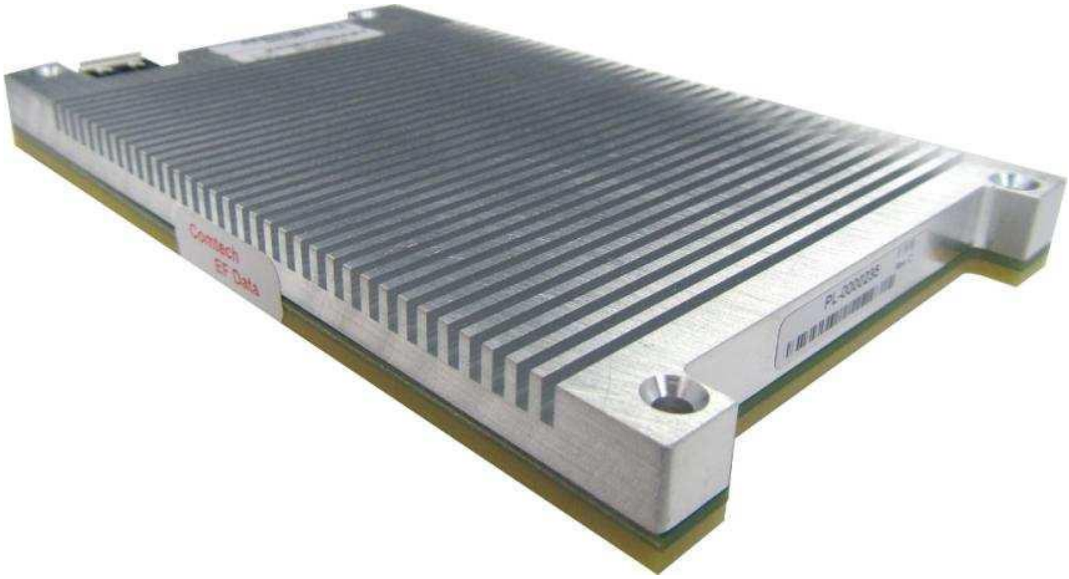

Figure 2 - Unified Crypto Module (Top)

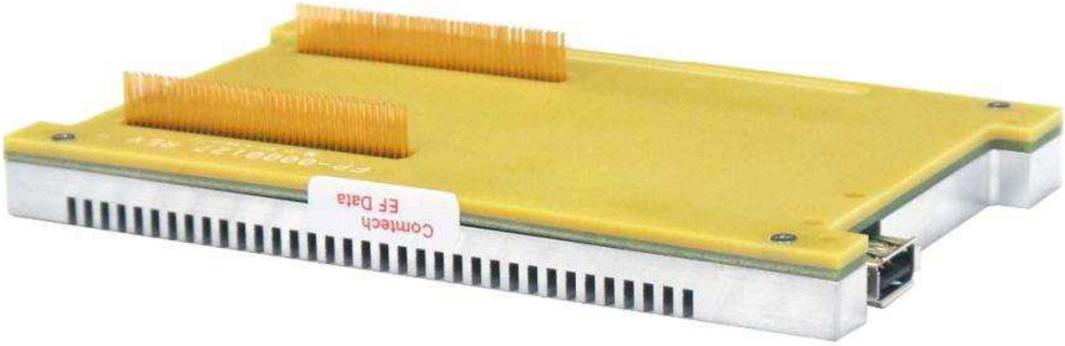

Figure 3 - Unified Crypto Module (Bottom)

2.2.2 Unified Crypto Module Logical Representation

With two mixed modes of operation, the Unified Crypto Module is capable of interacting with both the SLM-5650A Satellite Modem (SLM-5650A Mixed Mode) and the DMD2050E Satellite Modem (DMD2050E Mixed Mode). In either mode the processor of the module interacts with the FPGA, flash memory, and RAM. When operating in the SLM-5650A Mixed Mode, the module will directly interact with the Ethernet switch of the SLM-5650A Satellite Modem. When operating in the DMD2050E Mixed Mode, the module will directly interact with the Ethernet switch and the CPU[8] of the DMD2050E Satellite Modem.

Figure 4 is a block diagram showing the module interfacing with the SLM-5650A Satellite Modem and operating in the SLM-5650A Mixed Mode. The module’s cryptographic boundary is portrayed as the red dotted line and consists of the blue components within the dotted line boundary.

[8] CPU – Central Processing Unit

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

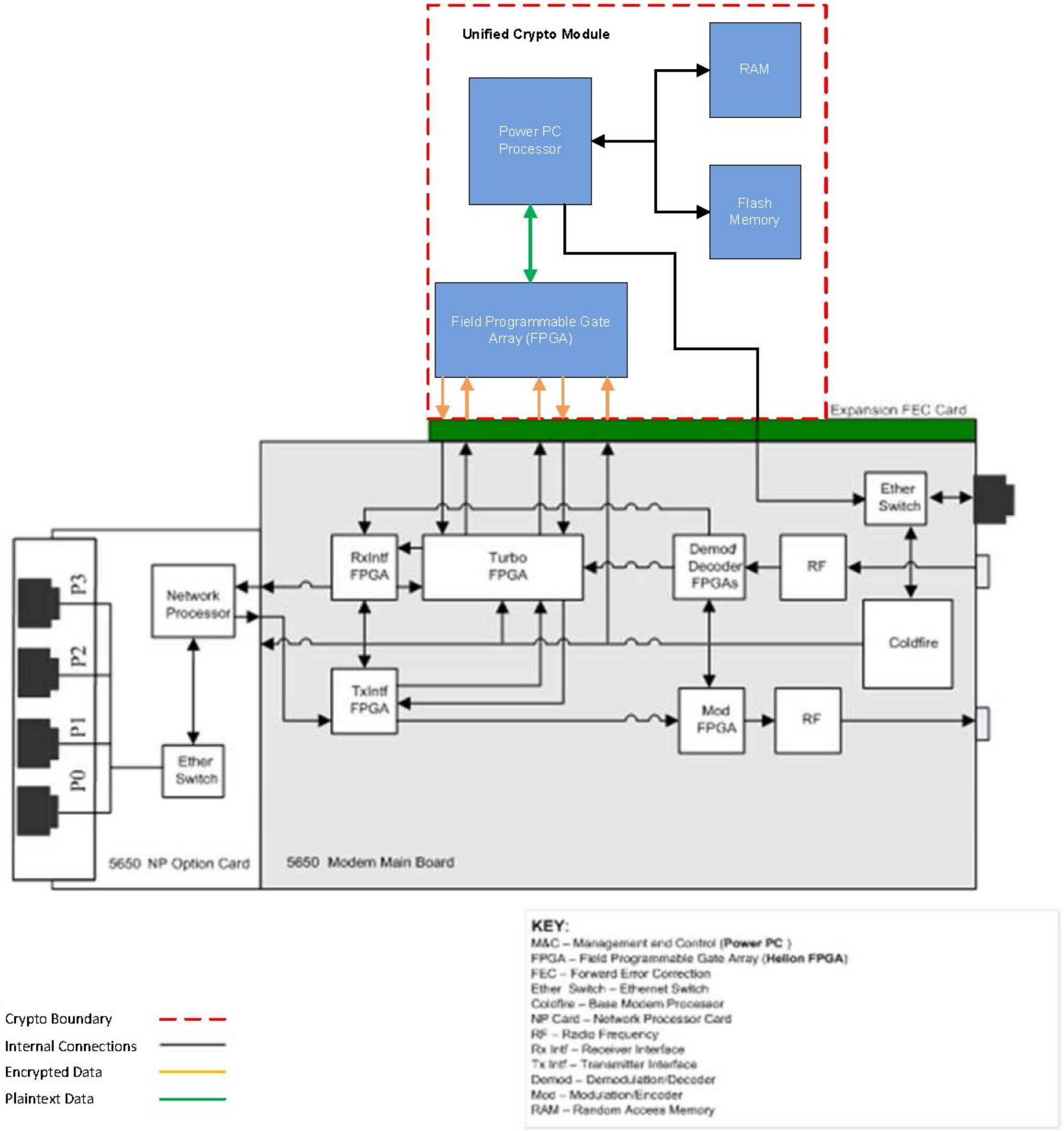
Unified Crypto Module
RAM
Power PC Processor
Flash Memory
Field Programmable Gate Array (FPGA)
Expansion FEC Card
Ether Switch
RxIntf FPGA
Turbo FPGA
Demod Decoder FPGAs
RF
Network Processor
Coldfire
TxIntf FPGA
Mod FPGA
RF
P3
P2
P1
P0
Ether Switch
5650 NP Option Card
5650 Modem Main Board
KEY:
M&C – Management and Control (Power PC)
FPGA – Field Programmable Gate Array (Helion FPGA)
FEC – Forward Error Correction
Ether Switch – Ethernet Switch
Coldfire – Base Modem Processor
NP Card – Network Processor Card
RF – Radio Frequency
Rx Intf – Receiver Interface
Tx Intf – Transmitter Interface
Demod – Demodulation/Decoder
Mod – Modulation/Encoder
RAM – Random Access Memory
Crypto Boundary
Internal Connections
Encrypted Data
Plaintext Data

Figure 4 - Unified Crypto Module with the SLM-5650A Satellite Modem (SLM-5650A Mixed Mode)

The block diagram in Figure 5 shows the module interfacing with the DMD2050E Satellite Modem and operating in the DMD2050E Mixed Mode. The module’s cryptographic boundary is portrayed as the red dotted line and consists of the blue components within the dotted line boundary.

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

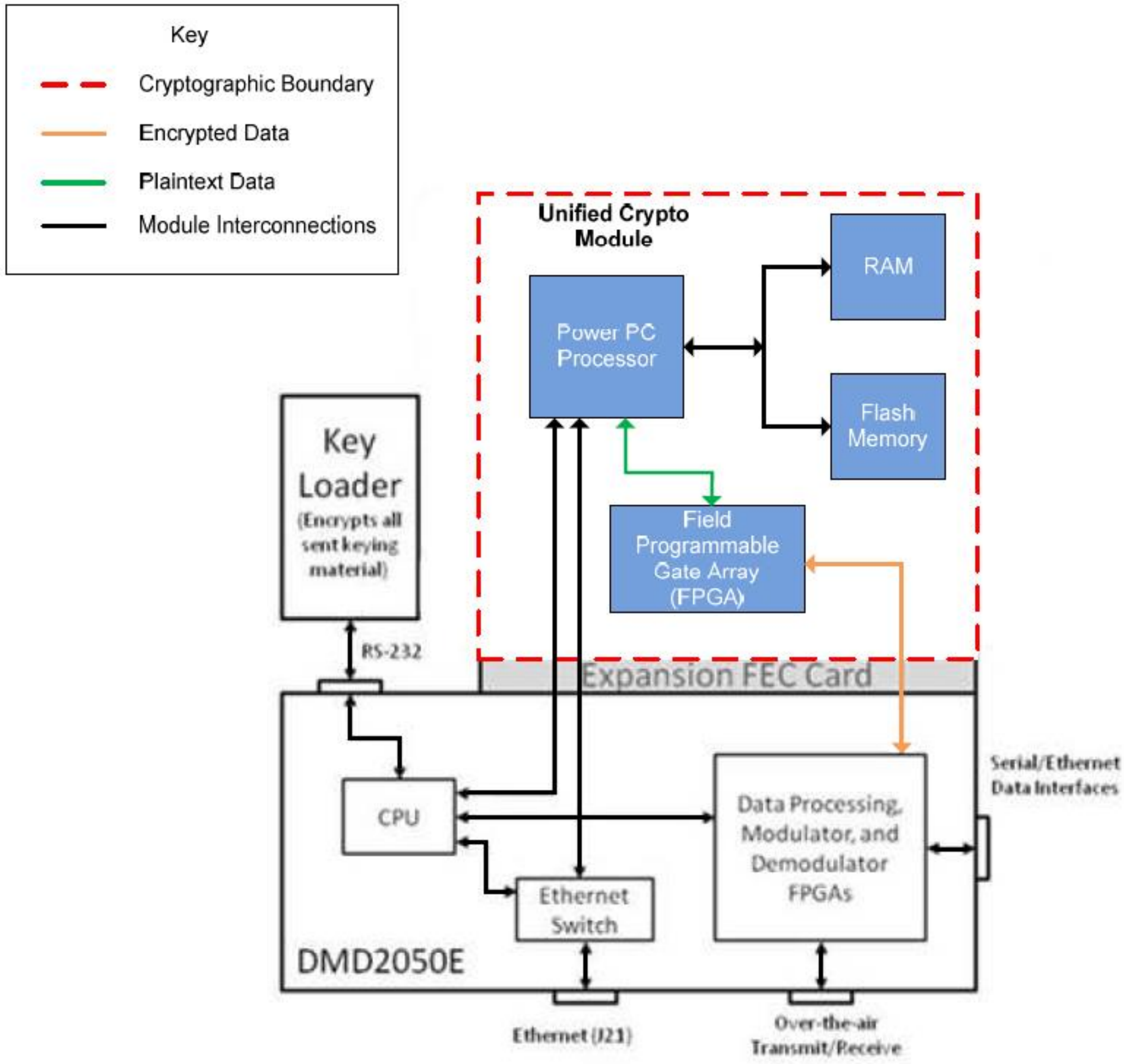

Figure 5 - Unified Crypto Module with the DMD2050E Satellite Modem (DMD2050E Mixed Mode)

2.3 Module Interfaces

The Unified Crypto 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

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.3.1 Physical Interfaces

The module features two 80-pin connector physical interfaces, as depicted in Figure 3. These 80-pin connectors provide a physical interface for the module's data, status, control, and power. The physical interfaces provided by each 80-pin connector (Interface Connector and M&C Connector) are as follows:

- Interface Connector
  - Receiver(Rx) FPGA Interface
  - Transmitter(Tx) FPGA Interface
  - Encoder/Modulator Interface
  - Decoder/Demodulator Interface
  - Ethernet Interface
  - Power Interface
- M&C Connector
  - System Clock Interface
  - Mailbox Interface
  - Power Interface

The interfaces listed above each map to individual pins on each of the connectors. Table 2 provides a mapping of each physical interface to the pins which support that interface.

Table 2 - Mapping of Unified Crypto Module Physical Interfaces to Pin Assignment

Connector	Physical Interface	Pin Assignment
Interface Connector[9]	Receiver (Rx) FPGA Interface	19-26, 29, 30
	Transmitter (Tx) FPGA Interface	33-40, 43, 44
	Encoder/Modulator Interface	47-54, 57, 58
	Decoder/Demodulator Interface	5-12, 15, 16
	Ethernet Interface	77-80
	Power Interface	1-4, 13, 14, 17, 18, 27, 28, 31, 32, 41, 42, 45, 46, 55, 56, 59-62, 75, 76
M&C Connector[10]	System Clock Interface	3, 4
	Mailbox Interface	13-15, 19, 20, 2330, 33, 34, 37-44
	Power Interface	1, 2, 5-12, 16-18, 21, 22, 31, 32, 35, 36, 45-76

Note: The USB[11] interface shown on the left-hand side of the module in Figure 2 and Figure 3 is not supported by the module when operating both mixed modes. Therefore the interface is not considered a physical interface to the module.

2.3.2 Logical Interfaces

The physical interfaces listed in Table 2 of Section 2.3.1 can be mapped to the logical interfaces defined by FIPS 140-2. Logical interfaces are identical between the two mixed modes of operation. Table 3 provides a mapping of each FIPS 140-2 logical interface to each physical interface.

[9] Pins 63-74 are not used by the module

[10] Pins 77-80 are not used by the module

[11] USB – Universal Serial Bus

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 3 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Unified Crypto Module Interface
Data Input	Receiver (Rx) FPGA Interface, Decoder/Demodulator Interface, Ethernet Interface, Mailbox Interface
Data Output	Transmitter (Tx) 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

In both mixed modes of operation, the module supports a Crypto Officer (CO) role and a User role. The CO role is responsible for the secure management of the module. The User role can modify encryption and decryption parameters and performs the actual data protection services of encryption and decryption.

The module supports the ability for multiple concurrent operators to be accessing the module at once. The services available to the CO and User roles are dependent on which mixed mode is operating on the module. The tables below show the services that are available to the CO and User in each mixed mode and the Critical Security Parameters (CSPs) that are accessed by those services. Please note that the keys and CSPs listed in the tables use the following notation to indicate the type of access required:

- R – The item is read or referenced by the service.
- W – The item is written or updated by the service.
- X – The item is executed by the service. (The item is used as part of a cryptographic function.).

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 when operating in the SLM-5650A Mixed Mode are provided in Table 4 below.

Table 4 - Mapping of Crypto Officer Role's Services to CSPs and Type of Access in the SLM-5650A Mixed Mode

Service	Description	CSP and Type of Access
Initialize and install	Initialize and install the Unified Crypto Module	None
Configure the FIPS Unified Crypto Module	Allows the operator to configure security-sensitive parameters	TRANSEC[12] Passphrase – W TRANSEC Key – W Operator Password – W/X TEK[13] and TDK[14] – W
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	Operator Password – W

[12] TRANSEC – Transmission Security
[13] TEK – Transmission Encryption Key
[14] TDK – Transmission Decryption Key

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	CSP and Type of Access
Create Secure Web Management Session (Web GUI)	Access the module using TLS protocol	Operator Password – X TLS Public/Private keys – R/X TLS Session Authentication Key –W/R/X TLS Session key – W/R/X
Create Secure CLI Management Session (SSH)	Access the module using SSH protocol	Operator Password – X SSH Public/Private keys – R/X SSH Session Authentication Key – W/R/X SSH Session Key – W/R/X Diffie-Hellman Parameters – W/R/X
Set TRANSEC Seed Key (TSK)	Set the TSK via SSH or HTTPS	Operator Password – X SSH Public/Private keys – R/X SSH Session Authentication Key – W/R/X SSH Session Key – W/R/X Diffie-Hellman Parameters – W/R/X TLS Public/Private keys – R/X TLS Session Authentication Key –W/R/X TLS Session key – W/R/X TRANSEC Seed Key – W
Set TRANSEC Passphrase	Set the TRANSEC Passphrase via HTTPS or SSH	Operator Password – X SSH Public/Private keys – R/X SSH Session Authentication Key – W/R/X SSH Session Key – W/R/X Diffie-Hellman Parameters – W/R/X TLS Public/Private keys – R/X TLS Session Authentication Key –W/R/X TLS Session key – W/R/X TRANSEC Passphrase – W
Firmware Upgrade (via TLS)	Configure firmware upgrade parameters of the module	Upgrade Key – R/X TLS Public/Private keys – R/X TLS Session Authentication Key – R/X TLS Session key – R/X
Event Log Parameters	Check the event log parameters of the module	None
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 – W

Descriptions of the services available to the Crypto Officer role when operating in the DMD2050E Mixed Mode are provided in Table 5 below.

Table 5 - Mapping of Crypto Officer Services to CSPs and Type of Access in the DMD2050E Mixed Mode

Service	Description	CSPs and Type of Access
Initialize and install	Initialize and install the Unified Crypto Module	None
Configure the FIPS Unified Crypto Module	Allows the operator to configure security-sensitive parameters	DRBG[15] SP800- 90A seed – W/R/X SMAT[17] – W Operator Password – W/X TEK and TDK – W
Configure Network Parameters	Allows the operator to configure	None

[15] DRBG – Deterministic Random Bit Generator

[17] SMAT - Shared Message Authentication Token

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	CSPs and Type of Access
	network parameters of the module	
Configure Operator Credential Parameters	Allows the operator to configure operator credential parameters of the module	Operator Password – W
Create Secure Web Management Session (Web GUI)	Access the module using TLS protocol	Operator Password – X TLS Public/Private keys – R/X TLS Session Authentication Key –W/R/X TLS Session key – W/R/X
Create Secure CLI Management Session (SSH)	Access the module using SSH protocol	Operator Password – X SSH Public/Private keys – R/X SSH Session Authentication Key – W/R/X SSH Session Key – W/R/X Diffie-Hellman Parameters – W/R/X
Set the SMAT (HTTPS)	Set the SMAT via HTTPS	Key Encryption Key (KEK) – R/X Operator Password – X TLS Public/Private keys – R/X TLS Session Authentication Key –W/R/X TLS Session key – W/R/X SMAT – W
Set the SMAT (SSH)	Set the SMAT via SSH	Key Encryption Key (KEK) – R/X Operator Password – X Diffie-Hellman Parameters – W/R/X SSH Public/Private keys – R/X SSH Session Authentication Key – W/R/X SSH Session Key – W/R/X SMAT – W
Load TLS Keys	Load externally generated TLS Public and Private key components onto the module using existing TLS session	TLS Public/Private keys (new) – W TLS Public/Private keys (existing) – R/X TLS Session Authentication Key – R/X TLS Session key – R/X
Firmware Upgrade (via TLS)	Configure firmware upgrade parameters of the module	Upgrade Key – R/X TLS Public/Private keys – R/X TLS Session Authentication Key – R/X TLS Session key – R/X
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 – W

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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. The User also has access to configuration items such as IP address and encryption/decryption parameters. The User has access to the services listed in Table 6 when operating in either mixed mode. CSP access varies slightly between modes, and is shown in the table below.

Table 6 - Mapping of User Services to CSPs and Type of Access for both Mixed Modes

Service	Description	CSPs and Type of Access	
		SLM 5650A Mixed Mode	DMD2050E Mixed Mode
Configure encryption/decryption parameters	Configure encryption/decryption parameters of the module	None	None
Encryption/decryption	Perform encryption and/or decryption of data	TEK – X TDK – X	TEK – X TDK – X SMAT – X
Key Agreement	Key exchange and key agreement for remote session establishment	Diffie-Hellman Parameters – W, R, X	ECDH[18] Parameters – W, R, X
Change IP address and Subnet	Change the module's IP address and subnet	None	None
Change network default gateway	Change the module's IP network default gateway	None	None

2.4.3 Additional Services

In both mixed modes, the module provides a limited amount of services for which the operator does not have to assume an authorized role. Interaction with the module is done through the Mailbox interface via the front panel of either satellite modem. Table 7 lists the services for which the operator is not required to assume an authorized role. These services are available in both mixed modes of operation. None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

Table 7 - Mapping of Additional Services to CSPs and Type of Access for both Mixed Modes

Service	Description	CSP and Type of Access	
		SLM-5650A Mixed Mode	DMD2050E Mixed Mode
Change IP address and Subnet	Change the module's IP address and subnet	None	None
Change network default gateway	Change the module's IP network default gateway	None	None
Zeroization	Zeroize all the cryptographic keys and key components	All keys and CSPs – W	All keys and CSPs – W

[18] ECDH – Elliptic Curve Diffie-Hellman

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4.4 Non-Approved Services

While operating in the SLM-5650A Mixed Mode or DMD2050E Mixed Mode, the Unified Crypto Module provides services, which when used, will result in the module operating in a non-Approved mode of operation. The module will transition back to an Approved mode of operation at the completion of the service. The list of those services is provided in Table 8.

Table 8 - List of Non-Approved Services

Service	Service Accessible?	
	SLM-5650A Mixed Mode	DMD2050E Mixed Mode
RSA Signature Generation (with SHA-1)	✓	✓
1024-bit Diffie-Hellman Key Agreement	✓	✓

2.4.5 Authentication Mechanism

The module supports role-based authentication with implicit role selection in both mixed modes of operation. An operator of the module will login to the module using the described methods below. The operator authenticates to a set of roles and will assume the role of CO or User implicitly, based on the service that is accessed. Depending on which mixed mode the module is in, there are a variety of methods that the operator may use to log in.

2.4.5.1 SLM-5650A Mixed Mode Authentication

The operator authenticates with a username and password over a TLS or SSH connection. Passwords are required to be at least 7 characters long. All printable ASCII[19] characters (33-126) except for #34 ("), #58 (:), #60 (<), #62 (>), and #126 (~) can be used, which gives a total of 89 characters to choose from. These password restrictions are enforced by the module. With the possibility of repeating characters, the probability of a random attempt falsely succeeding is 1 in 89^7, or 1 in 44,231,334,895,529.

A minimum of 442,313,348 password attempts would be required in one minute to lower the random attempt success rate to less than 1:100,000. The fastest connection supported by the module is less than 155 Mbps[20]. Hence, at most 9,300,000,000 bits of data ($155 \times 10^6 \times 60$ seconds, or 9.3×10^9) 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. This is much less than the minimum 442,313,348 password attempts that are required.

2.4.5.2 DMD2050E Mixed Mode Authentication

The operator authenticates with a username and password over a TLS or SSH connection. Passwords are required to be at least 7 characters long. All printable ASCII characters, including "space", can be used, which gives a total of 95 characters to choose from. These password restrictions are enforced by the module. With the possibility of repeating characters, the probability of a random attempt falsely succeeding is 1:957, or 1:69,833,729,609,375.

A minimum of 698,337,296 password attempts would be required 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.

[19] ASCII - American Standard Code for Information Interchange

[20] Mbps - Megabits per second

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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. This is much less than the minimum 698,337,296 password attempts that would be required.

The User can also authenticate by proving knowledge of a shared secret (SMAT) that is a 40-character secret specified by the User. The secret can consist of upper-case characters, numbers (0-9), and space, giving a total of 37 possible characters to choose from. With the possibility of repeating characters, the probability of a random attempt falsely succeeding is 1:37^{40}, which is less than the required 1:1,000,000.

When authenticating with the SMAT, the operator provides knowledge of a shared secret that is larger than the standard password. The probability of success for a brute force attack against the User's authentication mechanism using this method is even less likely than when using a 7 character password. Therefore, the SMAT provides assurance that the probability of a random successful attempt in minute is less than 1:100,000.

2.5 Physical Security

The Unified Crypto 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[21] 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 Unified Crypto 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 Unified Crypto Module was designed to operate in two mixed modes of operation; the SLM-5650A Mixed Mode and the DMD2050E Mixed Mode. Each mixed mode provides access to a different set of cryptographic algorithms, based on the needs of the satellite modem.

2.7.1 Cryptographic Algorithm Implementations

Table 9 lists the cryptographic algorithms implemented by the Unified Crypto Module when it is operating in the SLM-5650A Mixed Mode.

[21] IC - Integrated Circuit

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 9 - Cryptographic Algorithm Implementations in the SLM-5650A Mixed Mode

Approved or Allowed Security Function	Certificate Number
Symmetric Key Algorithm	
AES[22] – 128, 192 and 256-bit (ECB [23], CBC[24], CFB1, CFB8, CFB128 , OFB[26], CTR, CCM, CMAC and GCM)	Cert. #4077
AES – 256-bit in ECB and CBC (FPGA)	Cert. #4079
Triple-DES[27] – K1, K2, K3 independent in ECB, CBC, TCFB1, TCFB8, TCFB64 and OFB modes	Cert. #2229
Secure Hashing Algorithm (SHA)	
SHA[28] -1, SHA-224, SHA-256, SHA-384 and SHA-512 (SHA-1 only allowed for hashing)	Cert. #3359
Message Authentication Code (MAC) Function	
HMAC using SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Cert. #2663
Random Number Generator (RNG)	
DRBG SP800- 90A	Cert. #1225
Asymmetric Key Algorithm	
RSA[29]	Cert. #2209
ECDSA[32]	Cert. #922
NIST SP 800-108 KBKDF	
KBKDF	Cert. #131
NIST SP 800-135 KDF	
KDF (TLS 1.2 and SSH)	Cert. #1084
Vendor Affirmation (Key generation compliance with NIST SP 800-133)	
CKG (vendor affirmed)	Affirmed

Caveats:

Additional information concerning SHA-1 and the DRBG SP800- 90A and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The module employs the following key establishment methodologies when operating in the SLM-5650A Mixed Mode. These key establishment methodologies are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (2048-bit)
  - (key agreement: key establishment methodology provides 112 bits of encryption strength)
- RSA (2048-bit)
  - (key wrapping; key establishment methodology provides 112 bits of encryption strength)

The module implements the following non-Approved security functions when operating in the SLM-5650A Mixed Mode. These algorithms and protocols are allowed for use in a FIPS-Approved mode of operation:

- Message Digest 5 (MD5)
  - For use with password obfuscation

[22] AES - Advanced Encryption Standard
[23] ECB - Electronic Codebook
[24] CBC - Cipher-Block Chaining
[26] OFB - Output Feedback
[27] DES - Data Encryption Standard
[28] SHA - Secure Hash Algorithm
[29] RSA - Rivest, Shamir, Adleman
[32] Elliptic Curve Digital Signature Algorithm

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

  - For use with the TLS 1.2 protocol
- Non-Deterministic Random Number Generator (NDRNG)
  - Provides seeding material for Approved DRBG

The module implements the following non-Approved security function when operating in the SLM-5650A Mixed Mode. Use of this function will transition the module into a non-Approved mode:

- Diffie-Hellman (1024-bit)
  - (key agreement; provides 80 bits of encryption strength)
- FIPS 186-2 RNG

Warning about the use of Triple-DES: As per NIST SP 800-67, the security of Triple-DES is affected by the number of blocks processed with one key bundle. Therefore, the key bundle ***shall not*** be used to encrypt more than 2^{32} 64-bit data blocks. The module services affected by this restriction are those listed in Tables 4 and 5 which use TLS session keys.

Table 10 lists the cryptographic algorithms implemented by the Unified Crypto Module when it is operating in the DMD2050E Mixed Mode.

Table 10 - Cryptographic Algorithm Implementations in the DMD2050E Mixed Mode

Approved or Allowed Security Function	Certificate Number
Symmetric Key Algorithm	
AES – 128, 192 and 256-bit (ECB, CBC, CFB8, CFB128, OFB, CTR, CCM, CMAC and GCM)	Cert. #4077
AES – 256-bit in ECB and CTR[36] mode (FPGA)	Cert. #4078
Triple-DES – K1, K2, K3 independent in ECB, CBC, TCFB1, TCFB8, TCFB64 and OFB modes	Cert. #2229
Secure Hashing Algorithm (SHA)	
SHA -1, SHA-224, SHA-256, SHA-384 and SHA-512 (SHA-1 only allowed for hashing)	Cert. #3359
Message Authentication Code (MAC) Function	
HMAC using SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Cert. #2663
Random Number Generator (RNG)	
DRBG SP800- 90A	Cert. #1225
Asymmetric Key Algorithm	
RSA	Cert. #2209
ECDSA	Cert. #922
EC Diffie-Hellman (CVL)	Cert. #899
NIST SP 800-135 KDF	
KDF (TLS 1.2 and SSH)	Cert. #1084
Vendor Affirmation (Key generation compliance with NIST SP 800-133)	
CKG (vendor affirmed)	Affirmed

[36] CTR - Counter

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Caveats:

Additional information concerning SHA-1 and the DRBG SP800- 90A and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The module employs the following key establishment methodologies when operating in the DMD2050E Mixed Mode. These key establishment methodologies are allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (2048-bit)
  - (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC[38] Diffie-Hellman
  - (key agreement; provides 256-bits of encryption strength)
- RSA (2048-bit)
  - (key wrapping; key establishment methodology provides 112 bits of encryption strength)

The module implements the following non-Approved security functions when operating in the DMD2050E Mixed Mode. These functions are allowed for use in a FIPS-Approved mode of operation:

- Message Digest 5 (MD5)
  - For use with password obfuscation
  - For use with the TLS 1.2 protocol
- NDRNG
  - Provides seeding material for Approved RNGs

The module implements the following non-Approved security function when operating in the DMD2050E Mixed Mode. Use of this function will transition the module into a non-Approved mode:

- Diffie-Hellman (1024-bit)
  - (key agreement; provides 80 bits of encryption strength)

Warning about the use of Triple-DES: As per NIST SP 800-67, the security of Triple-DES is affected by the number of blocks processed with one key bundle. Therefore, the key bundle ***shall not*** be used to encrypt more than 2^{32} 64-bit data blocks. The module services affected by this restriction are those listed in Tables 4 and 5 which use TLS session keys.

[38] EC - Elliptic Curve

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.7.2 Critical Security Parameters

Each mixed mode has its own set of cryptographic keys, cryptographic key components, and CSPs. The key derivation functions in TLS and SSH have been tested as per NIST SP 800-135Rev1. No parts of the TLS or SSH protocols, other than the KDF, have been tested by the CAVP and CMVP.

Table 11 shows the CSPs employed by the module when operating in the SLM-5650A Mixed Mode.

Table 11 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs in the SLM-5650A Mixed Mode

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
TRANSEC Seed Key (TSK)	AES 256-bit key	256-bit	Generated by external and trusted key authority; Entered into the module electronically in encrypted form via TLS/SSH	ED/EE[39]	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Used as Key Derivation Key in NIST SP 800-108 KBKDF
TRANSEC Passphrase	Passphrase	N/A	Generated externally; Entered into the module electronically in encrypted form via TLS/SSH	ED/EE	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Used as part of the Fixed Input Data in NIST SP 800-108 KBKDF
TRANSEC Encryption keys (TEKs)	AES -CBC 256 bit	256-bit	Internally derived using NIST SP 800-108 KBKDF	Not applicable	Never exits the module	Stored in plaintext in volatile memory	By Zeroize command or power cycling the module	Encrypt the data
TRANSEC Decryption keys (TDKs)	AES -CBC 256 bit	256-bit	Internally derived using NIST SP 800-108 KBKDF	Not applicable	Never exits the module	Stored in plaintext 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 DRBG SP800- 90A	ED/EE	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Facilitates SSH sessions

[39] ED/EE – Electronic Distribution/Electronic Entry

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
TLS private Key	RSA 2048-bit key	112-bit	Factory default until externally generated	ED/EE	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Facilitates TLS sessions
SSH public key	RSA 2048-bit key	112-bit	Internally generated using the DRBG SP800- 90A	ED/EE	Public key exported electronically in plaintext	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Facilitates SSH
TLS public key	RSA 2048-bit key	112-bit	Factory default until externally generated	ED/EE	Public key exported electronically in plaintext	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	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 plaintext in volatile memory	Power cycle or session termination	Facilitates SSH/TLS sessions
TLS Session Authentication Key	HMAC SHA-1	112-bit	Established during the TLS handshake	TLS	Never exits the module	Stored in plaintext 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	112-bit; 128, 256-bit	Established	TLS	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data encryption/decryption for TLS sessions
SSH Session Authentication Key	HMAC SHA-1 Key	112-bit	Established during the SSH handshake	SSH	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data authentication for SSH sessions
SSH Session Key	AES-CTR 128-, 192-, 256-bit key	112-bit	Established during the SSH handshake	SSH	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data encryption/decryption for SSH sessions
Diffie-Hellman Public Parameters	Diffie-Hellman 2048-bit key	112-bit	Internally generated using the DRBG	Not applicable	Public exponent electronically	Stored in plaintext in volatile	Power cycle or session termination	Key exchange/agreement for SSH sessions

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
			SP800- 90A		in plaintext, private component not output	memory		
Diffie-Hellman Private Parameters	Diffie-Hellman 224-bit key	112-bit	Internally generated using the DRBG SP800- 90A	Not applicable	Public exponent electronically in plaintext, private component not output	Stored in plaintext in volatile memory	Power cycle or session termination	Key exchange/agreement for SSH sessions
Operator password	Password	See Section 2.4.5.1	Input by the CO during initialization	Not applicable	Never exits the module	Stored obfuscated[40] in non-volatile memory	By Zeroize command and then power cycling the module	Operator authentication
DRBG SP800-90A seed	256-bit key	256-bit	Internally generated. Additional entropy material may be input through TLS or SSH[41]	Not applicable	Never exits the module	Stored in plaintext in volatile memory	Power cycle	Generates FIPS-Approved random number
DRBG SP800-90A nonce	128-bit	128-bit	Internally generated.	Not applicable	Never exits the module	Stored in plaintext in volatile memory	Power cycle	Generates FIPS-Approved random number
Upgrade Key	ECDSA Public Key	P-521 curve	Externally generated; Hard coded into module	Not applicable	Never exits the module	Stored in plaintext in non-volatile memory	N/A	Upgrade to new firmware; Firmware load test

Table 12 shows the CSPs employed by the module when operating in the DMD2050E Mixed Mode.

[40] Obfuscation provided by MD5

[41] Additional entropy is checked to ensure the first and second half of the input value do not match

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 12 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs in the DMD2050E Mixed Mode

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
ECDH Public Parameters	ECDH 521-bit key	256-bit	Internally generated using the DRBG SP800-90A	ED/EE	Public exponent electronically in plaintext, private component not output	Stored in plaintext in volatile memory	Power cycle or session termination	Key exchange/agreement for over-the-air data encrypted sessions with peer devices
ECDH Private Parameters	P-521 curve size	256-bit	Internally generated using the DRBG SP800-90A	ED/EE	Public exponent electronically in plaintext, private component not output	Stored in plaintext in volatile memory	Power cycle or session[42] termination	Key exchange/agreement for over-the-air data encrypted sessions with peer devices
Key Encryption Key (KEK)	AES-256 CBC	256-bit	Generated externally and entered into the module electronically over the Key Loader	ED/EE	Never exits the module	Stored in plaintext in volatile memory	Power cycle	Encrypts the SMAT and DRBG SP800- 90A seed during entry
SMAT	Password	See Section 2.4.5.2	Generated externally and entered into the module electronically over TLS or SSH	ED/EE	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command or power cycling the module	Authenticate the user and over-the-air data transmitted and received packets
TRANSEC Encryption Keys (TEKs)	AES-CTR – 256-bit key	256-bit	Established during the ECDH handshake	ECDH	Never exits the module	Stored in plaintext in volatile memory	By Zeroize command or power cycling the module	Encrypt the data
TRANSEC Decryption keys (TDKs)	AES-CTR – 256-bit key	256-bit	Established during the ECDH handshake	ECDH	Never exits the module	Stored in plaintext 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 DRBG SP800-90A	ED/EE	Never exits the module	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Facilitates SSH sessions
TLS private Key	RSA 2048-bit key	112-bit	Factory default until externally	ED/EE	Never exits the module	Stored in plaintext in	By Zeroize command	Facilitates TLS sessions

[42] A session is defined as a single message transmitted from the key loader to the module. The session will end at the end of each message transmission.

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
			generated			non-volatile memory	and then power cycling the module	
SSH public key	RSA 2048-bit key	112-bit	Internally generated using the DRBG SP800-90A	ED/EE	Public key exported electronically in plaintext	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	Facilitates SSH
TLS public key	RSA 2048-bit key	112-bit	Factory default until externally generated	ED/EE	Public key exported electronically in plaintext	Stored in plaintext in non-volatile memory	By Zeroize command and then power cycling the module	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 plaintext in volatile memory	Power cycle or session termination	Facilitates SSH/TLS sessions
TLS Session Authentication Key	HMAC SHA-1	112-bit	Established during the TLS handshake	TLS	Never exits the module	Stored in plaintext 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	112-bit; 128, 256-bit	Established	TLS	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data encryption/decryption for TLS sessions
SSH Session Authentication Key	HMAC SHA-1 Key	112-bit	Established during the SSH handshake	SSH	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data authentication for SSH sessions
SSH Session Key	AES-CTR 128-, 192-, 256-bit key	112-bit	Established during the SSH handshake	SSH	Never exits the module	Stored in plaintext in volatile memory	Power cycle or session termination	Data encryption/decryption for SSH sessions
Diffie-Hellman Public Parameters	Diffie-Hellman 2048-bit key	112-bit	Internally generated using the DRBG SP800-90A	Not applicable	Public exponent electronically in plaintext, private component not output	Stored in plaintext in volatile memory	Power cycle or session termination	Key exchange/agreement for SSH sessions
Diffie-Hellman Private	Diffie-Hellman	112-bit	Internally generated using	Not applicable	Public exponent electronically in	Stored in plaintext in	Power cycle or session	Key exchange/agreement for

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Key Strength	Generation / Input	FIPS-Approved Establishment Mechanism	Output	Storage	Zeroization	Use
Parameters	224-bit key		the DRBG SP800-90A		plaintext, private component not output	volatile memory	termination	SSH sessions
Operator password	Password	See Section 2.4.5.1	Input by the CO during initialization	Not applicable	Never exits the module	Stored obfuscated[43] in non-volatile memory	By Zeroize command and then power cycling the module	Operator authentication
DRBG SP800-90A seed	256-bit	256-bit	Internally generated. Additional entropy[44] material may be input through TLS or SSH.	Not applicable	Never exits the module	Stored in plaintext in volatile memory	Power cycle	Generates FIPS-Approved random number
DRBG SP800-90A nonce	128-bit	128-bit	Internally generated.	Not applicable	Never exits the module	Stored in plaintext in volatile memory	Power cycle	Generates FIPS-Approved random number
Upgrade Key	ECDSA Public Key	P-521 curve	Externally generated; Hard coded into module	Not applicable	Never exits the module	Stored in plaintext in non-volatile memory	N/A	Upgrade to new firmware; Firmware load test

[43] Obfuscation provided by MD5

[44] Additional entropy is checked to ensure the first and second half of the input value do not match

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.7.3 Key Generation

When operating in the SLM-5650A Mixed Mode, the module uses NIST SP 800-108 Key-Based Key Derivation Function (KBKDF) to generate keys. When the module is operating in the DMD2050E Mixed Mode, only the FIPS-Approved NIST SP800-90A DRBG is used to generate keys.

2.7.4 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 secret or private keys or CSPs from its physical boundary.

2.7.5 CSP Storage and Zeroization

All of the keys and CSPs are stored in either non-volatile or volatile memory in plaintext or obfuscated form and can be zeroized by using the Zeroization command and then power cycling the cryptographic module. More information on zeroization techniques can be found in Section 3.1.5.

2.8 EMI/EMC

The Unified Crypto 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). The module was tested in both the SLM-5650A Satellite Modem and the DMD2050E Satellite Modem.

2.9 Self-Tests

The Unified Crypto Module performs the required power-up self-tests during the initial power-up in both mixed modes of operation. On-demand self-tests can be performed by the "Perform Self-Test" service[45] available to the CO or by cycling the power of the module. The module executes conditional self-tests during normal operation whenever a new random number or asymmetric key pair are generated. The power-up and conditional self-tests that are run by the module are dependent on which mixed mode the module is operating in. The following sections describe the power-up and conditional self-tests that are run by the module in each mixed mode.

2.9.1 Power-Up Self-Tests

The Unified Crypto Module performs a CRC[46]-32 firmware integrity test on its first power-up. Upon the successful completion of the firmware integrity test, the module will detect the modem and determine the correct mixed mode required. After selecting the correct firmware, the module will perform the mode's power-up self-tests. Until the power-up self tests are successfully completed the module will not output any data.

The power-up self-tests that are run by the module when operating in the SLM-5650A mixed Mode is:

- FPGA AES Encryption Known Answer Test (KAT)
- FPGA AES Decryption KAT
- AES KAT
- TDES KAT
- SHA-1 KAT
- SHA-224 KAT, tested as part of SHA-256 KAT
- SHA-256 KAT
- SHA-384 KAT, tested as part of SHA-512 KAT
- SHA-512 KAT
- HMAC SHA-1 KAT
- HMAC SHA-224 KAT
- HMAC SHA-256 KAT
- HMAC SHA-384 KAT

[45] "Perform Self-Test" service only available when operating in the SLM-5650A Mixed Mode

[46] CRC – Cyclic Redundancy Check

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- HMAC SHA-512 KAT
- RSA KAT
- ECDSA Pairwise Consistency Test (PCT)
- SP800- 90A CTR DRBG KAT
- SP800- 90A Hash Based DRBG KAT
- SP800- 90A HMAC Based DRBG KAT
- NIST SP 800-90A, Section 11.3 Health Tests
- EC Diffie-Hellman (Primitives) KAT

The power-up self-tests that are run by the module when operating in the DMD2050E Mixed Mode are:

- FPGA AES Encryption KAT
- FPGA AES Decryption KAT
- AES KAT
- TDES KAT
- SHA-1 KAT
- SHA-224 KAT, tested as part of SHA-256 KAT
- SHA-256 KAT
- SHA-384 KAT, tested as part of SHA-512 KAT
- SHA-512 KAT
- HMAC SHA-1 KAT
- HMAC SHA-224 KAT
- HMAC SHA-256 KAT
- HMAC SHA-384 KAT
- HMAC SHA-512 KAT
- RSA KAT
- ECDSA PCT
- SP800- 90A CTR DRBG KAT
- SP800- 90A Hash Based DRBG KAT
- SP800- 90A HMAC Based DRBG KAT
- NIST SP 800-90A, Section 11.3 Health Tests

2.9.2 Conditional Self-Tests

Conditional self-tests are run every time a new random number is generated or a new asymmetric key pair is generated. Depending on the mixed mode the module is operating in, different conditional self-tests will be run during normal operation. In both mixed modes, data output is inhibited while conditional self-tests are executing.

The module performs the following conditional self-tests when operating in the SLM-5650A Mixed Mode:

- Continuous RNG Test for the DRBG SP800- 90A
- Continuous RNG Test for the NDRNG
- Pairwise Consistency Test for RSA
- Pairwise Consistency Test for ECDSA
- Firmware load test (ECDSA digital signature verification)

The module performs the following conditional self-tests when operating in the DMD2050E Mixed Mode:

- Continuous RNG Test for the DRBG SP800- 90A
- Continuous RNG Test for the NDRNG
- Pairwise Consistency Test for RSA
- Pairwise Consistency Test for ECDSA
- Firmware load test (ECDSA digital signature verification)

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.9.3 Self-Test Failures

If the firmware integrity test fails, the system will not boot into either mixed mode. 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 the standby firmware is corrupt, the module must be serviced by Comtech EF Data Corporation.

For both mixed modes of operation, the following self-test error behavior occurs:

If any of the power-up self-tests fail, the module disables data transmission, shows a fault indication on the modem's front panel and LEDs, and writes the fault information to the modem event log. No data output or cryptographic operations are possible when the module enters the critical error state. The CO can attempt to clear this error by power-cycling the module.

If a conditional self-test fails, the module disables data transmission, shows a fault indication on the modem's front panel and LEDs, and writes the fault information to the modem event log. No data output or cryptographic operations are possible when the module enters a temporary error state. To clear the error state, the module resets itself, performs power-up self-tests, and resumes normal operation.

2.10Mitigation of Other Attacks

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

3 Secure Operation

The Unified Crypto Module meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in one of the two mixed modes 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 Unified Crypto Module is designed to be embedded in either the SLM-5650A or DMD2050E Satellite Modem as a single FIPS card called the Unified Crypto Module. The module is capable of operating in two mixed modes of operation. The first mixed mode is the SLM-5650A Mixed Mode and is defined as when the Unified Crypto Module is embedded and operating within the SLM-5650A Satellite Modem. The second mixed mode is the DMD2050E Mixed Mode and is defined when the Unified Crypto Module is embedded and operating within the DMD2050E Satellite Modem.

The following steps provide the rules for the secure installation of the cryptographic module into either the SLM-5650A or DMD2050E Satellite Modems:

<u>Installation:</u>

- Turn off modem power
- Put on Electrostatic Discharge (ESD) protection
- Remove top cover of the satellite modem
- Install Forward Error Correction (FEC) board into modem
- Install Unified Crypto Module card onto FEC board
- Replace the top cover of the satellite modem
- Turn on modem power

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Once the Unified Crypto Module is properly installed into either of the satellite modems, the CO shall configure the module for the correct mixed mode of operation. If the module was installed into the SLM-5650A Satellite Modem, the CO shall perform the following configuration steps to place the module into the SLM-5650A Mixed Mode:

Configuration into the SLM-5650A Mixed Mode:

- Configure IP Address
- Log into either the HTTPS or SSH interface as the Crypto Officer for first time access (Default username and password: comtech, comtech)
- Change default Crypto Officer Password
- Enter the initial TRANSEC Seed Key
- Enter the initial TRANSEC Passphrase

If the module was installed into the DMD2050E Satellite Modem, the CO shall perform the following configuration steps to place the module into the DMD2050E Mixed Mode:

Configuration into the DMD2050E Mixed Mode:

- Configure IP Address
- Log into either the HTTPS or SSH interface as the Crypto Officer for first time access (Default username and password: comtech, comtech)
- Change default Crypto Officer Password
- Change SMAT from the factory-default value

3.1.2 Management

The module is only capable of operating in one of two mixed modes 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 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, one label on each side. Figure 6 and Figure 7 show the required label placement (denoted by the red oval).

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

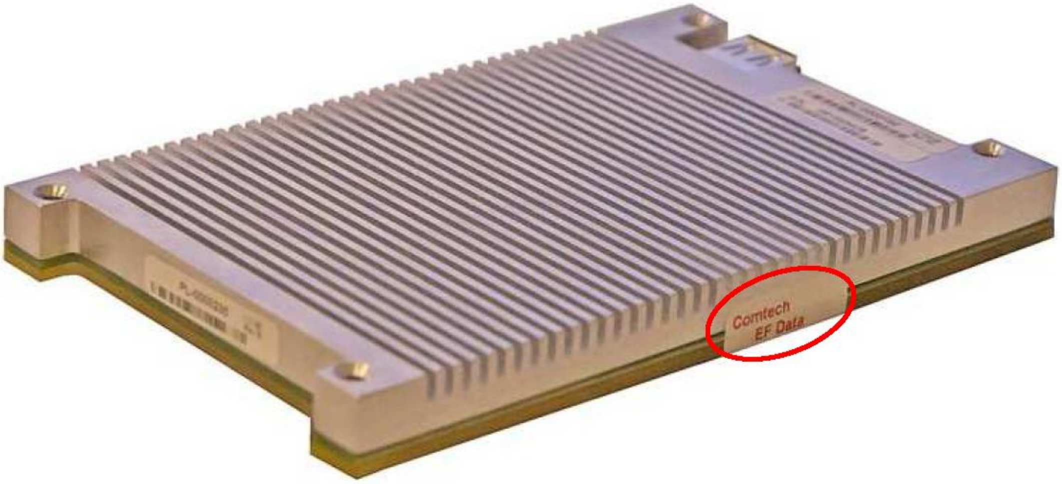

Figure 6 - Tamper-Evident Label Placement (Right Side View)

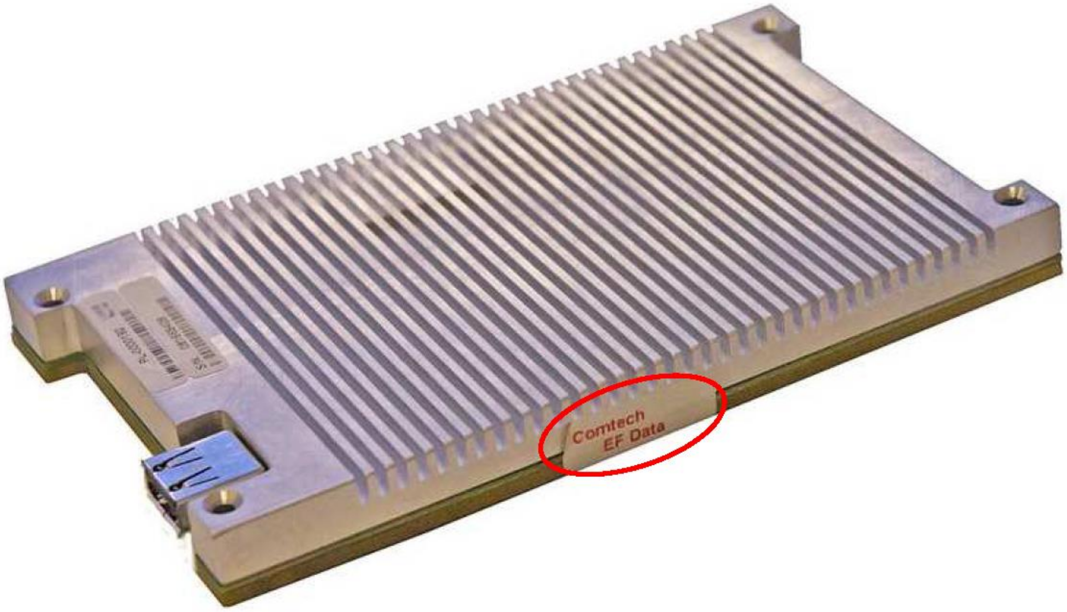

Figure 7 - Tamper-Evident Label Placement (Left Side View)

- 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 detected, the CO should remove the module from service and contact Comtech EF Data Corporation.

3.1.5 Zeroization

In both mixed modes of operation, to perform zeroization of private keys and CSPs and bring the module back to the factory default setting, the CO shall navigate to the “Configure” page via HTTPS or SSH and choose the “Zeroize All Keying Material” option. After performing the task, 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.

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Operators may also be able to initiate zeroization via the front panel of the satellite modem. When the module receives the appropriate zeroization command, it will proceed to zeroize all cryptographic secret keys and CSPs. The module shall be power cycled to complete the zeroization process. Zeroization by this method shall be performed under direct control of the operator.

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Acronyms

Table 13 defines the acronyms used throughout the Security Policy.

Table 13 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American Standards Code for Information Interchange
CBC	Cipher Block Chaining
CFR	Code of Federal Regulations
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CTR	Counter
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DES	Data Encryption Standard
EC	Elliptic Curve
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
ESD	Electrostatic Discharge
FEC	Forward Error Correction
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
GUI	Graphical User Interface
HMAC	(keyed-) Hashed Message Authentication Code
HTTPS	Hyper Text Transfer Protocol
IC	Integrated Circuit
IP	Internet Protocol
KAT	Known Answer Test
KBKDF	Key-Based Key Derivation Function
KEK	Key Encryption Key
MAC	Message Authentication Code
Mbps	Megabits per second

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

MD5	Message Digest 5
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
PCT	Pairwise Consistency Test
PRNG	Pseudo-Random Number Generator
PVCS	Polytron Version Control System
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
Rx	Receiver
SHA	Secure Hash Standard
SMAT	Shared Message Authentication Token
SSH	Secure Shell
SSL	Secure Socket Layer
TDK	TRANSEC Decryption Key
TEK	TRANSEC Encryption Key
TLS	Transport Layer Security
TRANSEC	Transmission Security
TSK	TRANSEC Key
Tx	Transmitter
USB	Universal Serial Bus

Copyright © 2017 Comtech EF Data Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.