Comtech Satellite Network Technologies, Inc.

Gen 2 TRANSEC

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.1
Date: December 27, 2022

Prepared by:

intertek acumen security

Table Of Contents

1. Introduction 3
1.1 Purpose 3
1.2 Disclaimer 3
1.3 Notices 3
2. Gen 2 TRANSEC Overview 4
2.1 Cryptographic Module Specification 4
2.1.1 Cryptographic Boundary 5
2.1.2 Mode of Operation 6
2.2 Cryptographic Module Ports and Interfaces 7
2.3 Roles, Services, and Authentication 7
2.3.1 Authorized Roles and Authentication Mechanisms 7
2.3.2 Crypto Officer Services 8
2.3.3 User Services 9
2.3.4 Unauthenticated Services 10
2.4 Physical Security 10
2.5 Operational Environment 10
2.6 Cryptographic Key Management 11
2.6.1 Key Generation 14
2.6.2 Key Entry/Output 14
2.6.3 Zeroization Procedures 14
2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) 15
2.8 Self-Tests 15
2.8.1 Power-On Self-Tests 15
2.8.2 Conditional Self-Tests 15
2.8.3 Self-Tests Error Handling 16
2.9 Mitigation of Other Attacks 16
3. Secure Operation 16
3.1 Installation and Configuration 16
3.2 Management 16
3.3 Delivery 17
3.4 Maintenance of Physical Security 17
3.5 Zeroization 17
Appendix A: Acronyms 18

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for Comtech Satellite Network Technologies, Inc. Gen 2 TRANSEC, also referred to as the "module" in this document. Below are the details of the product certified:

Hardware Version #: PL-0023315, Rev A
Firmware Version #: 1.1.1
FIPS 140-2 Security Level: 2

1.1 Purpose

This document was prepared as a Federal Information Processing Standard (FIPS) 140-2 validation process. The National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing. The CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

This document describes how the Gen 2 TRANSEC meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. The target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Comtech Satellite Network Technologies, Inc. shall have no liability for any error or damages of any kind resulting from the use of this document.

1.3 Notices

This document may be freely reproduced and distributed in its entirety without modification.

2. Gen 2 TRANSEC Overview

Comtech Satellite Network Technologies, Inc. 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 upconverters, 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 Satellite Network Technologies, Inc. is based in Arizona and operates as a subsidiary of Comtech Telecommunications Corp. (NASDAQ: CMTL)

The Gen 2 TRANSEC (the module) is a multi-chip embedded module validated at FIPS 140-2 Security Level 2. Specifically, the module meets that following security levels for individual sections in FIPS 140-2 Standard:

Table 1 - Security Level for each FIPS 140-2 Section

#	Section Title	Security 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	2
9	Self-Tests	2
10	Design Assurances	2
11	Mitigation of Other Attacks	N/A
Overall Level		2

2.1 Cryptographic Module Specification

The Gen 2 TRANSEC module is a FIPS 140-2 validated module that adds over-the-air encryption to satellite modems to protect and cover user data. It features support for both static key provisioning with AES-256 CBC encryption, as well as dynamic key exchange with AES-256 CTR encryption for STANAG 4486 ed. 3. Crypto Officers (COs) manage the module and enter keys using an HTTPS or SSH interface. Protected by an enclosure with a full-size heat spreader, the module is designed to operate over a wide range of temperatures and environmental scenarios.

2.1.1 Cryptographic Boundary

The cryptographic boundary is the physical boundary of the device. 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. The module plugs into a host modem that controls the module and provides some level of module status to the user. The CO also can connect directly to the module's encrypted management interfaces to load keys, change firmware, and view extended status information.

Figure 1 - Front View of Gen 2 TRANSEC Module

Figure 2 - Back View of Gen 2 TRANSEC Module

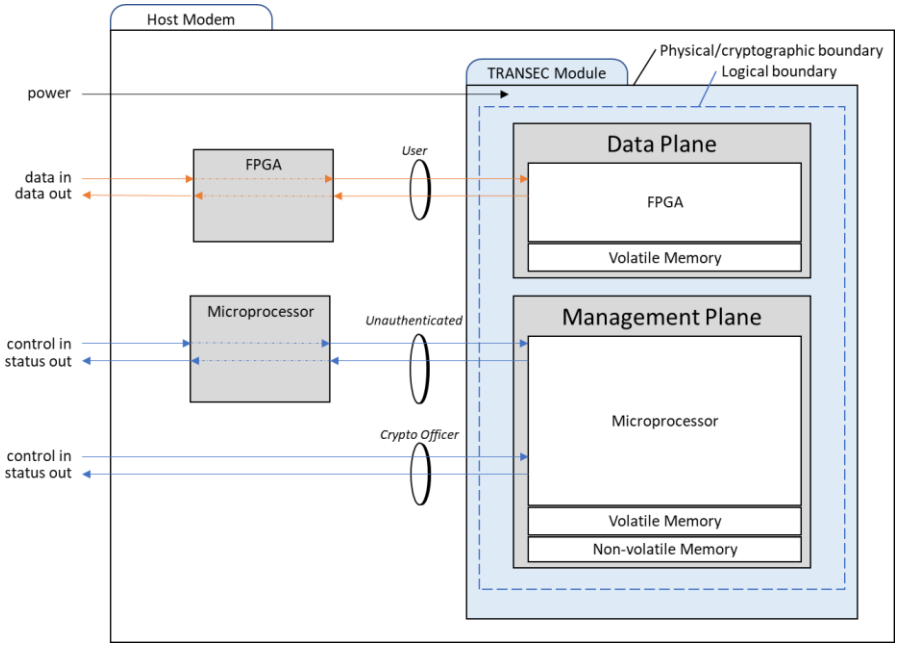

Figure 3 - Cryptographic Boundary and Interfaces

2.1.2 Mode of Operation

The module always operates in a FIPS-approved mode where it uses only allowed or approved algorithms:

Table 2 - Supported Hardware Algorithms

CAVP Cert. #	Algorithm	Modes and Sizes	Usage
A2341	AES	256-bit CBC, CTR	Traffic encryption/decryption

Table 3 - Supported Firmware Algorithms[1]

CAVP Cert. #	Algorithm	Modes and Sizes	Usage
A2340	AES	256-bit CTR 128, 192, 256-bit GCM[2]	TLS and SSH session encryption/decryption
A2340	SHS	SHA-1 SHA2-256, 384, 512	Hashing
A2340	HMAC	HMAC-SHA2-256, 512	Authentication
A2340	KAS SSC	P-521 Ephemeral Unified	Key agreement in TLS and SSH
A2340	DRBG	Counter using AES 256	Random number generation
A2344	KBKDF	Counter using HMAC-SHA2-256	Traffic key derivation in static mode
A2340	ECDSA	P-521 Signature Verification	Firmware authentication
A2340	RSA	2048, 3072-bit Key Generation	SSH host key generation
A2340	CVL	TLS KDF, SSH KDF[3]	Key derivation in TLS/SSH
A2344	KDA	One Step KDF using SHA-512	Traffic key derivation in dynamic mode
A2340	KAS[4]	P-521 Ephemeral Unified with TLS KDF or SSH KDF	Key agreement in TLS and SSH
-	ENT	SP800-90B compilant entropy source	Entropy source for DRBG
Vendor Affirmed	CKG	Seeds used for generating asymmetric keys via the direct output of the DRBG	Seed values for asymmetric key generation

[1] There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.
[2] The module supports TLS 1.2, with support for acceptable AES GCM ciphersuites from Section 3.3.1 of SP 800-52.
[3] No parts of SSH or TLS have been tested by the CAVP other than the KDF.
[4] The module obtains owner assurances of its ephemeral keypairs by generating them as specified in section 5.6.1.

2.2 Cryptographic Module Ports and Interfaces

The module has a single connector which provides the following FIPS Logical interfaces: Data Input, Data Output, Control Input, Status Output and Power Input. Table 4 below describes the mapping between the physical ports of the connector and the FIPS logical interfaces:

Table 4 - Module Interface Mapping

Connector	Physical Interface	Pin Assignment	FIPS Logical Interface
Interface Connector	Receiver (Rx) FPGA Interface	18, 24, 13, 19	Data Input
	Transmitter (Tx) FPGA Interface	6, 12, 1, 7	Data Output
M&C and General Purpose Connectors	System Clock Interface	30, 36, 102, 108	Control Input
	Mailbox Interface	37 – 46, 51 – 58	Data Input, Data Output, Control Input, Status Output
	Power Interface	61 – 63, 78, 94, 95, 100, 101	Power Input
	General Purpose Interface	85, 91, 25, 33, 96, 97, 79, 47 – 50, 109, 115, 114, 120, 60	Data Input, Data Output, Control Input, Status Output

2.3 Roles, Services, and Authentication

The following sections provide details about roles supported by the module, how these roles are authenticated and the services the roles are authorized to access.

2.3.1 Authorized Roles and Authentication Mechanisms

The module supports both a CO and User role. The host modem can perform non-crypto-related configuration via an unauthenticated role. Roles are selected implicitly.

Table 5 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Crypto Officer	Password	The CO is authenticated using a password that is from 7 through 25 ASCII characters long. Since there are 95 printable ASCII characters, the likelihood a single, random authentication attempt succeeds is 1/95^7. The module can process less than 350 authentication attempts per minute, so the likelihood a random authentication attempt succeeds within a one-minute period is 350/95^7.

User	Password	The host modem authenticates as the User role with a 16-byte password. the likelihood a single, random authentication attempt succeeds is 1/2^128. Any failed authentication attempt results in the module zeroizing all keys. Since multiple unsuccessful attempts are not permitted, the likelihood a random authentication attempt succeeds within a one-minute period is 1/2^128.
Unauthenticated	None	The host modem uses a non-authenticated interface to control the module and read status.

2.3.2 Crypto Officer Services

The following services are allocated to the CO.

Table 6 – Crypto Officer Services

Service	Description	Key/CSP and Type of Access
Initialize Module	Initialize and install the TRANSEC module	User Password - G
Configure Module	Allows the operator to configure security-sensitive parameters	TLS Host Keypair – W SSH Host Key Pair – G Current/Future Seed Key – W Current/Future Passphrase – W SMAT - W Crypto Officer Password – W/X TEK and TDK – W
Configure Network Parameters	Allows the operator to configure network parameters of the module	None
Configure Crypto Officer Credential Parameters	Allows the operator to configure Crypto Officer credential parameters of the module	Crypto Officer Password – W
Create Secure Web Management Session (Web GUI)	Access the module using TLS protocol	Crypto Officer Password – X DRBG State – W/X TLS Host Key pair – X TLS Ephemeral Keypair – G/X TLS Premaster Secret – G/X TLS Master Secret – G/X TLS Session Keys –G/X
Create Secure CLI Management Session (SSH)	Access the module using SSH protocol	Crypto Officer Password – X SSH Host Key Pair –X SSH Ephemeral Keypair – G/X

Service	Description	Key/CSP and Type of Access
		SSH Session Keys – G/X
Set Current/Future Seed Key (Static Key mode)	Set the Current and Future Seed Key CSPs via SSH or HTTPS	SSH Session Keys – X TLS Session keys – X Current/Future Seed key – W/X
Set Current/Future Passphrase (Static Key mode)	Set the Current/Future Passphrase via HTTPS or SSH	SSH Session Keys – X TLS Session keys – X Current/Future Passphrase – W/X
Set SMAT (Dynamic Key mode)	Set the STANAG 4486 SMAT for authentication of ECDH key exchange messages via HTTPS or SSH	SSH Session Keys – X TLS Session keys – X SMAT – W
Firmware Upgrade (via TLS)*	Configure firmware upgrade parameters of the module	SSH Session Keys – X TLS Session keys – X Upgrade Verification Key –X/W
Event Log Parameters	Check the event log parameters of the module	SSH Session Keys – X TLS Session keys – X
Cryptographic module status	Check the health and operational status of the 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 – Z

R – Read, W – Write, G – Generate, X – Execute, Z – Zeroize

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

2.3.3 User Services

The following services are allocated to the User.

Table 7 – User Services

Service	Description	Key/CSP and Type of Access
User Authenticate	Authenticate the user	User Password – X
Encryption/decryption	Perform encryption and/or decryption of data	TEK – X TDK – X
Key Agreement	Key exchange and key agreement for remote session establishment	Ephemeral ECDH Key Pair – G/X Dynamic Mode Shared Secret –

		G/X SMAT – X
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

R – Read, W – Write, G – Generate, X – Execute, Z – Zeroize

2.3.4 Unauthenticated Services

The following services are available without authentication.

Table 8 – Unauthenticated Services

Service	Description	Key/CSP and Type of Access
Zeroization	Zeroize all the cryptographic keys and key components	All keys and CSPs – Z
Reboot	Initiate a soft reboot of the module.	None
Configure Static vs Dynamic Mode	Configure whether the module should run in static or dynamic mode.	None

R – Read, W – Write, G – Generate, X – Execute, Z – Zeroize

2.4 Physical Security

The module is classified as multi-chip embedded. It is protected by an opaque cover. The top and sides of the cover are metal, and the bottom of the cover is a hard plastic. Removal of the cover is protected by tamper-evident seals. The seals come pre-installed from the factory. If signs of tampering are detected, the module must be returned to the vendor.

It is the CO'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.

2.5 Operational Environment

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

2.6 Cryptographic Key Management

Table 9 - Details of Cryptographic Keys and CSPs

Key/CSP	Type	Generation/Input	Output	Storage	Zeroization	Usage
Current/Future Seed key	KDF seed key for SP800-108 KBKDF (HMAC-SHA-256)	Over SSH/HTTPS	N/A	Plaintext in flash	Overwrite with default key	Static key generation
Current/Future Passphrase	KDF Parameter for SP800-108 KBKDF (HMAC-SHA-256)	Over SSH/HTTPS	N/A	Plaintext in flash	Overwrite with default key	Static key generation
SMAT	HMAC-SHA2-256, 512	Over SSH/HTTPS	N/A	Plaintext in flash	Overwrite with default key	Authenticate ECDH key exchange
Crypto Officer Password	Password	Over SSH/HTTPS	N/A	Plaintext in flash	Overwrite with default	Crypto Officer login
User Password	Password	Generated randomly as the direct output of the DRBG	Plaintext during initialization (MD/EE)	Plaintext in flash	Delete	User login
Entropy Input	Entropy from ENT (P)	Generated by the SP800-90B ENT (P) source.	N/A	Plaintext in volatile memory	Power-cycle	Entropy input used to seed for DRBG

Key/CSP	Type	Generation/Input	Output	Storage	Zeroization	Usage
DRBG State (key, V)	SP800-90A Counter DRBG (AES 256)	Generated internally per SP800-90A	N/A	Plaintext in volatile memory	Power-cycle	Internal state for SP800-90A DRBG
SSH Host Key Pair	RSA 2048, 3072 (112 and 128 bits of strength)	Generated randomly per B.3.3	Private key - N/A Public key - Output in plaintext	Plaintext in flash	Delete and optionally overwrite with new key	SSH session establishment
SSH Ephemeral Keypair	KAS ECC P-521 ephemeral keypair (256 bits of strength)	Generated randomly using testing candidates	Private key – N/A Public Key – Output in plaintext	Plaintext in volatile memory	Power-cycle	Ephemeral key used for KAS ECC
SSH Session Keys	AES 256, HMAC-SHA2-256, 384	SSH Session	N/A	Plaintext in volatile memory	Power-cycle	SSH session encryption and authentication
TLS Host Key pair (HTTPS server private key and certificate)	RSA 2048 (112 and 128 bits of strength)	Loaded by operator	Private key – N/A Public Key/Certificate – Output in plaintext	Plaintext in flash	Overwrite with default key	TLS session establishment
TLS Ephemeral Keypair	KAS ECC P-521 ephemeral keypair (256 bits of strength)	Generated randomly using testing candidates	Private key – N/A Public Key – Output in plaintext	Plaintext in volatile memory	Power-cycle	Ephemeral key used for KAS ECC

Key/CSP	Type	Generation/Input	Output	Storage	Zeroization	Usage
TLS Premaster Secret	KAS ECC (P-521) shared secret	KAS ECC shared secret	N/A	Plaintext in volatile memory	Power-cycle	Premaster Secret used in TLS.
TLS Master Secret	TLS KDF 1.2	TLS KDF	N/A	Plaintext in volatile memory	Power-cycle	Premaster Secret used in TLS.
TLS Session Keys	AES GCM 128, 192, 256	TLS Session	N/A	Plaintext in volatile memory	Power-cycle	TLS session encryption and authentication
Ephemeral ECDH Key Pair	KAS ECC P-521 ephemeral keypair (256 bits of strength)	Generated Internally	Private key – N/A Public Key – Output in plaintext	Plaintext in volatile memory	Power-cycle	Ephemeral ECDH keypair for STANAG 4486 key exchange
Dynamic Mode Shared Secret	KAS ECC (P-521) Shared Secret	KAS ECC shared secret	N/A	Plaintext in volatile memory	Power-cycle	Shared secret for STANAG 4486 key exchange
Traffic Encryption Key (TEK)	AES 256	Static mode: Derived from Current/Future Seed key via SP 800-108 Dynamic mode: Derived from Dynamic Mode Shared Secret via NIST SP 800-56C one-step KDF.	N/A	Plaintext in volatile memory	Power-cycle	Traffic data encryption

Key/CSP	Type	Generation/Input	Output	Storage	Zeroization	Usage
Traffic Decryption Key (TDK)	AES 256	Static mode: Derived from Current/Future Seed key via SP 800-108 Dynamic mode: Derived from Dynamic Mode Shared Secret via NIST SP 800-56C one-step KDF.	N/A	Plaintext in volatile memory	Power-cycle	Traffic data decryption
Upgrade Verification Key	ECDSA P-521 (256 bits of strength)	Input in plaintext embedded in the firmware image	N/A	Plaintext in flash	N/A	Authenticate firmware updates

2.6.1 Key Generation

Keys are generated in compliance to SP 800-133 using the module's approved DRBG. The DRBG is seeded with a minimum of 4096-bytes of entropy. RSA keys are generated per FIPS 186-4 and ECDH ephemeral keypairs are generated per SP 800-56A revision 3.

2.6.2 Key Entry/Output

Keys that can be input into the module are input by the CO over SSH and/or TLS. Only RSA public keys are output. The Crypto Officer can optionally view the SMAT.

2.6.3 Zeroization Procedures

All keys can be zeroized by executing the zeroize service, and then power cycling the module.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The Gen 2 TRANSEC Module was tested and found to be in conformance with the Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) requirements specified by the 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 the SLM-5650B Satellite Modem.

2.8 Self-Tests

All power-on self-tests are run automatically, without operator intervention.

2.8.1 Power-On Self-Tests

The module implements the following power-on self-tests:

Firmware integrity test:

- 32-bit CRC

FPGA algorithm tests:

- FPGA AES-256 CBC encrypt and decrypt KAT
- FPGA AES-256 CTR encrypt and decrypt KAT

Firmware algorithm tests:

- AES GCM 256 encrypt and decrypt KAT
- RSA 2048 PKCS 1.5 signature generation and verification KAT
- ECDSA P-521 with SHA-256 signature verification test
- KAS ECC P-521 primitive 'Z' computation KAT
- CTR DRBG AES 256 Instantiate, Generate, Reseed KAT (SP 800-90A)
- SP 800-90B RCT and APT Test
- HMAC SHA-256, -512 KAT
- SHA-1, SHA2-256, -512 KAT
- KBKDF HMAC-SHA2-256 KAT (SP 800-108)
- SP 800-56C using SHA2-512 KDF KAT
- TLS KDF KAT
- SSH KDF KAT

2.8.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- SP 800-90A Conditional Self-Test
- SP 800-90B APT and RCT Health Tests
- RSA Sign/Verify PCT
- Firmware update ECDSA P-521 with SHA-256 signature verification

2.8.3 Self-Tests Error Handling

If a power-on self-test fails, the module enters an error state which outputs an error message, logs the event and zeroizes all keys.

2.9 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 Gen 2 TRANSEC Module meets Level 2 requirements for FIPS 140-2. The Crypto Officer is responsible for initializing and managing the module.

3.1 Installation and Configuration

The module is installed into a host modem in the factory. If a field replacement is necessary, the following steps outline the installation procedure:

Installation

- Equip Electrostatic Discharge (ESD) protection
- Turn off host modem and disconnect power cable
- Remove access cover of the host modem
- Install TRANSEC module by plugging in the interface and securing with screws
- Replace the access cover of the satellite modem

Once the TRANSEC Module is properly installed, the CO shall complete the following steps to configure the module for operation:

Configuration

- Configure module IP Address using host modem's user interface
- Log into the HTTPS interface as the Crypto Officer for first time access (Default username and password: comtech, comtech)
- Change default Crypto Officer Password
- Provision module with a trusted TLS server key and a CA-signed certificate
- For Static Key mode: Enter the initial Current/Future Seed Key and Current/Future Passphrase to generate TEKs and TDKs
- For Dynamic Key mode: Enter the SMAT

3.2 Management

The Crypto Officer can monitor and configure the module via the web GUI (HTTPS over TLS) and SSH.

3.3 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 Satellite Network Technologies, Inc.

3.4 Maintenance of 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 Satellite Network Technologies, Inc. prior to delivery. However, it is the CO'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 (one label on each side) to be placed on it to meet FIPS requirements. Figures 2 and 3 show the required label placement.

- The CO must periodically visually inspect the module 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 Satellite Network Technologies, Inc.

3.5 Zeroization

In order to perform zeroization of secret keys, 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 used by the module.

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

Appendix A: Acronyms

This section describes the acronyms used throughout the document, and those that are commonly used in satellite communications.

Table 10 - 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

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
Tx	Transmitter
USB	Universal Serial Bus