

Hughes Network Systems, LLC

HT Satellite Terminals

Hardware Version: HT2300, HT2500, HT2550, HT2650

Firmware Version: 7.4.1.19

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 1.4

Prepared for:

HUGHES

Hughes Network Systems, LLC
11717 Exploration Lane
Germantown, MD 20876
United States of America

Phone: +1 301 428 5500
www.hughes.com/

Prepared by:



Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

- 1. Introduction4**
 - 1.1 Purpose.....4
 - 1.2 References.....4
 - 1.3 Document Organization4
- 2. Hughes HT Satellite Terminals5**
 - 2.1 Overview.....5
 - 2.2 Module Specification.....7
 - 2.2.1 Modes of Operation 10
 - 2.3 Module Interfaces 10
 - 2.4 Roles, Services, and Authentication 11
 - 2.4.1 Authorized Roles 12
 - 2.4.2 Operator Services 12
 - 2.4.3 Additional Services 14
 - 2.4.4 Non-Approved Services 15
 - 2.4.5 Authentication..... 15
 - 2.5 Physical Security 16
 - 2.6 Operational Environment..... 16
 - 2.7 Cryptographic Key Management..... 17
 - 2.8 EMI / EMC..... 20
 - 2.9 Self-Tests 20
 - 2.9.1 Power-Up Self-Tests 20
 - 2.9.2 Conditional Self-Tests..... 20
 - 2.9.3 Critical Function Self-Tests 21
 - 2.9.4 Self-Test Failures 21
 - 2.10 Mitigation of Other Attacks..... 21
- 3. Secure Operation22**
 - 3.1 Installation and Setup..... 22
 - 3.1.1 Initial Tamper-Evident Label Inspection..... 22
 - 3.1.2 Initial Setup and Configuration..... 25
 - 3.2 Crypto Officer Guidance 25
 - 3.2.1 Management 26
 - 3.2.2 Load IPsec Key Files..... 26
 - 3.2.3 On-Demand Self-Tests..... 26
 - 3.2.4 Zeroization..... 26
 - 3.2.5 Decommission 26
 - 3.2.6 Monitoring Status..... 27
 - 3.3 User Guidance 27
 - 3.4 Additional Guidance and Usage Policies 27
- 4. Appendix28**
 - 4.1 Acronyms..... 28

List of Tables

Table 1 – Security Level per FIPS 140-2 Section6

Table 2 – Cryptographic Algorithm Providers7

Table 3 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal OpenSSL Crypto Library 1.0)7

Table 4 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal SWP Hardware Crypto Library 1.0)8

Table 5 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal UPP Hardware Crypto Library 1.0)9

Table 6 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal DPP Hardware Crypto Library 1.0)9

Table 7 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal IKEv2 Protocol Library 1.0)9

Table 8 – Allowed Algorithm Implementations.....9

Table 9 – FIPS 140-2 Logical Interface Mappings 10

Table 10 – LEDs and Status Indications 11

Table 11 – Mapping of Authenticated Module Services to Roles, CSPs, and Type of Access 12

Table 12 – Mapping of Unauthenticated Module Services to Roles, CSPs, and Type of Access 13

Table 13 – Additional Services..... 14

Table 14 – Non-Approved Services 15

Table 15 – Cryptographic Keys, Cryptographic Key Components, and CSPs..... 17

Table 16 – Acronyms 28

List of Figures

Figure 1 – Terminals within the Jupiter System5

Figure 2 – Back View of the HT2300..... 23

Figure 3 – Bottom view of the HT2300..... 23

Figure 4 – Top View of the HT2500/HT2550 24

Figure 5 - Bottom right view of HT2650 24

Figure 6 - Bottom left view of HT2650 25

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HT Satellite Terminals from Hughes Network Systems, LLC, hereafter referred to as “Hughes”. This Security Policy describes how the HT Satellite Terminals meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.¹ and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at <http://csrc.nist.gov/groups/STM/cmvp>.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The HT Satellite Terminals are referred to collectively in this document as Terminals, crypto 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 Hughes website (<https://www.Hughes.com>) contains information on the full line of products from Hughes.
- The search page on the CMVP website (<https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search>) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

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

¹ U.S. – United States

2. Hughes HT Satellite Terminals

2.1 Overview

Hughes is a global leader in broadband satellite technology and managed network services for home and office. Hughes’ broadband satellite systems enable operators and enterprises to deliver a comprehensive range of services including broadband Internet access, cellular backhaul, communications on the move, and VoIP² telephony.

The Hughes’ Jupiter System is a broadband satellite system designed to support high-throughput satellite communications and offers a range of operations for optimized traffic capacity, terminal performance, gateway (GW) design, and network management. It consists of satellite terminals, single rack or multi rack Jupiter GWs (facilities used to host the equipment providing uplink and downlink connectivity to the satellite), and the capabilities to manage these devices over the network.

The Hughes Terminals is the indoor unit (IU), which connects the client workstation to the outdoor unit (ODU) over an inter-facility link (IFL). **Figure 1** below shows the Terminals integration within the Hughes Jupiter System.

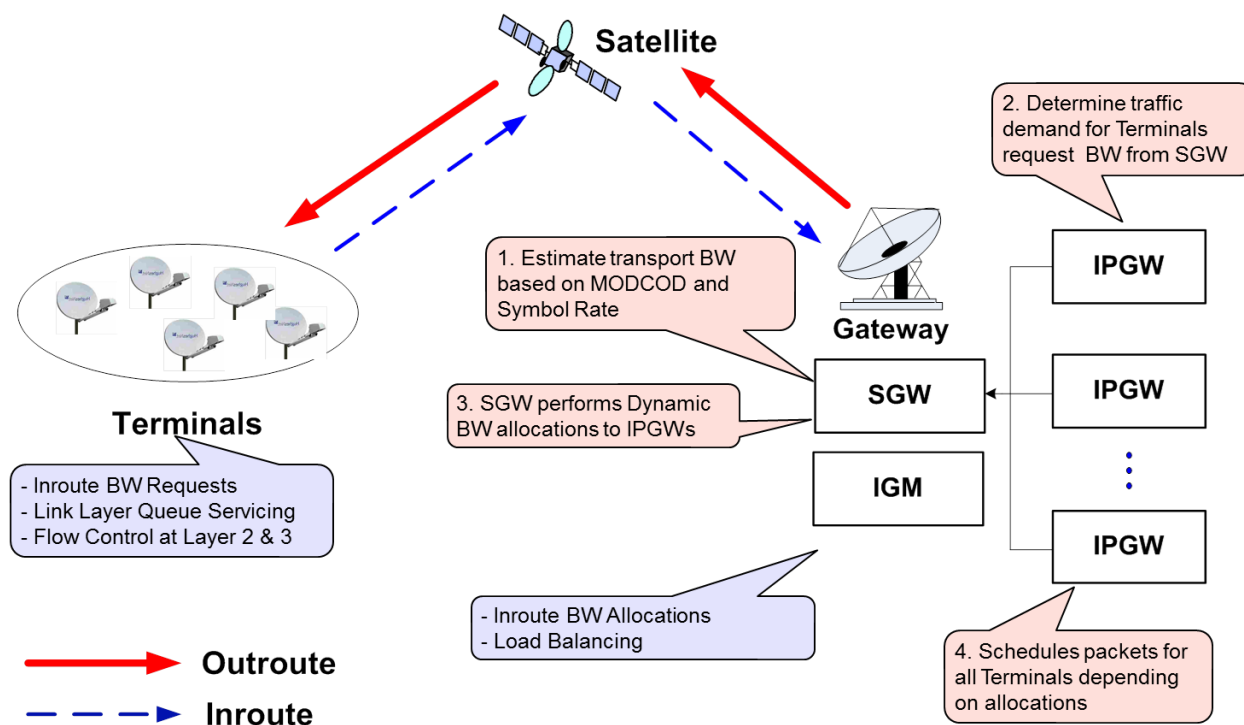


Figure 1 – Terminals within the Jupiter System

The Hughes Terminals FIPS 140-2 validation focuses on the following Terminals models:

² VoIP – Voice Over Internet Protocol

- HT2300 – desktop chassis
- HT2500 – 1U rack mount server
- HT2550 – 1U rack mount server
- HT2650 – rugged outdoor chassis

Even though they vary in form factor, each model offers the following market-leading, next-generation functions:

- Forward channel wideband DVB-S2X³ support
- Return channel Low Density Parity Coding (LDPC) with Adaptive In-route Selection (AIS)
- Provides 200 Mbps⁴ throughput support

The Terminals provide an embedded web-based GUI⁵. The GUI provides easy accessibility for quick and reliable installation, status monitoring, troubleshooting, and diagnostics.

The Terminals firmware supports control plane and data plane cryptography through the Hughes OpenSSL Crypto Library, which is based on the OpenSSL FOM⁶ 2.0.16 (with OpenSSL 1.0.1p). Random number generation is provided by a hash based DRBG, which receives entropy from an SP800-90B compliant entropy source. The module supports SNMP and IKE through protocol-specific cryptographic libraries. An Acadia ASIC⁷ provides AES-NI encryption acceleration.

The Terminals cryptographic module is validated at the FIPS 140-2 Section levels shown in Table 1.

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 ⁸ |
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC ⁹ | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

³ DVB-S2X – Digital Video Broadcasting – Satellite – Second Generation (Extension)

⁴ Mbps – Megabits per second

⁵ GUI – Graphical User Interface

⁶ FOM – FIPS Object Module

⁷ ASIC – Application Specific Integrated Circuit

⁸ N/A – Not Applicable

⁹ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The Terminals are hardware modules with a multiple-chip standalone embodiment. The overall security level of the module is 2. The cryptographic boundary is defined by the physical enclosure of each of the Terminals and includes all internal hardware as well as the v7.4.1.19 application firmware. The module includes an Acadia ASIC with an ARM Cortex-A9 Quad Core 720 MHz¹⁰ processor.

The module includes the cryptographic algorithm providers listed in Table 2 below.

Table 2 – Cryptographic Algorithm Providers

| Certificate Number | Implementation Name and Version | Use |
|--------------------|--|---|
| A1460 | Hughes HT Satellite Terminal OpenSSL Crypto Library 1.0 | Firmware-based cryptographic primitives (based on OpenSSL FOM 2.0.16 with OpenSSL 1.0.2S) |
| A1437 | Hughes HT Satellite Terminal SWP Hardware Crypto Library 1.0 | Hardware-based cryptographic primitives |
| A1435 | Hughes HT Satellite Terminal UPP Hardware Crypto Library 1.0 | Hardware-based cryptographic primitives |
| A1436 | Hughes HT Satellite Terminal DPP Hardware Crypto Library 1.0 | Hardware-based cryptographic primitives |
| A1461 | Hughes HT Satellite Terminal IKEv2 Protocol Library 1.0 | IKE KDF (based on a Hughes proprietary IKE library) |

The FIPS-Approved algorithms listed in Table 3 are implemented in the Hughes Terminals OpenSSL Crypto Library.

Table 3 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal OpenSSL Crypto Library 1.0)

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|------------------------|---------------------|---------------------------------------|-------------------------------|---|
| A1460 | AES ¹¹ | FIPS PUB 197 | CBC ¹² , CTR ¹³ | 128, 256 | Encryption/decryption |
| Vendor Affirmed | CKG ¹⁴ | NIST SP 800-133rev2 | - | - | Cryptographic key generation |
| A1460 | DRBG ¹⁵ | NIST SP 800-90Arev1 | Hash-based | SHA ¹⁶ -256 | Deterministic random bit generation |
| A1460 | DSA ¹⁷ | FIPS PUB 186-4 | PKCS ¹⁸ v1.5 | 2048 (SHA2-256) | Digital signature verification |
| N/A | ENT (NP) ¹⁹ | NIST SP 800-90B | - | - | Non-deterministic random bit generation |
| A1460 | HMAC ²⁰ | FIPS PUB 198-1 | SHA-1, SHA2-256-128, SHA2-256 | - | Message authentication |

¹⁰ MHz – Mega Hertz

¹¹ AES – Advanced Encryption Standard

¹² CBC – Cipher Blocker Chaining

¹³ CTR – Counter

¹⁴ CKG – Cryptographic Key Generation

¹⁵ DRBG – Deterministic Random Bit Generator

¹⁶ SHA – Secure Hash Algorithm

¹⁷ DSA – Digital Signature Algorithm

¹⁸ PKCS – Public Key Cryptography Standard

¹⁹ ENT - Entropy

²⁰ HMAC – (keyed-) Hashed Message Authentication Code

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|----------------------------|---------------------|--|---|--|
| A1460 | KAS-SSC ²¹ | NIST SP 800-56Arev3 | FFC ²² DH ²³ Primitive | Key establishment methodology provides 112 or 150 bits of encryption strength (MODP-2048 and MODP-4096) | Shared secret computation |
| A1460 | RSA ²⁴ | FIPS PUB 186-4 | PKCS v1.5 SigGen | 2048 (SHA2-256) | Digital signature generation |
| | | | PKCS v1.5 SigVer | 2048 (SHA2-256) | Digital signature verification |
| A1460 | Safe Primes Key Generation | NIST SP 800-56Arev3 | Safe Prime Groups: MODP-2048 MODP-4096 | 2048, 4096 | Diffie-Hellman key agreement |
| A1460 | SHS ²⁵ | FIPS PUB 180-4 | SHA2-256-128, SHA2-256 | - | Message digest <i>The cryptographic library supports the truncation of HMAC SHA-2 to 128 bits according to NIST SP 800-107rev1.</i> |

The module includes the following vendor-affirmed security methods in the Hughes Terminals OpenSSL Crypto Library v1.0:

- Cryptographic key generation** – As per NIST SP 800-133rev2, the module uses the FIPS-Approved Hash-based DRBG specified in NIST SP 800-90Arev1 to generate random seeds. The resulting generated seeds are unmodified output from the DRBG. According FIPS 140-2 Implementation Guidance D.12, a component key generation (CKG) using the unmodified output of an approved DRBG can be used to generate seed for the asymmetric key generation. This method is valid per option 1 from section "4. Using the Output of a Random Bit Generator" of FIPS SP 800-133rev2. Based on Additional Comments #1 of FIPS IG D.12, this statement is enough and it is not necessary that the vendor justifies the equivalency between this operation and XORing U and V with V as a string of zeros.

The FIPS-Approved algorithms listed in Table 4, Table 5, and Table 6 below are implemented in the module hardware.

Table 4 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal SWP Hardware Crypto Library 1.0)

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|-----------|----------------|---------------|-------------------------------|------------------------|
| A1437 | AES | FIPS PUB 197 | CBC | 256 | Encryption/decryption |
| A1437 | HMAC | FIPS PUB 198-1 | SHA2-256 | - | Message authentication |

²¹ KAS-SSC – Key Agreement Scheme Shared Secret Computation

²² FFC – Finite Field Cryptography

²³ DH – Diffie-Hellman

²⁴ RSA – Rivest Shamir Adleman

²⁵ SHS – Secure Hash Standard

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|-----------|----------------|---------------|-------------------------------|----------------|
| A1437 | SHS | FIPS PUB 180-4 | SHA2-256 | - | Message digest |

Table 5 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal UPP Hardware Crypto Library 1.0)

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|-----------|--------------|-------------------|-------------------------------|-----------------------|
| A1435 | AES | FIPS PUB 197 | CTR ²⁶ | 256 | Encryption/decryption |

Table 6 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal DPP Hardware Crypto Library 1.0)

| Certificate Number | Algorithm | Standard | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|-----------|--------------|---------------|-------------------------------|-----------------------|
| A1436 | AES | FIPS PUB 197 | CTR | 256 | Encryption/decryption |

The FIPS-Approved algorithms listed in Table 7 below are implemented in the Hughes Terminals IKEv2 Protocol Crypto Library.

Table 7 – Algorithm Certificate Numbers (Hughes HT Satellite Terminal IKEv2 Protocol Library 1.0)

| Certificate Number | Algorithm | Specification | Mode / Method | Key Lengths / Curves / Moduli | Use |
|--------------------|-----------|---------------------|---------------|-------------------------------|--|
| A1461 | CVL | NIST SP 800-135rev1 | IKEv2 | - | Key derivation function <i>No parts of the IKE protocol, other than the KDFs, have been tested by the CAVP or CMVP.</i> |

The algorithm implementations shown in Table 8 below are allowed for use in a FIPS-Approved mode of operation:

Table 8 – Allowed Algorithm Implementations

| Algorithm | Caveat | Use |
|---------------------------------|--------|----------------|
| AES ²⁷ (Cert. A1437) | - | Key unwrapping |

The module implements the non-Approved algorithms listed below (these algorithms shall not be used in the Approved mode of operation):

- SNMPv2²⁸ KDF (non-compliant)

²⁶ CTR - Counter

²⁷ MD5 – Message Digest

²⁸ SNMP – Simple Network Management Protocol

2.2.1 Modes of Operation

The module supports two modes of operation: Approved and Non-approved. The module will be in FIPS-Approved mode when all power up self-tests have completed successfully, and only Approved or Allowed algorithms are invoked. See Table 3, Table 4, Table 5, Table 6, and Table 7 for a list of the Approved and Allowed algorithms.

The module can alternate service-by-service between Approved and non-Approved modes of operation. The module will switch to the non-Approved mode upon execution of a non-Approved service. The module will switch back to the Approved mode upon execution of an Approved service.

The services available in the non-Approved mode of operation are listed in section 2.4 below.

2.3 Module Interfaces

The module’s design separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

The cryptographic boundary is defined as the outer casing of the Terminals. The physical access points on the appliance are the interfaces for the module. Table 9 below specifies the physical ports and manual controls employed by the module and provides a mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2.

Table 9 – FIPS 140-2 Logical Interface Mappings

| Physical Port/Interface | Quantity | | | Description | FIPS 140-2 Logical Interface |
|-------------------------|----------|-------------------|--------|--|---|
| | HT2300 | HT2500/ HT2550 | HT2650 | | |
| Satellite In | 1 | 1 | 1 | F-Type coaxial connector | • Data Input |
| Satellite Out | 1 | 1 | 1 | F-Type coaxial connector | • Data Output |
| Ethernet Port | 4 | 4 | 2 | 10/100/1000Base-T RJ-45 Ethernet LAN ²⁹ port | • Data Input • Data Output • Control In • Status Out |
| Power Connector | 1 | 1 | 1 | HT2300 – 4-pin Molex Connector HT2500/HT2550 – 3-pin Molex Connector HT2650 – XLR 3-pin DC Power Cable | • Power supply |
| Reset/Rescue Button | 1 | 1 | 1 | Button to turn power to the modem on/off | • Control Input |

²⁹ LAN – Local Area Network

The HT2300, HT2500 and 2550 models have a USB³⁰ port and the HT2500, HT2550 and HT2650 have a NMEA port. The USB port is not in use while the NMEA port provides GPS location data and is not security-relevant. All data input and output are inhibited through these ports. The HT2500 and HT2550 models have a console port that are not used in the evaluated configuration.

The module uses LEDs³¹ to provide status indications for the state and health of the modem. Table 10 below lists each LED and its meaning.

NOTE: The LEDs and their meaning are the same for all modems being validated.

Table 10 – LEDs and Status Indications

| LED Type | Description | FIPS 140-2 Logical Interface |
|------------------|--|------------------------------|
| Ethernet LAN LED | <ul style="list-style-type: none"> • OFF: no connection • ON: modem is connected to a computer network card or Ethernet • BLINKING: transmitting and/or receiving data | Status output |
| Transmit LED | <ul style="list-style-type: none"> • OFF: condition preventing transmission • ON: transmit path is operational • BLINKING – FAST: transmitting data • BLINKING – SLOW: the terminal is measuring the distance to the satellite to calibrate transmit timing and transmit power | Status output |
| Receiver LED | <ul style="list-style-type: none"> • OFF: condition preventing receipt of data • ON: receive path is operational • BLINKING: receiving data | Status output |
| System LED | <ul style="list-style-type: none"> • OFF: condition preventing full operation • ON: connection established • BLINKING: error state | Status output |
| Power supply LED | <ul style="list-style-type: none"> • OFF: no power • ON – BLUE (HT2300), WHITE (HT2500/HT2550): power is on and the terminal is functioning normally • ON – RED: error condition • BLINKING: operating with fallback-bin (backup) version of software | Status output |

2.4 Roles, Services, and Authentication

The sections below describe the module’s roles and services and define any authentication methods employed.

³⁰ USB – Universal Serial Bus

³¹ LED – Light Emitting Diode

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two roles that operators may assume: Crypto Officer (CO) role and User role. The CO role has access to all module services, while the User has access to a subset of services. Operators implicitly assume the CO and User roles upon invocation of the services specified in tables 10 or 11 below, note that the services in table 10 require authentication in order for the operator to invoke. The module supports multiple concurrent operators.

2.4.2 Operator Services

Descriptions of the services available to the CO role and User role are provided in Table 11 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, or modified.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.
- Z – Zeroize: The CSP is zeroized.

Table 10 below specifies the services which require authentication to the module.

Table 11 – Mapping of Authenticated Module Services to Roles, CSPs, and Type of Access

| Service | Operator | | Description | Input | Output | CSP and Type of Access |
|------------------------|----------|------|--|------------------------|------------------|--|
| | CO | User | | | | |
| Load Firmware | ✓ | ✓ | Load new firmware into the module while in a FIPS-approved mode of operation | Command and parameters | Status Output | Firmware Verification Key – R/X NMS-Terminal SDL Protocol – R/X |
| Upload SBC Config file | ✓ | | Upload new or replacement SBC Config file | Command and parameters | Command response | SBC Config file Verification Key – R/X NMS-Terminal SDL Protocol – R/X |
| Decommission | ✓ | ✓ | Decommissions the module | Command | Command response | All ephemeral keys – Z IKE/IPsec Authentication Certificate - Z IKE/IPsec Authentication RSA Private Key – Z |

| Service | Operator | | Description | Input | Output | CSP and Type of Access |
|---------|----------|------|-----------------------|---------|------------------|---|
| | CO | User | | | | |
| Zeroize | ✓ | ✓ | Zeroize keys and CSPs | Command | Command response | All ephemeral keys – Z IKE/IPsec Authentication CA Certificate – Z IKE/IPsec Authentication Certificate – Z IKE/IPsec Authentication RSA Private Key – Z |

Table 11 below specifies the services which do not require authentication to the module.

Table 12 – Mapping of Unauthenticated Module Services to Roles, CSPs, and Type of Access

| Service | Operator | | Description | Input | Output | CSP and Type of Access |
|------------------------------------|----------|------|---|------------------------|------------------|---|
| | CO | User | | | | |
| Decrypt keys | ✓ | ✓ | Decrypt effective master key; decrypt session keys | Command | Status output | TMK ³² – R/X EEMK ³³ – R/X EMK ³⁴ – W/R/X EUSK ³⁵ – R/X USK ³⁶ – W EMSK ³⁷ – R/X MSK ³⁸ – W EISK ³⁹ – R/X ISK ⁴⁰ – W |
| Perform terminal key request | ✓ | | Request updated session keys from the KMS ⁴¹ | Command | Command response | EMK – R/X EUSK ⁴² – R/X USK ⁴³ – W EMSK ⁴⁴ – R/X MSK ⁴⁵ – W EISK ⁴⁶ – R/X ISK ⁴⁷ – W |
| Encrypt/decrypt link layer traffic | ✓ | ✓ | Secure unicast, multi-cast, and in-route traffic | Command and parameters | Command response | USK – R/X MSK – R/X ISK – R/X |

³² TMK – Terminal Master Key
³³ EEMK – Encrypted Effective Master Key
³⁴ EMK – Effective Master Key
³⁵ EUSK – Encrypted Unicast Session Key
³⁶ USK – Unicast Session Key
³⁷ EMSK – Encrypted Multicast Session Key
³⁸ MSK – Multicast Session Key
³⁹ EISK – Encrypted In-route Session Key
⁴⁰ ISK – In-route Session Key
⁴¹ KMS – Key Management Server
⁴² EUSK – Encrypted Unicast Session Key
⁴³ USK – Unicast Session Key
⁴⁴ EMSK – Encrypted Multicast Session Key
⁴⁵ MSK – Multicast Session Key
⁴⁶ EISK – Encrypted In-route Session Key
⁴⁷ ISK – In-route Session Key

| Service | Operator | | Description | Input | Output | CSP and Type of Access |
|------------------------------|----------|------|---|------------------------|------------------|--|
| | CO | User | | | | |
| Establish IKE/IPsec session | ✓ | ✓ | Establish IKE/IPsec session for secure data transmission | Command and parameters | Command response | IKE/IPsec Authentication CA ⁴⁸ Certificate – R/X IKE/IPsec Authentication Certificate – R/X IKE/IPsec Authentication RSA Private Key – R/X DH Public Key (DH public key component)- R/W/X DH Secret Key (DH private Key component) – R/W/X IKE Shared Secret – W/X IKE Session Key – W/X IKE Authentication Key – W/X IPsec Shared Secret – W/X IPsec Session Key – W/X IPsec Authentication Key – W/X DRBG Entropy – R/X DRBG Seed – R/W/X DRBG 'V' Value – R/W/X DRBG 'C' Value – R/W/X |
| Perform self-tests on demand | ✓ | ✓ | Perform self-tests on demand by rebooting or power-cycling the module | Command | Status output | FW Verification Key – R/X All ephemeral keys - Z |

2.4.3 Additional Services

The module provides a limited number of services for which the operator is not required to authenticate or assume an authorized role. Table 13 lists the services for which the operator is not required to assume an authorized role or authenticate to the module in order to perform. None of these services disclose or substitute cryptographic keys and CSPs or otherwise affect the security of the module.

Table 13 – Additional Services

| Service | Description | Input | Output | CSP and Type of Access |
|-------------------------------|--|------------------------|------------------|---------------------------------|
| Authenticate to the module | Authenticate to the module | Command and parameters | Status output | Authentication password – R/W/X |
| Show status | View system status | Command | Status output | None |
| Display status and statistics | View current VSAT status and statistics, including IKE/IPSEC | Command | Command response | None |

⁴⁸ CA – Certificate Authority

| Service | Description | Input | Output | CSP and Type of Access |
|--------------------------------------|--|---------------------------|---------------|------------------------|
| Display result of built-in self-test | Display results of non-cryptographic self-tests to confirm the health of the system | Command | Status output | None |
| Access help | Link to Jupiter Worldwide Enterprise to access help information for troubleshooting and operating the system | Command | Status output | None |
| Reboot | Manually reboot the module | Power-cycle; reset button | Status output | All ephemeral keys – Z |

2.4.4 Non-Approved Services

The module performs service-by-service switching between FIPS-Approved and non-FIPS Approved mode. Table 14 below lists the services available in the non-Approved mode of operation.

Table 14 – Non-Approved Services

| Service | Operator | | Security Function(s) |
|--------------------------------|----------|------|----------------------------|
| | CO | User | |
| Get VSAT statistics via SNMPv2 | ✓ | ✓ | None |
| Send/Receive SNMPv2 traps | ✓ | ✓ | SNMPv2 KDF (non-compliant) |

2.4.5 Authentication

The module supports role-based authentication. The VSAT provides access to Limited Advanced page locally only, via a PC connected to the VSAT LAN port. Certain links on the Limited Advanced page are password protected.

A successful authentication grants access to services that require authentication, and the module does not offer a method to change roles. Once an operator logs out, then re-authentication is required to again access module services.

Operator passwords shall be constructed using uppercase and lowercase letters, digits, and special characters, and will follow the password complexity policies found in section 3.4 of this document. The minimum length of the password is eight characters, with 90 different case-sensitive alphanumeric characters and symbols possible for usage. The probability that of a random attempt will succeed or a false acceptance will occur is 1 per 90⁸ possible passwords, or 1 per 4.3x10¹⁵ attempts, which is a lesser probability than 1 per 1,000,000 required by FIPS 140-2.

The fastest network connection supported by the module is 1000 Mbps. At most (1x10⁹ bits/second × 60 seconds) = 6x10¹⁰ = 60,000,000,000 bits of data can be transmitted in one minute. The minimum password is 64 bits (8 bits per character × 8 characters), meaning 9.375x10⁸ passwords can be passed to the module (assuming there is no overhead). This equates to a 1:4,591,650 chance of a random attempt will succeed, or a false acceptance will occur in a one-minute period, which is a lesser probability than 1 per 100,000 required by FIPS 140-2.

2.5 Physical Security

The Terminals comprise a multiple-chip standalone cryptographic module. The contents of the module, including hardware components, firmware, and data are all protected by the module enclosure. The module enclosure is opaque within the visible spectrum and consists of a hard production-grade metal case that completely encloses all internal components. The enclosures have a removable cover that is secured with screws and serialized tamper-evident labels. Note that tamper evident labels used on the HT2650 are larger than on the other models but are otherwise identical in function.

In addition, all internal components of the module are production-grade and coated with commercial-standard passivation.

2.6 Operational Environment

The module does not provide a general-purpose OS to the user. The module has an Acadia ASIC processor which runs the MontaVista Linux (kernel 3.10.53) The module offers no mechanisms for the operator to modify software/firmware components of the operating system, nor does it offer a way to load and execute software or firmware that was not included as part of the module validation. Only the signed image installed on each module can be executed.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 15.

Table 15 – Cryptographic Keys, Cryptographic Key Components, and CSPs

| Key | Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|----------------------------------|-------------------------|---|-------------------------|----------------------------------|---|---|
| Firmware Verification Key | 2048-bit RSA public key | Generated externally and installed at the factory | Never exits the module | Plaintext in non-volatile memory | N/A | Used in firmware integrity check and firmware load test |
| SBC Config file Verification Key | 2048-bit RSA public key | Generated externally and installed at the factory | Never exits the module | Plaintext in non-volatile memory | N/A | Used in SBC config file integrity check |
| NMS-Terminal SDL Protocol Key | 2048-bit DSA public key | Generated externally and installed during initial configuration | Never exits the module | Plaintext in non-volatile memory | N/A | Authentication of packets sent from the NMS to the module |
| TMK | 256-bit AES-CBC key | Generated externally and installed at the factory | Never exists the module | Plaintext in non-volatile memory | Decommission | Encryption/decryption – decrypts EEMK |
| EEMK | 256-bit AES-CTR key | Generated externally and installed during initial configuration | Never exists the module | Encrypted in non-volatile memory | Decommission | Decrypted with TMK to generate the EMK |
| EMK | 256-bit AES-CTR key | Generated internally by decrypting the EEMK | Never exits the module | Plaintext in volatile memory | Decommission, reboot, power cycle, or session termination | Decrypts the session keys |
| EUSK | 256-bit AES-CTR key | Generated externally and entered encrypted via SDL protocol | Never exits the module | Encrypted in non-volatile memory | Decommission | Decrypted with EMK to generate the USK |
| USK | 256-bit AES-CTR key | Generated internally by decrypting the EUSK | Never exits the module | Plaintext in volatile memory | Decommission, reboot, power cycle, or session termination | Secure session traffic |
| EMSK | 256-bit AES-CTR key | Generated externally and entered encrypted via SDL protocol | Never exits the module | Encrypted in non-volatile memory | Decommission | Decrypted with EMK to generate the MSK |

| Key | Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|--|---------------------------------|---|-------------------------------|--|---|--|
| MSK | 256-bit AES-CTR key | Generated internally by decrypting the EMSK | Never exits the module | Plaintext in volatile memory | Decommission, reboot, power cycle, or session termination | Secure session traffic |
| EISK | 256-bit AES-CTR key | Generated externally and entered encrypted via SDL protocol | Never exits the module | Encrypted in non-volatile memory | Decommission | Decrypted with EMK to generate the ISK |
| ISK | 256-bit AES-CTR key | Generated internally by decrypting the EISK | Never exits the module | Plaintext in volatile memory | Decommission, reboot, power cycle, or session termination | Secure session traffic |
| Authentication Password | SHA-256 hash value | Generated externally and hashed during initial configuration | Never exits the module | Obfuscated in non-volatile memory | Decommission | Used for authentication |
| IKE/IPsec Authentication CA Certificate | 2048-bit RSA public key | Generated externally and installed during initial configuration | Never exits the module | Plaintext in configuration file in non-volatile memory | Decommission, deletion of configuration file | Authentication during IKE/IPsec session negotiation |
| IKE/IPsec Authentication Certificate | 2048-bit RSA public key | Generated externally and installed during initial configuration | Never exits the module | Plaintext in configuration file in non-volatile memory | Decommission, deletion of configuration file | Authentication during IKE/IPsec session negotiation |
| IKE/IPsec Authentication RSA Private Key | 2048-bit RSA private key | Generated externally and installed during initial configuration | Never exits the module | Plaintext in configuration file in non-volatile memory | Decommission, deletion of configuration file | Authentication during IKE/IPsec session negotiation |
| DH Public Key (DH public key component) | 2048 and 4096-bit DH public key | Internally generated based on SafePrime key generation method | Exits the module in plaintext | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys |
| DH Secret Key (DH private key component) | 2048 and 4096-bit DH public key | Internally generated based on SafePrime key generation method | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys |
| IKE Shared Secret | Shared Secret | Derived internally via DH shared secret computation | Never exits the module | Plaintext in volatile memory | Decommission, reboot; remove power; session termination | Derivation of the IKE Session Key and IKE Authentication Key |

| Key | Key Type | Generation / Input | Output | Storage | Zeroization | Use |
|--------------------------|-------------------------------|---|------------------------|------------------------------|---|--|
| IKE Session Key | 256-bit AES key | Derived internally via IKE KDF | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Encryption and decryption of IKE session packets |
| IKE Authentication Key | 256-bit HMAC key | Derived internally via IKE KDF | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Authentication of IKE session packets |
| IPsec Shared Secret | Shared Secret | Derived internally via DH shared secret computation | Never exits the module | Plaintext in volatile memory | Decommission, reboot; remove power; session termination | Derivation of the IPsec Session Key and IPsec Authentication Key |
| IPsec Session Key | 256-bit AES key | Derived internally via IKE KDF | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Encryption and decryption of IPsec session packets |
| IPsec Authentication Key | 256-bit HMAC key | Derived internally via IKE KDF | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle; session termination | Authentication of IPsec session packets |
| DRBG Seed | Hash based DRBG 440-bit value | Generated internally | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle | Seed material for NIST SP 800-90A Hash DRBG |
| DRBG Entropy | Hash based DRBG 256-bit value | Generated internally | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle | Entropy material for NIST SP 800-90A Hash DRBG |
| DRBG 'V' Value | Internal state value | Generated internally | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle | Used for NIST SP 800-90A Hash DRBG |
| DRBG 'C' Value | Internal state value | Generated internally | Never exits the module | Plaintext in volatile memory | Decommission, reboot; power cycle | Used for NIST SP 800-90A Hash DRBG |

Notes:

The module does not generate RSA keys. All RSA keys are generated externally and loaded into the module.

2.8 EMI / EMC

The Terminals were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed automatically by the module when the module is first powered up and loaded into memory as well as conditionally. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The Terminals performs the following self-tests at power-up:

- Firmware
 - Firmware integrity test (RSA 2048-bit with SHA256)
 - Hughes HT Satellite Terminal OpenSSL Crypto Library 1.0
 - AES encrypt and decrypt KATs⁴⁹ (ECB-mode)
 - DRBG KAT (NIST SP800-90A Hash DRBG)
 - HMAC KAT with SHA-1 (160-bit) and SHA2-2 (256-bit)
 - DSA pairwise consistency test
 - RSA KAT
 - DH Primitive “Z” Computation KAT (MODP-2048 and MODP-4096)

NOTE: A separate test for SHA-1 and SHA-2 is not needed as these algorithms are tested in the HMAC KAT.

- Hardware
 - Hughes HT Satellite Terminal SWP Hardware Crypto Library 1.0
 - AES encrypt and decrypt KATs (CBC-mode)
 - HMAC KAT using SHA2-256
 - SHA2-256 KAT
 - Hughes HT Satellite Terminal UPP Hardware Crypto Library 1.0
 - AES encrypt and decrypt KATs (CTR-mode)
 - Hughes HT Satellite Terminal DPP Hardware Crypto Library 1.0
 - AES encrypt and decrypt KATs (CTR-mode)

2.9.2 Conditional Self-Tests

The Terminals performs the following conditional self-tests:

- Firmware:
 - Hughes HT Satellite Terminal OpenSSL Crypto Library 1.0
 - Firmware Load Test (2048-bit RSA with SHA2-256)

⁴⁹ KAT – Known Answer Test

- Continuous Health Tests on the entropy source:
 - Stuck test on entropy source
 - Adaptive Proportion Test on entropy source
 - Repetition Count Test on entropy source
 - Lag predictor test

The entropy source are also performed on 1024 consecutives noise source samples at module power-up.

The module performs all applicable assurances for its key agreement scheme as specified in section 9 of *NIST SP 800-56Arev3*.

2.9.3 Critical Function Self-Tests

The module performs health checks for the DRBG's Generate, Instantiate, and Reseed functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These tests are performed at module power-up.

2.9.4 Self-Test Failures

If the module enters the critical error state due to a failure of the firmware integrity test, the fallback firmware is loaded, and the error message will be logged in the `/var/log/sig.log` file. The error condition is considered to have been cleared if the module successfully passes the integrity test and then all subsequent power-up self-tests. If the module continues to return to a halted state, the module is considered to be malfunctioning or compromised, and Hughes Customer Support must be contacted.

If the module enters the critical error state due to a failure of any of the remaining power-up self-tests, or if a conditional self-test fails (other than the firmware load test), all cryptographic functions and data output services are inhibited and an error message will be logged in the `/f10/fipskat_result.txt` log file and is also visible on the GUI. The CO must contact Hughes Customer Support if this error persists.

If the firmware load test fails, the firmware load process is aborted and no firmware is loaded; however, no module halts or restarts are required to clear the error state. This is a transient error state; once the module sends a status message of the error, then the error state is automatically cleared, and the module returns to a fully operational state.

The module outputs status on both success and failure of the power-up self-tests, check `/f10/fipskat_result.txt` for the results of self-tests.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Installation and Setup

The CO is responsible for receiving the module, verifying package contents, and ensuring the site is prepared for initial setup and configuration. Prior to beginning this process, the CO must review the appropriate User Guide and Install Manual provided by Hughes. The following sections provide guidance for verifying placement of the tamper evident seals and performing initial setup and configuration. All steps must be completed before the module's first use.

3.1.1 Initial Tamper-Evident Label Inspection

Tamper-evident labels are applied at the factory to the Terminals to protect against unauthorized access to the modules. The tamper evident seals shall be installed for the module to operate in the approved mode of operation. If an attacker attempts to remove the labels, a residue will be left on the appliance. When the module is received, the operator must confirm placement of all tamper-evident labels.

For the HT2300, tamper-evident labels are placed on the back, top, and bottom of the enclosure (3 in total). The tamper-evident label on the back of the enclosure connects the back to the top of the device. The tamper-evident labels on the top and bottom of the enclosure secure the seams. The label placement connects both surfaces of the device so evidence of a tamper attempt will be left behind if an attacker tries to open the enclosure. If upon inspection it is found the labels have been tampered with the CO shall return the module to Hughes.

Refer to Figure 2 and Figure 3 below for placement of the tamper-evident labels.



Figure 2 – Back View of the HT2300



Figure 3 – Bottom view of the HT2300

The HT2500/HT2550 has a single (1) tamper-evident label connecting the front closure to the top of the metal enclosure. The metal enclosure is a single unit that slides off the back of the appliance. Placement of the tamper-evident label between these two surfaces ensures that evidence of tampering would be visible if an attacker tried to remove the enclosure. Refer to Figure 4 below for placement of the tamper-evident label.

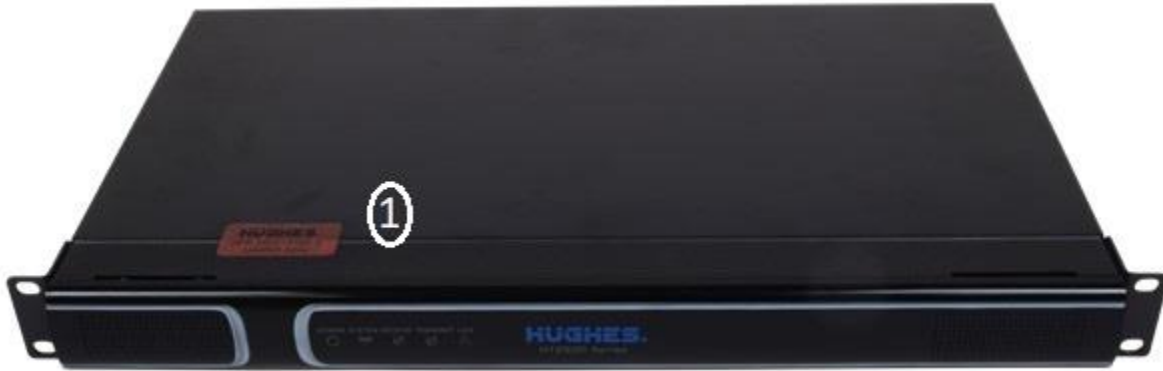


Figure 4 – Top View of the HT2500/HT2550

The bottom cover of the HT2650 is connected to the top cover of the server with screws. If these screws are removed, then the components of the module are exposed. A tamper-evident label is placed on a screw on the right and left side of the bottom cover (2 in total). Placement of the tamper-evident labels on each screw ensures that evidence of tampering would be visible if an attacker tried to remove the enclosure. Refer to Figure 5 and Figure 6 below for placement of the taper-evident labels.



Figure 5 - Bottom right view of HT2650



Figure 6 - Bottom left view of HT2650

3.1.2 Initial Setup and Configuration

For installation instructions, the CO shall refer to the User Guide and Install Guide for the appropriate model of the module. During the initial setup process the following steps will be performed:

1. The CO will power up the module, install the outdoor antenna, connect the cables and execute the terminal installation and registration procedure. As part of this procedure, will register with the system and the configuration files will automatically be downloaded from NMS. [Note: The terminal is NOT in FIPS-Approved mode when coming out of factory].
2. The SDL DSA Public key for SDL signature validation is downloaded from NMS
3. Configuration files are downloaded via SDL protocol. IPsec Keys are downloaded as a part of these configuration files
4. The module will check to confirm “FIPS_Mode = Enabled” in the configuration files. If enabled, the module will automatically reboot. Upon reboot, the firmware integrity check and power-up self-tests will be performed

The CO will validate that the module is operating in a FIPS-Approved mode by verifying status on the Web UI⁵⁰.

3.2 Crypto Officer Guidance

The CO is responsible for ensuring that the module is operating in the FIPS-Approved mode of operation.

⁵⁰ UI – User Interface

3.2.1 Management

Once installed and configured, the CO is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to sections 3.1, 3.2, and 3.4 for guidance that the CO must follow to ensure that the module is operating in a FIPS-Approved manner.

3.2.2 Load IPsec Key Files

The CO must follow the procedure below to load the key files, and only after this is done can the module be operated in the FIPS Approved mode. This process can be repeated whenever the module is in a FIPS-Approved mode of operation to update keys. The following steps are performed to load the key file:

1. The CO loads new keys into NMS
2. The SDL protocol automatically informs the Terminal that updated keys are available
3. The Terminal automatically executes the SDL protocol with the NMS and downloads the updated key files
4. The Terminal automatically deletes the existing keys and loads the new key file into non-volatile memory

3.2.3 On-Demand Self-Tests

Although power-up self-tests are performed automatically during module power up, they can also be manually launched on demand. Self-tests can be executed by power-cycling the module, using the reset button on the platform (if applicable), or via the Web UI in “Self-Test” submenu.

3.2.4 Zeroization

There are many CSPs within the module’s cryptographic boundary including symmetric keys, private keys, public keys, and passphrases. CSPs reside in multiple storage media including the RAM⁵¹ and system memory. All ephemeral keys are zeroized on module reboot, power removal, or session termination. Before taking the module out of FIPS-Approved mode, the CO must zeroize all unprotected secret and private keys by performing the following steps:

1. Authenticate to the Web UI and navigate to **Advanced Menu -> Installation -> Advanced -> Delete Key Files**
2. Select the **Delete Key Files** button
3. A “Delete All Key Files successfully” message will appear when all keys are deleted
4. Verify all key files are deleted by navigating to **Advanced Menu -> Installation -> Advanced -> Display Key Files**. A message of “No Key File found” will be displayed.

3.2.5 Decommission

To decommission the VSAT modules, the CO must do the following:

⁵¹ RAM – Random Access Memory

1. Authenticate to the Web UI and navigate to Advanced Menu -> Installation -> Install
2. Select the Reinstall button
3. A confirmation message will be displayed
4. Click OK to confirm. The VSAT will perform the decommission process and reboot automatically.

3.2.6 Monitoring Status

The CO shall be responsible for regularly monitoring the module's status for the FIPS-Approved mode of operation. The CO confirms the module status via the dashboard of the Web UI.

3.3 User Guidance

While the CO is responsible for ensuring that the module's physical security mechanisms are in place and that the module is running in a FIPS-Approved mode of operation, users should also monitor appliance status. Any changes in the status of the module should immediately be reported to the CO.

3.4 Additional Guidance and Usage Policies

The notes below provide additional guidance and policies that must be followed by module operators:

- For services requiring authentication the module shall be administered locally.
- To execute the module's power-up self-tests on-demand, the module's host device can be rebooted or power-cycled using the reboot command from the WebGUI or the reset button.
- All passwords are created and updated through the Hughes internal systems as hash values. Even though the Hughes internal system is outside the scope of this validation, it is the responsibility of all operators to ensure that the following password restrictions followed:
 - Password must be eight (8) characters long
 - At least one lowercase letter
 - At least one uppercase letter
 - At least one digit
 - At least one special character (~, ` , !, @, #, \$, %, ^, &, *, -, _ , =, +, {, }, [,], |, \, :, <, >, /, ., ,, ", ")
- The SDL service monitors the system for new firmware. When new firmware is available, it is automatically loaded into the module. Before loading the new firmware, a Firmware Load Test is performed. If the Firmware Load Test passes, the new firmware is loaded into flash and will replace the existing firmware when the module is rebooted. If the Firmware Load Test fails, the firmware is discarded, an error is logged, and the module returns to normal operation.

4. Appendix

4.1 Acronyms

Table 16 provides definitions for the acronyms used in this document.

Table 16 – Acronyms

| Acronym | Definition |
|---------|--|
| AES | Advanced Encryption Standard |
| AIS | Adaptive In-route Selection |
| API | Application Programming Interface |
| ASIC | Application Specific Integrated Circuit |
| CA | Certificate Authority |
| CAVP | Cryptographic Algorithm Validation Program |
| CBC | Cipher Block Chaining |
| CCCS | Canadian Centre for Cyber Security |
| CKG | Cryptographic Key Generation |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto Officer |
| CPU | Central Processing Unit |
| CRC | Cyclic Redundancy Check |
| CSP | Critical Security Parameter |
| CTR | Counter |
| CVL | Component Validation List |
| DH | Diffie-Hellman |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| DVB-S2X | Digital Video Broadcasting – Satellite – Second Generation (Extension) |
| EC | Elliptic Curve |
| ECC CDH | Elliptic Curve Cryptography Cofactor Diffie Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EEMK | Encrypted Effective Master Key |
| EMI/EMC | Electromagnetic Interference/Electromagnetic Compatibility |
| EMK | Effective Master Key |
| FFC | Finite Field Cryptography |
| FIPS | Federal Information Processing Standard |

| Acronym | Definition |
|---------|--|
| FOM | FIPS Object Module |
| GUI | Graphical User Interface |
| GW | Gateway |
| HMAC | (keyed-) Hash Message Authentication Code |
| IFL | Inter-Facility Link |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| ISK | In-Route Session Key |
| IU | Indoor Unit |
| IV | Initialization Vector |
| KAS | Key Agreement Scheme |
| KAS-SSC | Key Agreement Scheme – Shared Secret Computation |
| KAT | Known Answer Test |
| KDF | Key Derivation Function |
| KMS | Key Management Server |
| KPG | Key Pair Generation |
| LAN | Local Area Network |
| LDPC | Low Density Parity Coding |
| LED | Light-Emitting Diode |
| Mbps | Megabits Per Second |
| MBX | Multiplexed Block Exchange |
| MHz | Mega Hertz |
| MSK | Multi-Cast Session Key |
| N/A | Not Applicable |
| NIST | National Institute of Standards and Technology |
| NMS | Network Management Server |
| ODU | Outdoor Unit |
| OS | Operating System |
| PCT | Pairwise Consistency Test |
| PKCS | Public Key Cryptography Standard |
| PUB | Publication |
| RAM | Random Access Memory |
| RNG | Random Number Generator |
| RSA | Rivest Shamir Adleman |
| SATA | Serial Advanced Technology Attachment |

| Acronym | Definition |
|---------|------------------------------------|
| SCSI | Small Computer System Interface |
| SDL | Software Download |
| SHA | Secure Hash Algorithm |
| SHS | Secure Hash Standard |
| SNMP | Simple Network Management Protocol |
| SP | Special Publication |
| SSL | Secure Socket Layer |
| TMK | Terminal Master Key |
| UI | User Interface |
| U.S. | United States |
| USB | Universal Serial Bus |
| USK | Unicast Session key |
| VoIP | Voice Over Internet Protocol |
| VSAT | Very Small Aperture Terminal |

Prepared by:
Corsec Security, Inc.



13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050

Email: info@corsec.com

<http://www.corsec.com>
