Hughes Network Systems, LLC

HX280 Broadband Satellite Router

Hardware Part Number: Rev. C; Firmware Versions: 6.6.0.3 and 6.7.0.10

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.2

Prepared for:

Hughes Network Systems, LLC
11717 Exploration Lane,
Germantown, MD 20876
USA

Phone: +1 (301) 428-5500
http://www.hughesnet.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
USA

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HX280 Broadband Satellite Router (Hardware Part Number: Rev. C; Firmware Versions: 6.6.0.3 and 6.7.0.10) from Hughes Network Systems, LLC. This Security Policy describes how the HX280 Broadband Satellite Router meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which 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 National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) 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 HX280 Broadband Satellite Router is referred to in this document as the HX280, the hardware 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 corporate website (http://www.hughesnet.com) contains information on the full line of products available from Hughes.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer 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
- Finite State Model document
- Other supporting documentation as additional references

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.

2 HX280 Satellite Router

2.1 Overview

Geostationary satellite coverage available from Hughes Network Systems, LLC provides the capability to deliver broadband internet service anywhere around the world. Optimized for broadband IP[1] services, Hughes systems support a wide variety of applications, from high-speed internet/intranet access, to video conferencing, to voice over IP (VoIP), and adhere to industry standards for voice, video, and serial data protocols. The Hughes HX system is a broadband satellite system, designed and optimized for carrier-grade IP broadband networking and specialized for applications such as mobility and mesh networking. The system includes an economical gateway earth station and high performance remote terminals.

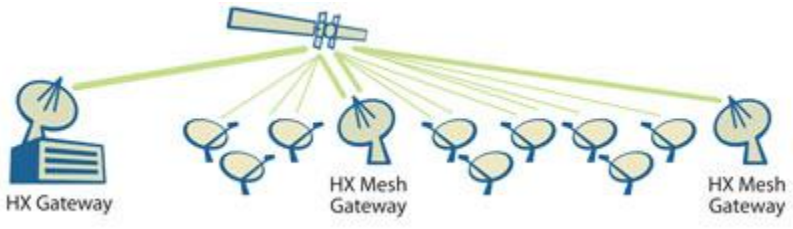

Figure 1 – Hughes HX System

The HX280 is one router in a family of Hughes' high performance remote terminal routers, and is ideal for commercial and government/military applications. The HX280 supports the HX System Enhanced Signaling Security (ESS) feature, which protects all data, management, and signaling traffic over the satellite network using a secure 256-bit AES[2] tunnel over the satellite port with keys that are established out of band.

The HX280 has been validated at the FIPS 140-2 section levels shown in Table 1 below.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC[3]	2

[1] IP – Internet Protocol
[2] AES – Advanced Encryption Standard
[3] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

.

Section	Section Title	Level
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The HX280 Broadband Satellite Router is a hardware module with a multi-chip standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the HX280 is defined by the chassis of the satellite router. The module is a 1U rack-mountable system that includes LED[4]s at the front panel to display operational status. A picture of the HX280 front panel is shown in Figure 2 below.

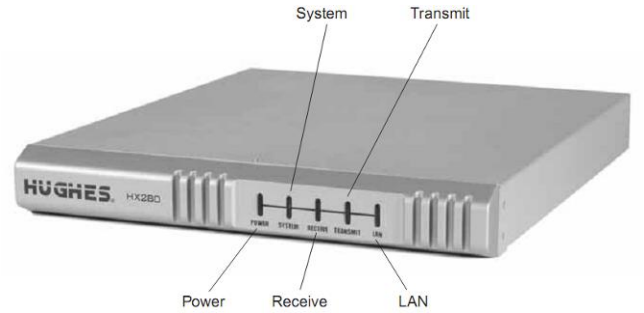

Figure 2 – Front Panel of HX280

The back panel of the module provides communication ports, including Ethernet ports and satellite ports. Ethernet ports have their own LEDs to show activity status, with green and yellow LEDs on each port to indicate link speed, status and Ethernet mode. The satellite ports connect the module with an Out-Door Unit (ODU) for satellite transmissions. The rear panel is also populated with a serial port, 10 Mega Hertz (MHz) signal ports, power switch, and a Rescue button. The AC[5] power interface and the 48 Volts (V) DC[6] power interface are also populated on the rear panel of the module as depicted in Figure 3.

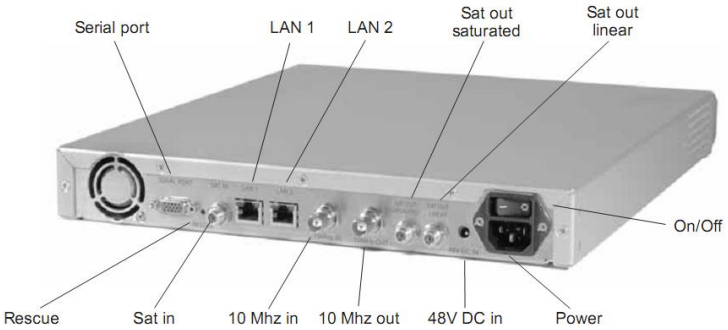

Figure 3 – Rear Panel of HX280

The hardware module consists of the integrated circuits of a motherboard, Mesh Receive Module (MRM) daughter card, a CPU[7], RAM[8], Flash memory, metal enclosure, power supply and fans. A block diagram of the module is shown in the figure below.

[4] LED – Light Emitting Diode
[5] AC – Alternating Current
[6] DC – Direct Current
[7] CPU – Central Processing Unit

.

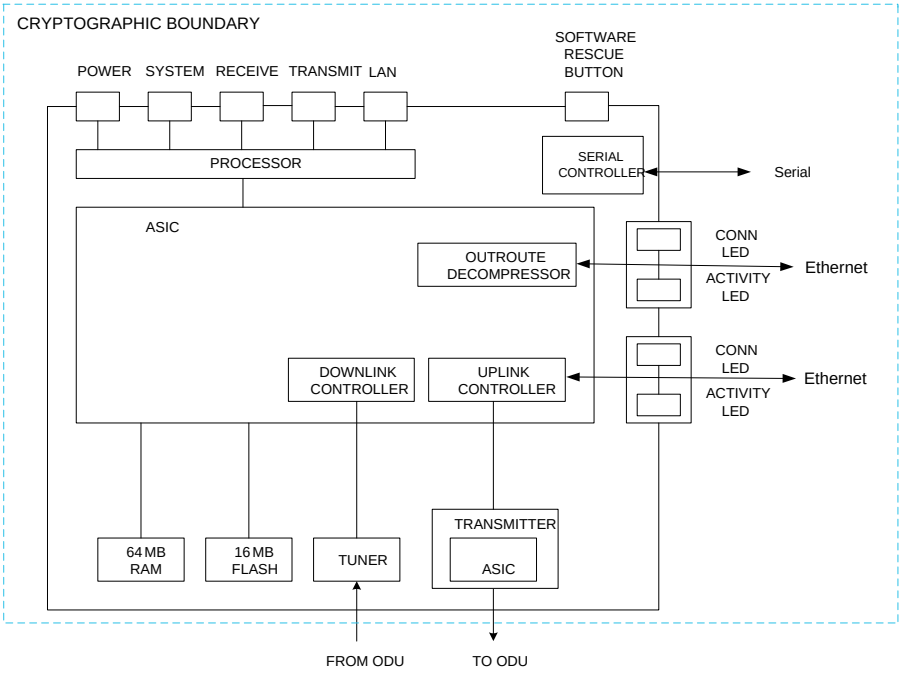

Figure 4 – Block Diagram

2.3 Module Interfaces

The physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

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

The module features physical ports as depicted in section 2.2 above. The following is a list details use of physical ports for the module in FIPS-approved mode of operation:

- Ethernet ports: The HX280 provides two 10/100 Local Area Network (LAN) ports. The Ethernet LAN port and the 10/100 LAN ports can be connected via a straight-through or crossover Cat-5 cable to a single computer or to an Ethernet hub/switch port.
- Satellite ports: Both the saturated ("Sat out saturated") and the linear ("Sat out linear") satellite ports transmit over outdoor units (ODUs). The Sat in port receives incoming satellite signals from the ODU.
- Serial port: The serial port is used for communicating to a global positioning system (GPS) terminal or an antenna
- 10MHz port: These ports provide 10MHz reference clock input and output
- Light Emitting Diodes: LEDs provide operational status indications for the router
- Rescue button: The module can be returned to the factory default configuration by pressing the Rescue button.

[8] RAM – Random Access Memory

- Power switch: The power switch turns the module on or off
- 48V DC: 48 V DC power supply voltage input port supporting the use of 8 Watt Ku-band radio transmissions, or 10 Watt C-band radio transmissions
- Power interface: The router requires 100 to 253 Volt AC input through a detachable power cord in order to be operational

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

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	HX280 Broadband Satellite Router Port/Interface
Data Input Interface	Ethernet port, Satellite IN port, 10MHz IN port, serial port
Data Output Interface	Ethernet port, Satellite OUT port, 10MHz OUT port, serial port
Control Input Interface	Ethernet port, Satellite IN port, Rescue button port, power switch
Status Output Interface	Ethernet port, Satellite OUT port, LEDs
Power Interface	Power interface, 48V DC power supply

2.4 Roles and Services

The module supports role-based authentication. There are three roles in the module that operators may assume: a Superuser role, a Crypto-Officer (CO) role and a User role.

2.4.1 Superuser Role

The "Superuser" installs and uninstalls the module and initializes the FIPS-Approved mode of operation. A Superuser accesses the module locally by connecting a Personal Computer (PC) to the module to an Ethernet port. The operator must authenticate to the module using an eight-character alphanumeric password to gain access. Please note that the keys and Critical Security Parameters (CSPs) listed in the following table indicate the type of access required using the following notation:

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

Table 3 – Superuser Services

Service	Description	CSP and Type of Access
Install the module	Install the module by following the Security Policy guidelines	Firmware upgrade key – R

.

Service	Description	CSP and Type of Access
Uninstall the module	Uninstall the module by following the Security Policy guidelines	Firmware upgrade key – R Preshared key – W ESS Encrypt key – W ESS MAC9 key – W Crypto-Officer password – W Superuser password – W
Commission the module	Set satellite, VSAT10, and LAN parameters, management IP address, and install ESS key file	Firmware upgrade key – R Preshared key – W ESS Encrypt key – W ESS MAC key – W Crypto-Officer password – W Superuser password – W
View status	Monitor log files of the system and services	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG[11] seed – R PRNG seed key – R
Load plaintext keys	Input plaintext keys into the module	Preshared key – W ESS Encrypt key – W ESS MAC key – W

2.4.2 Crypto-Officer Role

The CO may access the module both remotely and locally. CO local access does not allow the CO to make any configuration changes; it provides only an option to view the status of the module. The CO may make configuration changes and monitor the module's status remotely (via the Satellite port) or locally via Ethernet port. There are two secure ways to access the module remotely: using IKE[12]/IPsec[13] protocol or ESS protocol. Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Table 4 – Crypto-Officer Services

Service	Description	CSP and Type of Access
Access the System Control Center	Access the System Control Center via Ethernet port to monitor status on system, reception, transmission, and ESS/mesh	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R

[9] MAC – Message Authentication Code
[10] VSAT – Very Small Aperture Terminal
[11] PRNG – Pseudo Random Number Generator
[12] IKE – Internet Key Exchange
[13] IPsec – Internet Protocol Security

.

Service	Description	CSP and Type of Access
Configure outroute	Configure information for outroute traffic	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R
Configure Virtual LAN (VLAN)	Configure information for internal LAN	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R
Configure routing services	Configure IP stack and firewall related features	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R
View status	Monitor log files of the system and services	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R
Run diagnostics checks	Perform diagnostic checks on current traffic and systems	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R
Manage ESS traffic	Configuring signal IP over Satellite (IPoS) inroute signal management traffic	ESS Encrypt key – X ESS MAC key – X
Perform Self-tests	Perform self-tests on demand by rebooting the machine	Integrity Test key – X
Update firmware	Performs a update on the installed firmware	Firmware upgrade key – R
Decommission the module	Reset satellite, VSAT[14], and LAN parameters, management IP address, and remove ESS key file	Firmware upgrade key – R Preshared key – W ESS Encrypt key – W ESS MAC key – W Crypto-Officer password – W Superuser password – W
Load plaintext keys	Input plaintext keys into the module	Preshared key – W ESS Encrypt key – W ESS MAC key – W

[14] VSAT – Very Small Aperture Terminal

.

2.4.3 User Role

"Users" are defined as the end users who utilize the module's data transmitting capabilities for internet transmissions. User traffic enters or exits the module only via the Ethernet port and Satellite ports. The User services available in the module are based on the permissions set by the CO. Descriptions of the services available to the User role are provided in the table below.

Table 5 – User Services

Service	Description	CSP and Type of Access
Secure data transmission over Satellite port	Establish an IKE/IPsec session for data transmission	Preshared key – X IKE Key Agreement key – W IPsec Traffic key – W IPsec MAC key – W PRNG seed – R PRNG seed key – R Diffie Hellman public key – W, X Diffie Hellman private key – W, X

2.4.4 Authentication

The module supports role-based authentication. Table 6 lists the mechanisms employed by the module to authenticate different roles.

Table 6 – Authentication Mechanisms Supported by HX280 Broadband Satellite Router

Role	Authentication Mechanism	Strength of the Mechanism
CO, User	Preshared key	The key is 32-bytes long. The chance of a random attempt falsely succeeding is 1 in (2^{32} x 8 =) 1.158 x 10^{77}. Considering the network speed as a limiting factor, the chance of random success in a minute would be at most 1 in (6 x 10^{9} =) 6,000,000,000.
CO	ESS Encrypt key	The key is 32-bytes long. The chance of a random attempt falsely succeeding is 1 in (2^{32} x 8 =) 1.158 x 10^{77}. Considering the CPU speed as a limiting factor, the chance of random success in a minute would be at most 1 in (400 x 10^{6} x 60 =) 24,000,000,000.

.

Role	Authentication Mechanism	Strength of the Mechanism
Superuser, CO	Password	The minimum length of the password is 8 case-sensitive alphanumeric characters. Assuming only a 62-character set with repetition, the chance of a random attempt falsely succeeding is 1 in (62^8 =) 218,340,105,584,896. For multiple attacks within a one minute period the probability of a random attempt succeeding or false acceptance is 1 in 6×10^9. Considering the CPU speed as a limiting factor, the chance of random success in a minute would be at most 1 in (400 x 10^6 x 60 =) 24,000,000,000.

2.5 Physical Security

The entire contents of the module, including all hardware, firmware, and data are enclosed in a metal case. The case is opaque and sealed using a tamper-evident seal that prevents the case cover from being removed without signs of tampering. The manufacturer affixes a tamper-evident seal at the top of the chassis covering one screw, top removable cover, and the front bezel (Figure 5). All components are made of production-grade materials, and all integrated circuits in the module are coated with commercial standard passivation.

Figure 5 – Placement of Tamper-Evident Seal

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.6 Operational Environment

The operational environment requirements do not apply to the HX280 Broadband Satellite Router, because the module does not provide a general-purpose operating system (OS) to the user. The HX280 OS has a limited operational environment and only the module's custom written image can be run on the system.

The module provides a method to update the firmware in the module with a new version. This method involves downloading a digitally-signed firmware update (using DSA[15]) to the module.

2.7 Cryptographic Key Management

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

Table 7 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES CBC[16] (128-, 256-bit key)	1453
AES ECB[17], CTR[18] (256-bit key)	1451
SHA-1[19], SHA-256	1316
HMAC[20] SHA-1, HMAC-SHA-256	853
DSA (Signature Verification, 1024-bit)	463
ANSI[21] X9.31 PRNG (AES-128)	796

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementations:

- MD5[22] used in IKE/IPsec protocol
- Diffie-Hellman key agreement (caveat: 1024-bit Diffie-Hellman key agreement protocol provides 80 bits of encryption strength)
- non-FIPS-Approved random number generator for seed generation

[15] DSA – Digital Signature Algorithm
[16] CBC – Cipher Block Chaining
[17] ECB – Electronic Code Book
[18] CTR – Counter
[19] SHA-1 – Secure Hashing Algorithm 1
[20] HMAC – (Keyed-) Hash Message Authentication Code
[21] ANSI – American National Standard Institute
[22] MD5 – Message Digest 5

.

The module supports the CSPs listed below in Table 8.

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

Key/CSP	Generation / Input	Output	Storage	Zeroization	Use
Preshared key	Enter the module in plaintext	Never exit the module	Plaintext in Flash	Decommission or uninstall the module	Peer Authentication of IKE session
Diffie-Hellman public key	Generated internally	Exits the module in plaintext	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key
Diffie-Hellman private key	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot or session termination	Generation of IKE Key Agreement key
IKE Key Agreement key	Generated during IKE negotiation	Never exit the module	Plaintext in volatile memory	Reboot or session termination	Exchanging shared secret during IKE
IPsec Traffic key	Generated during IKE negotiation	Never exit the module	Plaintext in volatile memory	Reboot or session termination	Encryption or decryption of IPsec ESP packets
IPsec MAC key	Generated during IKE negotiation	Never exit the module	Plaintext in volatile memory	Reboot or session termination	Authentication IPsec ESP packets
ESS Encrypt key	Enter the module in plaintext	Never exit the module	Plaintext in Flash	Decommission or uninstall the module	Encryption or decryption of signal controlling traffic and authentication the CO
ESS MAC key	Enter the module in plaintext	Never exit the module	Plaintext in Flash	Decommission or uninstall the module	Authentication of signal controlling traffic
Crypto-Officer password	Enters the module in encrypted form	Never exit the module	Plaintext in Flash	Decommission or uninstall the module	Authentication of the CO to the module
Superuser password	Enters the module in plaintext	Never exit the module	Plaintext in Flash	Decommission or uninstall the module	Authentication of the Superuser to the module

.

Key/CSP	Generation / Input	Output	Storage	Zeroization	Use
PRNG seed	Continually polled from various system resources to accrue entropy	Never exit the module	Plaintext in volatile memory	Reboot	Random number generation
PRNG seed key	Continually polled from various system resources to accrue entropy	Never exit the module	Plaintext in volatile memory	Reboot	Random number generation
Firmware upgrade key	Enters the module in plaintext	Exits the module in plaintext	Plaintext in Flash	Decommission or uninstall the module	Verification of integrity and authenticity of the updated firmware
Integrity Test key	Generated externally, hard-coded in module	Never exits the module	Hard-coded	Decommission or uninstall the module	Verification of module integrity

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

The HX280 Broadband Satellite Router performs the following self-tests at power-up:

- Firmware integrity test using a DSA public key
- KATs
    - AES 128-, 256-bit key CBC mode KAT (encryption and decryption)
    - SHA-1 and SHA-256 KATs
    - HMAC-SHA-1 and HMAC SHA-256 KATs
    - ANSI X9.31 PRNG KAT

Upon self-test failure, the module disables all access to the cryptographic functionality and CSPs. All data output is inhibited upon a self-test failure. The CO must reboot the machine to clear the error condition and return to a normal operational state.

2.8.2 Conditional Self-Tests

The HX280 Broadband Satellite Router performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for both the Approved and non-Approved PRNGs
- Firmware update test

2.8.3 Critical Functions Self-Tests

At the power-up, the module performs the following tests:

- Minimum available memory
- Operating system version

2.9 Mitigation of Other Attacks

The Mitigation of Other Attacks requirements are not applicable to the HX280 Broadband Satellite Router since the module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The HX280 Broadband Satellite Router meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-approved mode of operation.

3.1 Superuser Guidance

The Superuser receives the module from the vendor via trusted delivery services (using commercial services such as UPS or FedEx) and is responsible for initialization of the module. Tamper-evident seals are applied by the vendor during manufacturing. Placement of the seal is described in the 'Physical Security' section of this document. Upon receipt of the module, the Superuser shall visually inspect the seal to ensure it is in the proper location and that it has not already been tampered with. If the seal appears to be in an un-tampered status, then the Superuser should proceed with the initialization process as described in 3.1.1 below; otherwise Hughes should be contacted.

3.1.1 Initialization

It is the Superuser's responsibility to configure the module in the FIPS-Approved mode and commission the router. Commissioning is the process of registering an HX280 satellite installation and router for service. During the commissioning process, the Superuser manually enters parameters for communicating over satellite and local network interfaces. Please see Hughes' Installation Guide for more information on the commissioning process. Note that the module does not operate in its FIPS-Approved mode of operation during initial configuration.

The configuration files are loaded onto the HX280 via the ESS protocol once the Superuser has loaded the ESS keys. Once the module has been configured, the Superuser must restart the module to transition the module to operating in a FIPS-Approved mode. The FIPS mode can then be viewed via the web interface with the following result:

- FIPS mode: **Enabled**
- FIPS level: **Level 2**

3.1.2 Plaintext Key Entry/Output

The Superuser may load plaintext keys. Plaintext keys shall only be loaded via a local PC that is directly attached to the module. The PC shall only be connected to the module while loading keys, and no other devices may be connected to the HX280 while keys are being loaded. The output of plaintext keys is prohibited.

3.2 Crypto-Officer Guidance

The CO is responsible for making sure the module runs in a FIPS-Approved mode of operation.

3.2.1 Management

Once the Superuser configures the module for FIPS-Approved mode of operation and reboots the module, FIPS-Approved mode will be enforced. The CO is responsible for ensuring that the module remains in a FIPS-Approved mode of operation by making sure that only FIPS-Approved and Allowed algorithms are being used. FIPS-Approved algorithms are listed in Table 7. Diffie-Hellman is also allowed to be used in FIPS-Approved mode of operation. The CO is able to monitor and configure the module via the web interface (GUI[23] over IPsec). The status can also be monitored by connecting a PC or laptop to the module directly via the Ethernet port.

If any irregular activity is noticed or the module is consistently reporting errors, then Hughes Network Systems, LLC should be contacted.

3.2.2 Zeroization

All ephemeral keys used by the module are zeroized upon reboot or session termination. The module stores the Preshared key and the Enhanced Signaling Security keys in plaintext in Flash memory. These keys are zeroized when the module is decommissioned. Decommissioning shall only be performed by the CO, and must be accomplished using the 'deconfigure VSAT' option on the Setup menu found on the **Advanced** page of the web interface.

The CO shall always perform the decommissioning procedure when using the 'Rescue' button to recover the module.

3.2.3 Plaintext Key Entry/Output

The CO may load plaintext keys. Plaintext keys shall only be loaded via a local PC that is directly attached to the module. The PC shall only be connected to the module while loading keys, and no other devices may be connected to the HX280 while keys are being loaded. The output of plaintext keys is prohibited.

3.3 User Guidance

Only the module's cryptographic functionalities are available to the User. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is noticed.

[23] GUI – Graphical User Interface

.

4 Acronyms

This section describes the acronyms.

Table 9 – Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DC	Direct Current
DSA	Digital Signature Algorithm
ECB	Electronic Book Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESS	Enhanced Signaling Security
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
LLC	Limited Liability Company
IKE	Internet Key Exchange
IP	Internet Protocol
IPoS	Internet Protocol over Satellite
IPsec	Internet Protocol Security
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MD	Message Digest

.

Acronym	Definition
MHz	Mega Hertz
MRM	Mesh Receive Module
NIST	National Institute of Standards and Technology
ODU	Out-Door Unit
OS	Operating System
PC	Personal Computer
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
SHA	Secure Hash Algorithm
V	Volts
VLAN	Virtual LAN
VSAT	Very Small Aperture Terminal
VoIP	Voice over IP

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
USA

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