DragonWave, Inc.

DragonWave® Secure Cryptographic Module

Hardware Version: Horizon® Quantum (PN: 74-000320)
Horizon® Compact+ (PN: 74-000320)
Tamper Evident Seal (PN: 65-000185-01-01)

Firmware Version: 1.2.5 (Compact+)
1.3 (Quantum)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.4

Prepared for:

DragonWave, Inc.
600-411 Legget Drive
Ottawa, Ontario K2K 3C9
Canada

Phone: +1 613 599 9991
Email: info@dragonwaveinc.com
http://www.dragonwaveinc.com

Prepared by:

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

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

Table of Contents

1 INTRODUCTION 4
- 1.1 PURPOSE 4
- 1.2 REFERENCES 4
- 1.3 DOCUMENT ORGANIZATION 4

2 DRAGONWAVE SCM 5
- 2.1 OVERVIEW 5
  - *2.1.1 Product Description 5*
  - *2.1.2 Applications 7*
  - *2.1.3 Cryptographic Functionality 7*
- 2.2 MODULE SPECIFICATION 9
  - *2.2.1 Physical Cryptographic Boundary 9*
  - *2.2.2 Logical Cryptographic Boundary 10*
- 2.3 MODULE INTERFACES 12
  - *2.3.1 Physical 12*
  - *2.3.2 Logical 15*
- 2.4 ROLES AND SERVICES 16
  - *2.4.1 Crypto Officer Role 16*
  - *2.4.2 Admin and NOC Roles 18*
  - *2.4.3 User Role 19*
- 2.5 PHYSICAL SECURITY 19
- 2.6 OPERATIONAL ENVIRONMENT 20
- 2.7 CRYPTOGRAPHIC KEY MANAGEMENT 20
- 2.8 SELF-TESTS 24
  - *2.8.1 Power-Up Self-Tests 24*
  - *2.8.2 Conditional Self-Tests 24*
  - *2.8.3 Critical Functions Self-Tests 25*
- 2.9 MITIGATION OF OTHER ATTACKS 25
  - *2.9.1 Operator-applied Security Labels 25*

3 SECURE OPERATION 27
- 3.1 INITIAL SETUP 27
- 3.2 MANAGEMENT 27
  - *3.2.1 Initialization 27*
  - *3.2.2 Management 29*
  - *3.2.3 Zeroization 29*
- 3.3 USER GUIDANCE 29

4 ACRONYMS 30

Table of Figures

FIGURE 1 – HORIZON QUANTUM INDOOR AND OUTDOOR UNIT 5
FIGURE 2 – HORIZON COMPACT+ 6
FIGURE 3 – PHYSICAL CONFIGURATION OF MODULE HARDWARE COMPONENT 10
FIGURE 4 – DRAGONWAVE SCM FIRMWARE BOUNDARY 11
FIGURE 5 – HORIZON QUANTUM PHYSICAL PORTS (FRONT) 12
FIGURE 6 – HORIZON QUANTUM PHYSICAL PORTS (REAR) 12
FIGURE 7 – HORIZON COMPACT+ PHYSICAL PORTS 14
FIGURE 8 – HORIZON COMPACT+ SIDE VIEW W/ ANTENNA 14
FIGURE 9 – HORIZON QUANTUM TAMPER-EVIDENT SEAL PLACEMENT 26
FIGURE 10 – HORIZON COMPACT+ TAMPER-EVIDENT SEAL PLACEMENT 26

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 8
TABLE 2 – HORIZON QUANTUM FIPS 140-2 LOGICAL INTERFACE MAPPINGS (PHYSICAL BOUNDARY) 13
TABLE 3 – HORIZON COMPACT+ FIPS 140-2 LOGICAL INTERFACE MAPPINGS (PHYSICAL BOUNDARY) 15
TABLE 4 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS (CRYPTOGRAPHIC BOUNDARY) 16
TABLE 5 – CRYPTO OFFICER SERVICES 17
TABLE 6 – ADMIN AND NOC SERVICES 19
TABLE 7 – USER SERVICES 19
TABLE 8 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 20
TABLE 9 – NON-APPROVED ALGORITHMS AND SERVICES 21
TABLE 10 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 22
TABLE 11 – CRYPTO COMMANDS 29
TABLE 12 – ACRONYMS 30

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the DragonWave® Secure Cryptographic Module from DragonWave, Inc. This Security Policy describes how the DragonWave Secure Cryptographic Module 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 (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 1 FIPS 140-2 validation of the module. The DragonWave Secure Cryptographic Module is referred to in this document as DragonWave SCM, 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 DragonWave® website (http://www.dragonwaveinc.com/) contains information on the full line of products from DragonWave®.
- 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 DragonWave®. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to DragonWave® and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact DragonWave®.

2 DragonWave SCM

2.1 Overview

DragonWave® is a leading provider of high-capacity packet microwave solutions that drive next-generation IP[1] networks. DragonWave's carrier-grade point-to-point packet microwave systems transmit broadband voice, video, and data, enabling service providers, government agencies, enterprises and other organizations to meet their increasing bandwidth requirements rapidly and affordably. The principal application of DragonWave's products is wireless network backhaul. Additional solutions include leased line replacement, last mile fiber extension and enterprise networks. DragonWave's award winning Horizon® solutions are known in the industry for their leading capacity, reliability, and spectral efficiency.

2.1.1 Product Description

The module is designed and manufactured by DragonWave, Inc., for use on the Horizon® Quantum, and Horizon Compact+ PWBs[2]. The Horizon Quantum deployment consists of an indoor unit and outdoor unit. The Horizon Quantum indoor unit is a fully-featured Ethernet switch containing two modems, which are capable of supporting one or two outdoor units (radios) simultaneously. The outdoor units are mounted up-mast and attached to the indoor unit via Intermediate Frequency (IF) cabling. Figure 1 below depicts the Horizon Quantum indoor and outdoor units.

Figure 1 – Horizon Quantum Indoor and Outdoor Unit

The Horizon Compact+ is a compact radio unit, mounted entirely up-mast, which is capable of copper or fibre-optic Ethernet connectivity to an indoor switch. Power is supplied to the unit via Power on Ethernet (PonE), or through dedicated power cabling. Figure 2 below depicts the Horizon Compact+ unit.

[1] *IP: Internet Protocol*
[2] *PWB: Printed Wiring Board*

Figure 2 – Horizon Compact+

A Horizon data link consists of two Horizon Quantum indoor units connected to radios or two Horizon Compact+ units on either end. Each radio is capable of 400 Mbps[3] of over-the-air throughput on a single channel. Horizon Quantum radio units are capable of operating on two radio channels simultaneously, providing throughput of up to 800 Mbps. In addition, the modems provide bandwidth acceleration features, which achieve actual throughput of up to a total of 2 Gbps[4] per unit (Horizon Quantum) or 1Gbps (Horizon Compact+).

Horizon radios are capable of operating in licensed and unlicensed spectrums ranging from 6-60 MHz[5]. A single Horizon radio link constitutes two radios, each known as a peer. For licensed spectrums, the peer radios each operate on two separate frequency channels, one in a higher end of the radio spectrum, and the other on the lower end, allowing for full-duplex communications. In this scenario, each peer is designated as TxHigh (TXH) or TxLow (TXL). The TXH peer transmits on the higher channel, and receives on the lower channel. The TXL peer transmits on the lower channel, and receives on the higher channel. Radios operating in the unlicensed band transmit and receive on the same channel.

Each Horizon model is manufactured for a specific radio band, frequency, and channel (high or low). For example, a PL-HP-23-B1-R1 is an Horizon Compact+ TXL (indicated by PL), high power (HP), operating in the licensed 23 GHz spectrum (23), with the applicable diplexer for the frequency (B1), as well as revision (R1).

Horizon radios may also be deployed in pairs on the same end for redundancy or bandwidth doubling purposes. In these scenarios, the radio units on the same end are identical. Each unit in a pair is known as a partner. In a redundancy configuration, the standby partner assumes the active role in the event that the active partner goes down. Two Horizon Quantum partners may be deployed in a bandwidth doubling configuration for an overall maximum throughput of 4 Gbps. Other scenarios include Dual Polarization Radio Mount, which enables two Horizon Quantum outdoor units aligned vertically and horizontally for up to 4 Gbps throughput.

[3] *Mbps: Megabits per second*
[4] *Gbps: Gigabits per second*
[5] *MHz: Megahertz*

2.1.2 Applications

Horizon Quantum and Horizon Compact+ units provide wireless backhaul solutions in the following applications.

2.1.2.1 WiMax

DragonWave offers a high-capacity, carrier-grade, integrated solution for Ethernet backhaul using interference-free licensed spectrum. Horizon Quantum enables a high capacity network core for WiMax backhaul expansion and remote scalability from 10 Mbps to 1 Gbps. Horizon Compact+ enables rapid network expansion with remote scalability from 10 Mbps to 500 Mbps. Higher throughputs can be achieved with the Bandwidth Acceleration feature. The Horizon Quantum units provide a split-mount architecture optimized for the high growth environment of WiMax deployments. Horizon Compact+ radios are integrated into a single all-outdoor element attached directly to the antenna. Management integration into the base station Element Management System (EMS) provides a single point of control for operations personnel.

2.1.2.2 3G Cellular Backhaul / Ethernet Evolution

Meet the growing demand for increased capacity and data transport resulting from third-generation (3G) cellular deployments. Horizon Quantum provides a cost-effective, high capacity, core network for Time Division Multiplexing (TDM) and Ethernet base station backhaul. Horizon Compact+ provides cost-effective, low capacity TDM services for existing base stations. The DragonWave portfolio of products offers software controlled upgradeability to high-capacity native Ethernet and TDM services with ultra-low latency to enable 3G evolution with the minimum of network churn.

2.1.2.3 Leased Line Replacement

For many businesses, the only option for last mile access is the incumbent local exchange carrier (ILEC), provided on an aging copper infrastructure with long mean-time-to-repair (MTTR). Horizon Quantum and Horizon Compact+ can replace leased services and eliminate recurring and expensive telecom costs while at the same time improving service availability and enabling future growth and options for services with a scalable Ethernet network.

2.1.2.4 Last Mile Fibre Extension

The greatest demand for broadband services is within the core metro markets. Horizon Quantum and Horizon Compact+ provide a superior complementary networking solution to rapidly extend high speed IP services from locations already attached to the service provider's network. The DragonWave portfolio of products is ideal for network hardening, disaster recovery and applications that require legacy TDM services and carrier-grade, high capacity native Ethernet systems.

2.1.3 Cryptographic Functionality

The hybrid module consists of a firmware-based cryptographic toolkit and cryptographic key and state management libraries, as well as a hardware-based AES[6] accelerator that provides bulk encryption of over-the-air data for the Horizon Quantum and Horizon Compact+ models. AES acceleration is provided by encryptor/decryptor cores, which are implemented along with a set of Quadrature Modulation (QM) modems and Ethernet packet processing logic (segmentation and reassembly, or SAR) within a hardware FPGA[7]. Also within the module's physical boundary is the microprocessor and volatile memory as is necessary for the module's execution.

[6] *AES: Advanced Encryption Standard*
[7] *FPGA: Field-Programmable Gate Array*

The FPGA is connected to Ethernet switching circuitry on one side, and RF[8] circuitry on the other. These hardware-based components are collectively referred to as the "Data Plane". Note: Only the FPGA component of the data plane is included within the module boundary.

The module firmware is part of a larger monolithic binary image which contains various Horizon management applications including a web-based management interface, CLI[9], SNMP[10] management [11]daemon, and other various networking support packages. These firmware components are collectively referred to as the "Management Plane".

The cryptographic firmware found within the Management Plane, representing the firmware portion of the hybrid module, consists of a cryptographic algorithm library, a DragonWave proprietary cryptographic state management library (known as *dwiCrypto)*, a secure transport library, and an FPGA driver. These components are collectively referred to as the "FIPS Firmware", and are used to control the operation of and key the Data Plane encryptor/decryptor (e.g. the hardware portion of the module), as well as securely transmit commands and data to remote peer and partners via TLS[12].

The DragonWave® Secure 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[13]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	1
14	Cryptographic Module Security Policy	1

[8] *RF: Radio Frequency*
[9] *CLI: Command Line Interpreter*
[10] *SNMP: Simple Network Management Protocol*
[11] *Note: The SNMP KDF functionality is outside of the logical hybrid-firmware boundary.*
[12] *TLS: Transport Layer Security*
[13] *EMI/EMC: Electromagnetic Interference / Electromagnetic Compatibility*

2.2 Module Specification

The DragonWave® Secure Cryptographic Module is a firmware-hybrid module with a multi-chip standalone embodiment. The overall security level of the module is 1. The cryptographic module was tested and found compliant on the following platforms:

- QNX Neutrino Real-Time Operating System (RTOS) 6.4.1 running on the Freescale MPC8313 microprocessor (firmware)
- FPGA, PN: 74-000320 (hardware)

The tested models include:

- Horizon Quantum (PN: 60-000471-03) running firmware version 1.3
  - Dual Modem
  - Dual Radio
- Horizon Compact+ (PN: CP-HP-18-B1-S-X-010-N-00-R1) running firmware version 1.2.5
  - Power: High Power
  - Frequency/Band: 18 GHz Band 1
  - Port Configuration: Dual Copper (Ethernet), Rugged
  - Hardware Configuration: Advanced Hardware with Encryption
  - Data Rate: 10 Mbps
  - Advanced Features: Bulk Data Encryption
  - Standard Features: None
  - Revision: 1

In addition, the module requires the application of tamper evident seals (PN: 65-000185-01-01). Please refer to section 2.9.1 below for application instructions.

DragonWave offers a wide array of configuration options including frequency, band, power, port configurations, and data rates. The two configurations (one per model) identified above have been tested for FIPS 140-2 compliance. The module is designed to function on any Horizon model with support for "Advanced Hardware with Encryption", and thus, the module is vendor-affirmed for all other configurations. Vendor affirmation requires the use of the same FPGA specified in this validation.

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.2.1 Physical Cryptographic Boundary

As a Level 1 firmware-hybrid, the module relies on the physical security characteristics of the host Horizon Ethernet appliance. The physical boundary of the cryptographic module is defined by the hard production grade enclosure around the host appliance hardware on which it runs. The hardware platform can exist in one of two configurations:

- The Horizon Quantum hardware platform consists of a printed wiring board (PWB), a CPU, RAM, NAND Flash, ROM, FPGA, Ethernet PHYs, ADCs[14]/DACs[15], RF transmitters/receivers and other application-specific RF circuitry, power supply, hard metal enclosure, and fans.

- The Horizon Compact+ hardware platform consists of a PWB, a CPU, RAM, ROM, NAND Flash, ROM, FPGA, Ethernet PHYs, ADCs/DACs, RF transmitters/receivers, a ruggedized weatherproof enclosure, and power supply. In addition, it also includes an RF diplexer, as the Horizon Compact+ is intended to be mounted directly to an antenna.

[14] *ADC: Analog to Digital Converter*
[15] *DAC: Digital to Analog Converter*

Figure 3 below depicts the physical configuration of the module's FPGA hardware mounted on the PWB:

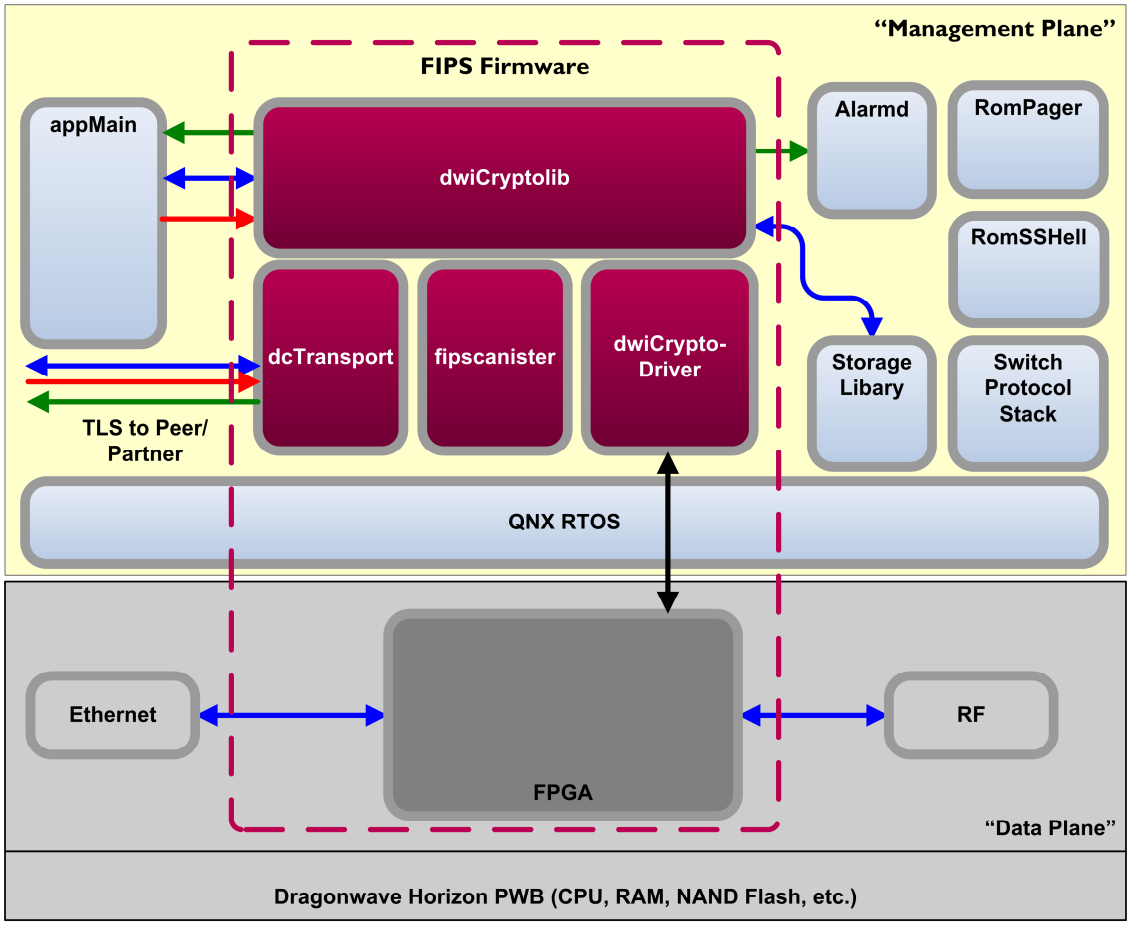
Figure 3 – Physical Configuration of Module Hardware Component

2.2.2 Logical Cryptographic Boundary

Within hardware, the cryptographic boundary encompasses only the FPGA (as it is necessary to execute the AES acceleration cores).

The firmware cryptographic boundary of the module is defined by the red dashed lines identified as "FIPS Firmware" in Figure 4 below. It encompasses the following firmware libraries:

- Cryptographic state management library (dwiCrypto)
- Transport library (dcTransport)
- Cryptographic algorithm library (fipscanister)
- FPGA Crypto driver library (dwiCryptoDriver)



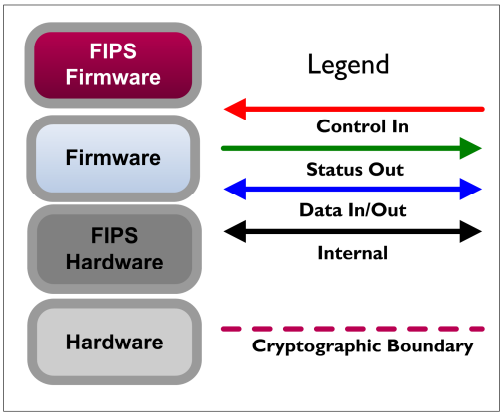


Figure 4 – DragonWave SCM Firmware Boundary

2.3 Module Interfaces

This section describes the module's physical and logical interfaces.

2.3.1 Physical

The module's physical ports are those of the host Horizon Quantum or Horizon Compact+ devices. Additionally, the module's manual controls, physical indicators, and physical, logical, and electrical characteristics are those of the Horizon Quantum and Horizon Compact+. The physical ports contained on the Horizon Quantum are depicted in Figure 5 and Figure 6 below:

Figure 5 – Horizon Quantum Physical Ports (Front)

The Horizon Quantum indoor unit provides an RJ-45 auxiliary console port, two SFP[16] ports, six gigabit Ethernet ports, power and status LEDs[17], and one or two N-Type IF connectors[18]. In addition, the rear of the unit contains a DB9 alarm output connector, two redundant -48V power feeds, and a fan housing.

Figure 6 – Horizon Quantum Physical Ports (Rear)

[16] *SFP: Small Form Factor Pluggable*
[17] *LED: Light Emitting Diode*
[18] During manufacturing, the Horizon Quantum is configured with either single or dual radio feeds. See section 3.0 "Physical Description" in Volume 1 of the Horizon Quantum product manual for more information.

The physical ports and interfaces for the Horizon Quantum are defined in Table 2 below:

Table 2 – Horizon Quantum FIPS 140-2 Logical Interface Mappings (Physical Boundary)

Physical Port/Interface	Quantity	FIPS 140-2 Interface
SFP Optical Ports (P1-P2)	2	• Data Input • Data Output • Control Input • Status Output
Ethernet Ports (P3-P8)	6	• Data Input • Data Output • Control Input • Status Output
RJ-45 Serial Port (CNTL)	1	• Not used
IF Connectors (ODU1-ODU2)	1	• Data Input • Data Output
Status LEDs (PWR & STAT)	2	• Non-cryptographic Status Output
Alarm Output Connector (ALARM OUTPUT)	1	• Non-cryptographic Status Output
Power (FEED A-B)	1	• Power Input

On the front of the Horizon Compact+ unit, an RF diplexer and antenna mount represent the over-the-air radio interface. The rear of the unit contains indicator LEDs (Radio/Ethernet/Alarm), and up to two data ports. Various physical port configurations are available on the parent Horizon Compact+ device, including Gigabit Ethernet, Fast Ethernet, and Optical Ethernet. Power is supplied via a dedicated -48V power feed (optical versions), or through PonE using a specialized Ethernet cable and power injector. The first data port is used for bulk data transfers (and power injection on Ethernet models), while the second port is typically reserved for out-of-band management. The module is implemented identically in all of the various Horizon Compact+ configurations; however, customers may choose between radio frequency bands and physical port configurations, depending on need. Table 4-1 in section 4.0 “Installation Requirements” in Volume 1 of the Horizon Compact+ product manual details the various installation kits and their specific power, connector, and locale configurations.

Figure 7 below depicts the physical ports on the Horizon Compact+; the LEDs are pictured on the left, while the data ports are shown on the bottom right:

Figure 7 – Horizon Compact+ Physical Ports

Figure 8 depicts a side view of the Horizon Compact+ appliance mounted to an antenna:

Figure 8 – Horizon Compact+ Side View w/ Antenna

In the tested configuration, Port 1 is a Gigabit Ethernet port used for power injection and bulk data transfers. Port 2 is a second Gigabit Ethernet port used for bulk data transfers and optionally, out-of-band management. All of the Horizon Compact+ physical interfaces described above are separated into logical interfaces defined by FIPS 140-2, as described in Table 3 below.

Table 3 – Horizon Compact+ FIPS 140-2 Logical Interface Mappings (Physical Boundary)

Physical Port/Interface	Port Configuration	Quantity	FIPS 140-2 Interface
Port 1	Gigabit Ethernet	1	• Data Input • Data Output • Control Input • Status Output • Power Input
Port 2	Gigabit Ethernet	1	• Data Input • Data Output • Control Input • Status Output • Power Input (PonE)
RF Diplexer	N/A	1	• Data Input • Data Output
Status LEDs (LINK, ETHERNET, POWER)	N/A	3	• Non-cryptographic Status Output

2.3.2 Logical

In addition to the physical ports described above, the Horizon Quantum and Horizon Compact+ firmware provides the following logical interfaces:

- dwiCrypto Application Programming Interface (API)
- Transport Interface
- Alarm Interface
- Modem Analog-to-Digital converter (ADC) GPIOs[19]
- Modem Digital-to-Analog converter (DAC) GPIOs
- Ethernet Reduced Gigabit Media Independent Interface (RGMII)

The logical cryptographic boundary includes only the FPGA hardware chip and the FIPS firmware libraries. The FIPS 140-2 Implementation Guidance (IG) 1.3 defines the requirements for a firmware module, while IG 1.9 defines the requirements of hybrid modules. This guidance states that all status and control ports and interfaces of the module shall be directed through the firmware interface in a firmware based module (controlling component). As such, the dwiCrypto API and the transport interface represent the entry point in the firmware for all status output and control input. In addition, the alarm interface is used to output status information, e.g. alarms, to an external alarm management daemon.

In addition, status output is directed to an alarm daemon running outside of the module boundary through the Alarm Interface. For peer and partner communication, a Transport Interface is used to initiate secure socket connections using TLS for transferring control and status information as well as passing data to/from the peer/partner device. The I/O pins connected to the modem ADC/DACs, and the Ethernet RGMIIs represent the data input/output ports.

[19] *GPIO: General Purpose Input/Output*

The module interfaces described above are separated into logical interfaces defined by FIPS 140-2, as described in Table 4 below:

Table 4 – FIPS 140-2 Logical Interface Mappings (Cryptographic Boundary)

Logical Port/Interface	FIPS 140-2 Interface
dwiCrypto API	• Data Input • Data Output • Control Input • Status Output
Transport Interface	• Data Input • Data Output • Control Input • Status Output
Alarm Interface	• Status Output
Modem ADC GPIO	• Data Input • Data Output
Modem DAC GPIO	• Data Input • Data Output
Ethernet RGMII	• Data Input • Data Output

2.4 Roles and Services

The module does not support role-based or identity-based operator authentication. All operators assume roles by authenticating to the underlying operating system (OS), or implicitly through the execution of APIs selected by the calling application. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role. The Crypto Officer (CO) is responsible for managing the module, and is implicitly assumed by authenticating to the module's underlying OS as the *superuser* account. The calling application also assumes the CO role when performing cryptographic management functions, which involves module power-up and initialization, and processing commands entered by the CO operator. Admin and NOC[20] users are the operators of the Horizon Quantum and Horizon Compact+ who have authenticated to the module's underlying OS with the *admin* or *NOC* accounts. Users are the end users or network devices that consume the module's bulk data encryption services (e.g. send/receive data to/from the module).

2.4.1 Crypto Officer Role

The Crypto Officer role has the ability to access the services provided to all other roles, and in addition, the CO performs cryptographic management functions. Descriptions of the services available to the Crypto Officer role are provided in Table 5 below. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

[20] *NOC: Network Operations Center*

- R – Read: The CSP[21] is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 5 – Crypto Officer Services

Service	Description	CSP and Type of Access	Approved Mode
Initialize module	Passes initialization instructions to the module	None	All Modes
Set "Enhanced Security" mode[22]	Changes default *superuser* account password and enforces strong operator authentication requirements	None	All Modes
Configure approved mode	Sets the module in Licensed or Non-licensed mode	None	All Modes
Set encryption mode	Sets the encryption mode (Enabled or Disabled). Setting mode to Disabled places the module in bypass.	None	Licensed Mode
Automatic key generation	Performs automatic key generation using Diffie Hellman key exchange.	DH[23] components (X)	Licensed Mode
Manual key entry	Enters AES encryption key (manual key entry mode only).	AES key (W)	Licensed Mode
Key activation	Activates a manually entered key.	AES key (X)	Licensed Mode
Force rekey	Initiates an on-demand automatic key exchange while in automatic key entry mode.	DH components (X) AES key (X)	Licensed Mode
Change rekey period	Modifies the period in which automatic keys are regenerated.	None	Licensed Mode
Show status	Monitor module status.	SHA[24]-256 hash of AES key (R)	All Modes
Symmetric encryption (TLS)	Encrypt plaintext using generated key for TLS communications with peer/partner.	AES key (X) TDES[25] key (X)	All Modes

[21] *CSP: Critical Security Parameter*
[22] *Note: The "Enhanced Security" mode is not available on Quantum models.*
[23] *DH: Diffie-Hellman*
[24] *SHA: Secure Hash Algorithm*
[25] *TDES: Triple Data Encryption Standard*

Service	Description	CSP and Type of Access	Approved Mode
Symmetric decryption (TLS)	Decrypt ciphertext using generated key for TLS communications with peer/partner.	AES key (X) TDES key (X)	All Modes
RSA[26] key wrap	Wrap/unwrap AES encryption key using RSA public key encryption for TLS communications with peer/partner.	RSA public key (X) RSA private key (X)	All Modes
DH key exchange	Perform DH key exchange	DH components (W)	Licensed Mode
Generate signature	Generates RSA signatures for TLS communications with peer/partner.	RSA private key (X)	All Modes
Verify signature	Verifies RSA signatures for TLS communications with peer/partner.	RSA public key (X)	All Modes
Generate random number	Returns specified number of random bits to calling application.	RNG[27] seed (W/X) RNG seed key (X)	All Modes
Generate keyed hash	Compute a message authentication code for TLS communications with peer/partner.	HMAC[28] key (X)	All Modes
Perform self-test	Performs start-up KATs on-demand.	HMAC key (X)	All Modes
Zeroize keys	Zeroize all cryptographic keys from module storage/memory. NOTE: The AES bulk data encryption key is zeroized via an API call, which clears the contents of the FPGA banks containing the key. All other keys are ephemeral and may be zeroized by power cycling or rebooting.	AES key (W) TDES key (W) DH components (W) RSA private/public key (W) HMAC key (W) RNG seed key (W)	All Modes

2.4.2 Admin and NOC Roles

The Admin and NOC Roles are implicitly assumed by users who have authenticated as *admin* and *NOC* accounts in the underlying OS. These roles have no access to run CO commands and therefore are not provided services offered by the module other than those offered to the User Role, except for the *reset*

[26] *RSA: Rivest, Shamir, Adleman*
[27] *RNG: Random Number Generator*
[28] *HMAC: Hash-Based Message Authentication Code*

system command, which causes the module to perform the power-up sequence and perform self-tests. For information on the services provided to the *admin* and *NOC* accounts by the outlier firmware applications, please refer to Volume 1 of the respective Horizon Quantum or Horizon Compact+ product manuals.

Descriptions of the module services available to the Admin and NOC role are provided in Table 6 below:

Table 6 – Admin and NOC Services

Service	Description	CSP and Type of Access	Approved Mode
Symmetric encryption	Pass unencrypted data to be encrypted by the module.	AES key (X)	Licensed Mode
Symmetric decryption	Pass encrypted data to be decrypted by the module.	AES key (X)	Licensed Mode
Bypass	Pass unencrypted data through the module.	None	All Modes
Reset system	Perform power-on self tests and zeroize ephemeral keys.	None	All Modes

2.4.3 User Role

The User role has the ability to consume the cryptographic services provided by the module. Users are the end users or network devices that pass data through the module. Only after the self-tests are performed, and the module is not in an alarm state, is the User able to utilize the cryptographic functionality of the module. Descriptions of the services available to the User role are provided in Table 7 below.

Table 7 – User Services

Service	Description	CSP and Type of Access	Approved Mode
Symmetric encryption	Pass unencrypted data to be encrypted by the module.	AES key (X)	Licensed Mode
Symmetric decryption	Pass encrypted data to be decrypted by the module.	AES key (X)	Licensed Mode
Bypass	Pass unencrypted data through the module.	None	All Modes

2.5 Physical Security

The DragonWave® Secure Cryptographic Module is a firmware-hybrid module, which FIPS defines as a multi-chip standalone cryptographic module. However, the physical cryptographic boundary is the enclosure of the host Horizon Quantum or Horizon Compact+ device. The entire contents of the module, including all hardware, firmware, and data are enclosed in the Horizon Quantum and Horizon Compact+ chassis. All physical components are made of production-grade materials, and all integrated circuits (ICs) in the module are coated with commercial standard passivation.

All keys, intermediate values, and other CSPs remain in the process space of a single operator. The operating system protects memory and process space from unauthorized access. No non-cryptographic processes may interrupt the module during execution.

2.6 Operational Environment

The DragonWave® Secure Cryptographic Module firmware operates on QNX Neutrino RTOS 6.4.1. For purposes of this evaluation, QNX is considered to be a limited operating environment. The system firmware is embedded within a Flash ROM. All services are provided through well-defined APIs and CLIs, and shell access is disabled. No methods exist to call into the module from any ports/interfaces other than those defined in this security policy. Furthermore, no firmware applications other than the defined calling application have been designed to interface with the module.

The module's AES acceleration hardware is wholly implemented within the FPGA. All cryptographic status and control interfaces are directed through the firmware portion of the module.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 8 below.

Table 8 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES–CFB[29]128 bit mode for 128, 192, and 256 bit key sizes (HW)	2707, 2709
AES–CBC[30] for 128, 192, and 256 bit key sizes	2706, 2708
TDES–CBC for keying option 1	1625, 1626
RSA PKCS[31]#1 v1.5 and PSS[32] signature generation/verification, keywrap – 2048, 3072, 4096 bit key sizes	1404, 1405
SHA-1, SHA-256	2273, 2274
HMAC-SHA-1	1687, 1688
ANSI[33] x9.31 Appendix A.2.4 Pseudo Random Number Generator	1256, 1257
TLS 1.0 Key Derivation Function (KDF)[34]	Component Validation: 164, 165

Caveat: Additional information concerning SHA-1, DH, and RSA and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

[29] *CFB: Cipher Feedback*
[30] *CBC: Cipher Block Chaining*
[31] *PKCS: Public Key Cryptography Standard*
[32] *PSS: Probabilistic Signature Scheme*
[33] *ANSI: American National Standards Institute*
[34] *Note: The TLS protocol has not been reviewed or tested by the CAVP and CMVP.*

The module includes the non-compliant cryptographic algorithms and services listed in Table 9 below, which are included in the module's cryptographic library. However, their use is strictly prohibited while operating in the FIPS-approved mode of operation. The use of these algorithms and services leads the module to operate in the non-Approved mode. These algorithms cannot be used with any of the services listed in Table 5, Table 6, and Table 7.

Table 9 – Non-Compliant Algorithms and Services

Algorithm	Non-Compliant Service
DSA[35]	Asymmetric Key Generation Digital Signature Generation
AES (ECB[36], OFB[37], CFB1, CFB8)	Encryption Decryption
Triple-DES (ECB, CFB, OFB)	Encryption Decryption
SHA-224, SHA-384, SHA-512	Digital Signature Generation
HMAC-SHA-224, HMAC-SHA-384, HMAC-SHA-512	Message Authentication
RSA GenKey 9.31	Digital Key Generation (key sizes <2048)
RSA SigGen 9.31	Digital Signature Generation (key sizes <2048)
RSA SigVer 9.31	Digital Signature Verification

The module employs the following key establishment methodology, which is allowed for use in a FIPS-Approved mode of operation:

- Diffie-Hellman (2048-bit keys; key agreement; key establishment methodology provides 112 bits of encryption strength)
- RSA (2048-, 3072- and 4096-bit keys; key wrapping; key establishment methodology provides 112 to 150 bits of encryption strength)

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

- MD5[38] within TLS only

The module supports the critical security parameters (CSPs) listed below in Table 10.

[35] *DSA: Digital Signature Algorithm*
[36] *ECB: Electronic Codebook*
[37] *OFB: Output Feedback*
[38] *MD5: Message Digest 5*

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key Type	Generation[39] / Input	Output	Storage	Zeroization	Use
AES Key (FPGA)	AES (128, 192, 256 bit key)	API call parameter	API call parameter (key is obfuscated with SHA-256)	Plaintext in volatile memory	By API call, power cycle, or reboot	Keys are passed as arguments to the module API, and output as API return data.
AES Key (TLS)	AES (128, 192, 256 bit key)	Internally generated	Never	Plaintext in volatile memory	Power cycle, reboot or after the API service is terminated	Keys are passed as arguments to the module API for cryptographic processing within the TLS protocol, and returned via API to the calling application
TDES Keys (TLS)	TDES (168 bit key)	Internally generated	Never	Plaintext in volatile memory	Power cycle, reboot or after the API service is terminated	Keys are passed to the module API for cryptographic processing within the TLS protocol.
HMAC Key (TLS)	HMAC (112 bit key)	Internally generated	Never	Plaintext in volatile memory	Power cycle, reboot or after the API service is terminated	Used for Keyed-Hash Message Authentication in the TLS protocol
CRC32 integrity checksums	CRC32 value	Hard-coded in the module	Never	Hard coded in the module in plaintext	N/A	Firmware integrity check
DH Domain Parameters	Values p and q	API call parameter	API call parameter	Plaintext in volatile memory	N/A	Used by module for DH auto key generation

[39] The module uses Scenario 1 of IG 7.8 during key generation.

Key/CSP	Key Type	Generation[39] / Input	Output	Storage	Zeroization	Use
DH Public Key	2048-bit key	Internally generated	API call parameter	Plaintext in volatile memory	Power cycle, reboot, or after the API service is terminated	Used by module for DH auto key generation
DH Private Key	224-bit key	Internally generated	Never	Plaintext in volatile memory	Power cycle, reboot, or after the API service is terminated	Used by host application for DH auto key generation
RSA Private Key	RSA (2048-bit private key)	API call parameter	Never	Plaintext in volatile memory	Power cycle, reboot, or after the API service is terminated	Signature generation, decryption
RSA Public Key	RSA (2048-bit public key)	API call parameter	API call parameter	Plaintext in volatile memory	Power cycle, reboot, or after the API service is terminated	Signature verification, encryption
X9.31 RNG seed	128-bit value	Generated internally using nonce along with entropy input from an external NDRNG[40]	Never	Plaintext in volatile memory	Power cycle or reboot	FIPS-Approved random number generation
X9.31RNG seed key	AES 256-bit key	Imported from external NDRNG	Never	Plaintext in volatile memory	Power cycle or reboot	FIPS-Approved random number generation

The module implements the TLS v1.0 protocol for transferring AES bulk data encryption keys and API commands to partners, and SHA-256 hashes of the AES key and API commands to remote peers. Key establishment for the TLS protocol is performed using RSA key wrap. The TLS authentication key (HMAC SHA-1 key) and TLS session key (AES key) provide message authentication and confidentiality, respectively, to the TLS data. RSA key pairs enter the module via well-defined APIs in plaintext, whereas the TLS authentication key and TLS session key are generated internally using a FIPS-Approved ANSI X9.31 RNG. All of these ephemeral keys reside only on the volatile memory and are zeroized whenever power is cycled or after the TLS session is terminated, or if the calling application requires the zeroization API function.

[40] NDRNG – Non-deterministic random number generator

The module implements DH key agreement for the exchange of AES keys; domain parameters are input via API call. Public and private DH components are generated internally and reside in the module's non-volatile and volatile memory. Only the public components are exported via API call. The public and private DH components are zeroized when the module is power cycled or the API session is terminated. The DH-generated or manually-entered AES bulk data encryption key is input via API call and exported via API call to a partner over TLS. The AES key is stored in volatile memory, and is zeroized upon a host reboot or power cycle, or when the calling application requests the zeroization API function.

The module additionally offers a FIPS-Approved random number generation service. The random number generator uses the ANSI X9.31 seed, seed key, and Entropy Input string. The RNG seed and seed key are generated internally and reside only in volatile memory. To zeroize, the module needs to be power-cycled, or the API service must be dropped.

2.8 Self-Tests

The following sections detail the self-tests performed by the module at startup, on-demand, or conditionally, when required.

2.8.1 Power-Up Self-Tests

The DragonWave® Secure Cryptographic Module performs the following self-tests at power-up:

- Firmware integrity check
  - HMAC-SHA-1 integrity check against *fipscanister.o.*
  - 32-bit Error detection code (EDC) against *dwiCryptolib.so, dwiTransportlib.so,* and *dwiCryptodriverlib.so.*
  - 32-bit EDC against FPGA firmware image
- Known Answer Tests (KATs)
  - AES-CFB128 Encrypt KAT
  - AES-CFB128 Decrypt KAT
  - AES-CBC (256-bit) Encrypt KAT
  - AES-CBC (256-bit) Decrypt KAT
  - Triple-DES Encrypt KAT
  - Triple-DES Decrypt KAT
  - RSA Sign KAT (PKCS#1 SHA-1, SHA-256, 4096-bit modulus)
  - RSA Verify KAT (PKCS#1 SHA-1, SHA-256, 4096-bit modulus)
  - SHA-1 KAT
  - SHA-256 KAT
  - HMAC-SHA-1 KAT
  - ANSI X9.31 RNG KAT

All cryptographic data output is inhibited while the module is performing its power-up self-tests. The module only provides cryptographic services only after all tests have passed. The success or failure of each test is reported to the calling application, or may be displayed via serial console during startup, or written to a system dump[41]. If any of the tests fail, the module enters a self-test failure state and an alarm is generated. While the module is in this state, all cryptographic data output is inhibited.

2.8.2 Conditional Self-Tests

The DragonWave® Secure Cryptographic Module performs the following conditional self-tests:

- Continuous RNG Test (CRNGT) for ANSI X9.31 RNG
- CRNGT for non-deterministic RNG (NDRNG)

[41] *Note: The system dump does not include any plaintext keys/CSPs.*

- DH Pairwise Consistency Test (PCT)
- RSA PCT
- Manual key entry test (duplicate entry)
- Exclusive bypass test

If any of the conditional tests fail (except for manual key entry test), the module enters a self-test failure state and an alarm is generated. While in this state, all cryptographic data output is inhibited.

If the manual key entry test fails, the key is not programmed and the CO must re-enter the key.

2.8.3 Critical Functions Self-Tests

The DragonWave® Secure Cryptographic Module calculates an integrity checksum on configuration data using SHA-256, and writes the digest, along with the data to Flash storage. Upon retrieving the configuration data, the module verifies the digest on the configuration file to ensure file integrity. If this test fails, the module loads the configuration defaults. The success/failure of the test can be reported via the CO "status" command.

In addition, the module performs a conditional test which compares the configuration and keys between two peers or partners. The keys are hashed using SHA-256; the resulting hashes are compared. The module compares the values of the peer configuration (version, state information, etc.). If the required configuration values or key digests do not match, an appropriate mismatch alarm is raised and data output is inhibited until the alarm can be cleared.

2.9 Mitigation of Other Attacks

The module mitigates the threat of physical tampering through the use of operator-applied tamper-evident seals over the RJ-45 console port of the Horizon Quantum as well as on Horizon Compact+ enclosure.

2.9.1 Operator-applied Security Labels

The Horizon Quantum and Horizon Compact+ appliances are shipped with security labels (PN: 65-000185-01-01) that must be applied to the module's physical enclosure for proper FIPS operation. On the Horizon Quantum, the tamper-evident seal must be applied over the RJ-45 port (CNTL) starting on the top cover reaching down to the appliance baffling, as shown in Figure 9 below.

Figure 9 – Horizon Quantum Tamper-Evident Seal Placement

On the Horizon Compact+, the seal must be placed over the edge on one of the four sides where the front and rear housing meet, as shown in Figure 10 below:

Figure 10 – Horizon Compact+ Tamper-Evident Seal Placement

3 Secure Operation

The DragonWave® Secure Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Initial Setup

This document assumes that the Crypto Officer has performed initial setup of the outlier firmware and hardware (e.g., configuring radio band and frequency channels, IP address, and user accounts/passwords). This document also assumes that the module's parent hardware has been mounted appropriately and radio alignment procedures have been performed.

3.2 Management

This section details the CO guidance for initialization and management of the module.

3.2.1 Initialization

The module firmware boots up and performs self-tests automatically and without operator intervention through a default entry point implemented through a firmware constructor routine. After the FPGA has been programmed, the results of the FPGA integrity check are passed along with further instructions to the firmware portion of the module. Only after all required self-tests have passed may the module operate in either of its Approved modes.

The module provides two Approved modes of operation: Non-licensed and Licensed. The module does not implement a non-Approved mode. The module, when powered on for the first time, is in Non-licensed mode by default, and will remain in this mode until a feature license key is installed. In Non-licensed mode, the hardware encryptor is placed into bypass indefinitely and all network packets traversing the module are sent across the link in plaintext. Licensed mode requires that the Crypto Officer enter an appropriate Data Encryption feature license key obtained from DragonWave. This is achieved by following the steps in section 3.0, "Upgrade/Downgrade License Features" in Volume 2 of the respective Horizon Quantum or Horizon Compact+ product manuals[42]. Once a license for the Data Encryption feature has been entered, the CO may enable or disable bulk data encryption; disabling encryption sets the encryptor into bypass, while enabling encryption requires a manual key to be entered or auto-keygen to be enabled. In both Non-licensed and Licensed modes, the module provides the firmware-based cryptographic services necessary to support TLS communication between peer and partner devices. Regardless of the mode, the self-tests are performed at power-on; switching between Non-licensed and Licensed mode requires that the module be rebooted to ensure that the required tests are run.

During initial configuration of the Horizon Compact+, the CO must configure the Enhanced Security environment option. This setting cannot be reversed without performing a full factory reset. This configuration option is not available in the Horizon Quantum.

Upon enabling Enhanced Security, the CO is required to change the *superuser* password. Passwords must be at least eight characters long and contain at least one of each: uppercase alpha, lowercase alpha, numeric character, and special character. Also, more than two repeated characters in a password are not allowed. Passwords are not visible to any user, and cannot be recovered if forgotten.

During initialization the module outputs the status of all of the module's self tests as defined in section 2.8.1 to the DragonWave CLI.

[42] *Please contact DragonWave to obtain a copy of the Horizon Quantum and Horizon Compact+ product manuals.*

Please refer to section 2.9.1 above for information on applying tamper-evident seals to the Quantum and Horizon Compact+ appliances.

3.2.2 Management

The Crypto Officer is responsible for making sure the module utilizes FIPS-Approved algorithms and key sizes. All RSA keys utilized by the module in the FIPS mode of operation must be 2048 bits or greater.

The Crypto Officer shall use the following DragonWave CLI commands defined in Table 11 below to control the module's operation:

Table 11 – Crypto Commands

Command	Description
Key	Enter hex string key of size 32, 48, or 64 characters long, and program this new key
Enable	Encrypt all over the air data
Disable	Stop encrypting all over the air data, allow user data to pass unencrypted (bypass)
Status	Displays the current status of the module.
Rekey	Change the rekeying interval of the module. Takes effect only after the next rekey.
Autokeygen	Change to Auto mode (run this from TxHigh Modem)
Activate	(In manual mode) Start using the newly written key. Run this from TxHigh (Active) modem only.
Help	Help command summary
Exit	Exit module
Quit	Exit module

3.2.3 Zeroization

The Crypto Officer may zeroize keys and CSPs using a zeroization API function call, by power cycling the module, or by issuing the *system reset* command.

3.3 User Guidance

The User is unable to determine the operational status of the module, and therefore has no control over whether the data being passed through it is being encrypted or not. This is all controlled by the CO. Therefore, there is no guidance for operators assuming the User role.

4 Acronyms

This section describes the acronyms.

Table 12 – Acronyms

Acronym	Definition
3G	Third Generation
ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CRC	Cyclic Redundancy Check
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DAC	Digital-to-Analog Converter
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Element Management System
FE	Fast Ethernet
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
GbE	Gigabit Ethernet
Gbps	Gigabits Per Second
HMAC	(Keyed-) Hash Message Authentication Code
HP	High Power
IC	Integrated Circuit
IF	Intermediate Frequency
IG	Implementation Guidance
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
KAT	Known Answer Test

Acronym	Definition
KDF	Key Derivation Function
Mbps	Megabits Per Second
MTTR	Mean-Time-To-Repair
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OFB	Output Feedback
OS	Operating System
PCT	Pairwise Consistency Test
PSS	Probabilistic Signature Scheme
PWB	Printed Wiring Board
PonE	Power On Ethernet
QM	Quadrature Modulation
RF	Radio Frequency
RGMII	Reduced Gigabit Media-Independent Interface
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TXH	Transmit High (TxHigh)
TXL	Transmit Low (TxLow)

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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