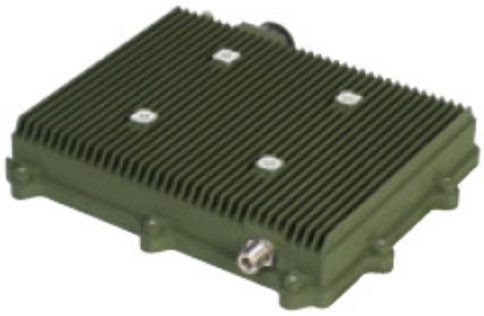
Harris Corporation
RF-7800W Broadband Ethernet Radio

(Hardware Version: RF-7800W, Firmware Versions: 4.00.072, 4.10.039, 13.00.127 and 13.01.129)



FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 2.2

Prepared for:

Harris Corporation,
RF Communications Division
1680 University Avenue
Rochester, NY 14610
Phone: (585) 244-5830
Fax: (585) 242-4755
http://www.harris.com

Prepared by:

Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Table of Contents

1 INTRODUCTION 3
1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 DOCUMENT ORGANIZATION 3
2 HARRIS CORPORATION RF-7800W BROADBAND ETHERNET RADIO 4
2.1 OVERVIEW 4
2.2 MODULE INTERFACES 5
2.3 ROLES AND SERVICES 6
2.3.1 Crypto-Officer Role 6
2.3.2 User Role 8
2.3.3 Bypass Mode 9
2.3.4 Authentication Mechanisms 9
2.4 PHYSICAL SECURITY 9
2.5 OPERATIONAL ENVIRONMENT 10
2.6 CRYPTOGRAPHIC KEY MANAGEMENT 10
2.7 ELECTROMAGNETIC INTERFERENCE / ELECTROMAGNETIC COMPATIBILITY 13
2.8 SELF-TESTS 13
2.9 MITIGATION OF OTHER ATTACKS 14
3 SECURE OPERATION 15
3.1 CRYPTO-OFFICER GUIDANCE 15
3.1.1 Initialization 15
3.1.2 Management 15
3.2 USER GUIDANCE 16
4 ACRONYMS 17

Table of Figures

FIGURE 1 – HARRIS RF-7800W BROADBAND ETHERNET RADIO 4
FIGURE 2 – TAMPER-EVIDENT LABEL LOCATIONS FOR RF-7800W 10

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 5
TABLE 2 – FIPS 140-2 LOGICAL INTERFACES 5
TABLE 3 – MAPPING OF CRYPTO-OFFICER ROLE'S SERVICES TO CSPS AND TYPE OF ACCESS 6
TABLE 4 – MAPPING OF USER ROLE'S SERVICES TO CSPS AND TYPE OF ACCESS 8
TABLE 5 – AUTHENTICATION MECHANISMS EMPLOYED BY THE MODULE 9
TABLE 6 – CERTIFICATE NUMBERS FOR CRYPTOGRAPHIC ALGORITHM IMPLEMENTATIONS 10
TABLE 7 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 11
TABLE 8 – ACRONYMS 17

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Harris Corporation's RF-7800W Broadband Ethernet Radio (running firmware version 4.00.072, 4.10.039, 13.00.127 or 13.01.129). This Security Policy describes how the RF-7800W Broadband Ethernet Radio meets the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) requirements for cryptographic modules as specified in Federal Information Processing Standards Publication (FIPS) 140-2. This document also describes how to run the module in its Approved FIPS 140-2 mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

The Harris RF-7800W Broadband Ethernet Radio running firmware version 4.00.072, 4.10.039, 13.00.127 or 13.01.129 is referred to in this document as the RF-7800W, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Harris website (http://www.harris.com/) contains information on the full line of products from Harris.
- The National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website (http://csrc.nist.gov/cryptval/) contains information about the FIPS 140-2 standard and validation program. It also lists contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Submission Summary
- Other supporting documentation as additional references

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

2 Harris Corporation RF-7800W Broadband Ethernet Radio

2.1 Overview

The RF-7800W Broadband Ethernet Radio by Harris Corporation leverages proven orthogonal frequency-division multiplexing (OFDM) technology to deliver high-speed Ethernet throughput over wireless links. Under clear line-of-sight conditions, the RF-7800W can provide robust, long-range connectivity at distances beyond 50 kilometers. The all-Internet Protocol (IP) design of the RF-7800W delivers a seamless extension of Ethernet local area networks and wide area networks, at proven Ethernet data rates greater than 80 Mbps[1]. The RF-7800W provides unmatched spectral flexibility with support for four different channel sizes (5, 10, 20, and 40 MHz[2]) in Point-to-Point (PTP) mode and three different channel sizes (5, 10, and 20 MHz) in Point-to-Multipoint (PMP) mode, and center frequency specification in 1 MHz increments (2.5 MHz increments in FCC[3] Part 90 compliant configurations). Extremely low latency in PTP (less than 4 ms[4]), and PMP (less than 10 ms) ensures the successful delivery of bandwidth-intensive applications such as Voice-over-IP (VoIP), real time video, teleconferencing, and C4I. Designed for the harshest outdoor conditions, the radio receives Direct Current (DC) Power Over Ethernet (POE) from the indoor unit via standard CAT[5]-5 Ethernet cable.

Operating over the 4.4–5.0 GHz[6] frequency band, covering the 4.94–4.99 GHz Public Safety band, the RF-7800W can be considered for wireless networking solutions such as public safety, first responders, training and simulation networks, and long/short-haul battlefield communications connectivity. Transmissions can be secured via the embedded encryption capability or via external Ethernet Inline Network Encryption (INE) devices.

The lightweight RF-7800W is easy to configure and deploy. Using a standard Web browser, an operator has access to all required configuration items and statistics necessary to configure and monitor the operation of the radio. Third-party network management applications can also be utilized via the standard Simple Network Management Protocol (SNMP) interface. Although SNMPv3 can support AES encryption in CFB mode, it does not utilize a FIPS-Approved key generation method; therefore, the module firmware has been designed to block the ability to view or alter critical security parameters (CSPs) through this interface. Also note that the SNMPv3 interface is a management interface for the Harris devices and that no CSPs or user data are transmitted over this interface.

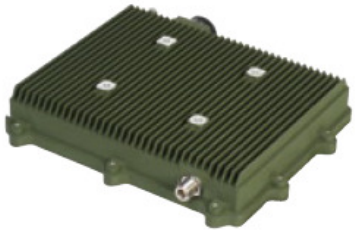


Figure 1 – Harris RF-7800W Broadband Ethernet Radio

The RF-7800W is validated at the FIPS 140-2 section Levels shown in Table 1 below.

[1] Mbps – megabits per second
[2] MHz – megahertz
[3] FCC – Federal Communications Commission
[4] ms – milliseconds
[5] CAT – category
[6] GHz – gigahertz

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	Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)	3
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Interfaces

The RF-7800W is a multi-chip standalone cryptographic module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the RF-7800W is defined by the aluminum case, which surrounds all the hardware and software components. Interfaces on the module can be categorized into the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

Ports on the module can be categorized into the following FIPS 140-2 physical interfaces:

- Ethernet port
- RF port
- Buzzer

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 Interfaces

FIPS 140-2 Logical Interface	Module Port/Interface
Data Input	Ethernet port, RF port
Data Output	Ethernet port, RF port
Control Input	Ethernet port, RF port
Status Output	Ethernet port, buzzer
Power	Ethernet port

2.3 Roles and Services

The module supports role-based authentication. There are two roles in the module that operators may assume: a Crypto-Officer role and a User role.

2.3.1 Crypto-Officer Role

The Crypto-Officer performs administrative services for the module, such as initialization, configuration, and monitoring of the module. Before accessing the module for any administrative service, the operator must authenticate to the module. The module offers three management interfaces:

- Web Interface
- Command Line Interface (CLI)
- SNMPv3 (Non-FIPS Mode)

The Web Interface is Harris's proprietary web-based GUI[7] that can be accessed via the local network using a web browser. The Web Interface serves as the primary management tool for the module. All Web Interface sessions with the module are protected over a secure TLS channel. Authentication of the CO requires the input of a username and password which is checked against a local password database and /or RADIUS server.

The CLI is accessed via the Ethernet port using a Secure Shell (SSH) session. Authentication of the CO on the CLI requires the input of a username and password.

Descriptions of the services available to the Crypto-Officer role are provided in the table below. The services listed for the Crypto-Officer role are mapped to relevant CSPs and the type of access required to CSPs associated with the service (Execute, Read, or Write).

Table 3 – Mapping of Crypto-Officer Role's Services to CSPs and Type of Access

Service	Description	CSP	Type of Access
Key Agreement	Used to establish keys for setting up a secure communications tunnel	Authentication Keys, TLS Key Agreement Keys, TLS Session Authentication Key, TLS Session Key, SSH Key Agreement Keys, SSH Session Authentication Key, SSH Session Key	Execute
Authenticate	Used to log in to the module	Administrator Password	Execute
Enable FIPS Mode	Allows Crypto-Officer to configure the module for FIPS Mode.	None	None
Configure Bypass mode	Allows Crypto-Officer to turn off encryption and go into bypass mode.	None	None

[7] GUI – Graphical User Interface

Service	Description	CSP	Type of Access
Encryption	Allows the Crypto Officer to enable encryption	TLS Session Authentication Key, TLS Session Key, SSH Session Authentication Key, SSH Session Key	Execute
Get FIPS Status	Allows Crypto-Officer to view general system identification and Configuration Settings.	None	None
Perform Self Tests	Allows the Crypto-Offficer to run on-demand self tests	None	None
System Status	Allows Crypto-Officer to view system, Ethernet, and wireless statistics.	None	None
System Log	Allows Crypto-Officer to view the system status messages.	None	None
Configure System	Allows Crypto-Officer to view and adjust configuration system, IP address, management, and wireless settings.	None	None
Upload Firmware	Allows Crypto-Officer to upload new software binary file	Harris Firmware Update Public Key	Execute
Add/Delete Operators	Allows Crypto-Officer to add/delete users	Administrator Passwords, User Passwords	Read/Write
Change Password	Modify existing login passwords	Administrator Passwords, User Passwords	Read/Write
Spectrum Sweep	Allows Crypto-Officer to scan radio frequencies to detect additional RF sources which could be a source of interference	None	None
Zeroize	Zeroize all keys and CSPs. When the command is issued all keys and CSPs will be erased from memory and replaced with “1”s.	All keys and CSPs	Write
Clear	Clears frequency list and log messages	None	None
Del	Deletes keys/certificates	Any specified key/certificate	Write
Freq	Used to enter the frequency ranges for autoscan and dynamic frequency selection	None	None
Generate	Creates new Diffie Hellman keys or DSA keys for use with SSH	Authentication Keys, Key Agreement Key	Write
Get	Displays statistic and parameter values	None	None
Load Cert	Loads new certificates	CA public keys	Execute
Load Script	Loads a script for backup. The config script contains a string of CLI commands that can be used to restore a previously exported configuration of the RF-7800W.	None	None
Ping	Ping utility	None	None

Service	Description	CSP	Type of Access
Reboot	Restarts the module	None	None
Reset Statistics	Resets the statistical values stored in the module	None	None
Save	Saves the selected configuration settings	None	None
Export Script	Generates and outputs a config script. The config script contains a string of CLI commands that can be used to restore the current (active) configuration of the RF-7800W.	None	None
Set	Displays system parameter values and allows modification to the displayed values	None	None
Show	Displays configuration and additional system compound objects	None	None
Test Config	Allows configuration changes to be run for a five minute test period. During the test period the configuration changes can be saved. If they are not saved by the end of the test period the previously saved settings are reloaded.	None	None

2.3.2 User Role

The User has the ability to view general status information about the module, and utilize the module's data transmitting functionalities via the Ethernet port. Descriptions of the services available to the User role are provided in the table below. The services listed for the User role are mapped to relevant CSPs and the type of access required to CSPs associated with the service (Execute, Read, or Write).

Table 4 – Mapping of User Role's Services to CSPs and Type of Access

Service	Description	CSP	Type of Access
Key Agreement	Used to establish keys for setting up a secure communications tunnel	Authentication Keys, TLS Key Agreement Keys, TLS Session Authentication Key, TLS Session Key, SSH Key Agreement Keys, SSH Session Authentication Key, SSH Session Key	Execute
Authenticate	Used to log in to the module	User Password	Execute
General Information	Allows Users to view general system identification and Configuration Settings.	None	None
System Status	Allows Users to view system, Ethernet, and wireless statistics.	None	None
System Log	Allows Users to view the system status messages.	None	None
Change Password	Allows Users to change login password	User Password	Read/Write

2.3.3 Bypass Mode

The cryptographic module supports an exclusive bypass capability by allowing the encryption type configuration parameter to be set to NONE, AES 128, AES 192, and AES 256. When encryption is enabled, no Ethernet packets are allowed to be transferred over-the-air in plaintext. The Crypto-Officer can determine the bypass status by examining the wireless encryption status with the web interface and CLI. If wireless encryption is enabled, then bypass capability is not activated; if wireless encryption is disabled, then bypass is activated.

2.3.4 Authentication Mechanisms

The module employs the following authentication methods to authenticate Crypto-Officers and Users. Passwords are used for authenticating with the RF-7800W and certificates are used when establishing a TLS session.

Table 5 – Authentication Mechanisms Employed by the Module

Type of Authentication	Authentication Strength
Password	Passwords are required to be at least 8 characters long. Alphabetic (uppercase and lowercase), numeric, and special characters can be used, which gives a total of 94 characters to choose from. With the possibility of repeating characters, the chance of a random attempt falsely succeeding is 1 in 94^8, or 1 in 6,095,689,385,410,816. MD5 hashes are used for authentication via RADIUS. MD5 hashes are typically represented as 32-digit hexadecimal values. The chance of a random authentication attempt falsely succeeding is 1 in 16^{32}, or 1 in 3.4028×10^{38}.
Certificate	Certificates used as part of TLS are (at a minimum) 1024 bits. The chance of a random attempt falsely succeeding is 1 in 2^{80}, or 1 in 1.2089×10^{24}.

2.4 Physical Security

The Harris RF-7800W is a multi-chip standalone cryptographic module. The module is enclosed in a weatherproof aluminum alloy case, which is defined as the cryptographic boundary of the module. The module's enclosure is opaque within the visible spectrum. The module's enclosure is sealed using tamper-evident labels, which prevent the case covers from being removed without signs of tampering.

It is the responsibility of the Crypto-Officer to ensure that both tamper-evident labels are properly placed on the module before use. The location of the tamper-evident labels is indicated with the red circles in Figure 2 below. Two tamper labels on opposite sides of the module will prevent unauthorized users from gaining undetected access, even if screws not covered by tamper labels are removed.

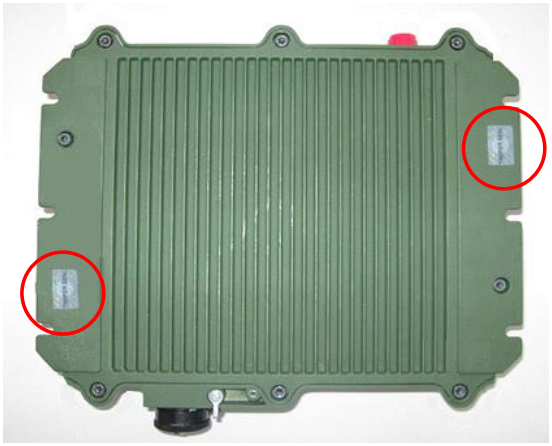


Figure 2 – Tamper-Evident Label Locations for RF-7800W

2.5 Operational Environment

The module does not provide a general purpose operating system nor does it allow operators to load untrusted software. The operating system (OS) employed by the modules is referred to as Wind River VxWorks version 6.5 OS. The OS is not modifiable by the operators of the modules, and only the modules' custom written image can be run in the system. The modules provide a method to update the firmware in the module with a new version. This method involves uploading a digitally signed firmware update to the module. If the signature test fails the new firmware will be ignored, and the current firmware will remain loaded. If the signature test passes the new firmware will be loaded and the Crypto-Officer is responsible to following the steps listed in Secure Operation to place the module in FIPS-approved mode of operation.

NOTE: In order to maintain validation for the module, only FIPS-validated firmware may be loaded, and it must be configured to execute in its defined FIPS mode of operation.

2.6 Cryptographic Key Management

The module implements the FIPS-Approved algorithms shown in Table 6 below.

Table 6 – Certificate Numbers for Cryptographic Algorithm Implementations

Approved Function	Certificate Number
Symmetric Key Algorithm	
Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CBC[8], ECB[9], CFB[10] modes	996
AES 128-, 192-, 256-bit in ECB, CCM[11] modes	930
Triple-DES[12] in CBC mode (2- and 3-key)	776
Secure Hashing Algorithm (SHA)	
SHA-1, SHA-256, SHA-384, and SHA-512	961

[8] CBC – Cipher-Block Chaining
[9] ECB – Electronic Codebook
[10] CFB – Cipher Feedback
[11] CCM – Counter with CBC-MAC
[12] DES – Data Encryption Standard

Approved Function	Certificate Number
Message Authentication Code (MAC) Function	
HMAC[13] using SHA-1, SHA-256, SHA-384, and SHA-512	561
Deterministic Random Bit Generator (DRBG)	
NIST[14] SP 800-90 DRBG[15]: Hash SHA-1 and Hash SHA-256	8
Asymmetric Key Algorithm	
RSA[16] PKCS[17]#1 sign/verify 1024, 1536, 2048-bit	479
Digital Signature Algorithm (DSA) sign/verify – 1024-bit	342

The module implements the following non-FIPS-Approved algorithm implementations:

- Diffie-Hellman 1024- and 2048-bits key (key agreement; key establishment methodology provides 80 and 112 bits of encryption strength, respectively)
- RSA 2048-bits key (key wrapping, key establishment methodology provides 112 bits of encryption strength)
- MD5

The module supports the following critical security parameters:

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key	AES 128-, 192-, 256-bit CFB key	Internally generated but not FIPS Compliant	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Provides secured channel for SNMPv3 management that is not FIPS-Approved.
Preshared Master Secret	AES 128-, 192-, 256-bit key	Externally generated	Never exits the module	Stored in non-volatile memory	Zeroize key	Provides confidentiality of management packets over wireless channel
Authentication public/private keys	RSA 1024-, 1536-, 2048-bit keys or DSA 1024-bit key	DSA keys are Internally generated and RSA keys are externally generated and imported in encrypted form	Public key exported electronically in plaintext via Ethernet port	Stored in non-volatile memory	By Zeroize command	Peer Authentication of SSH/TLS sessions

[13] HMAC – Hash Message Authentication Code
[14] NIST – National Institute of Standards and Technology
[15] DRBG – Deterministic Random Bit Generator
[16] RSA – Rivest, Shamir, and Adleman
[17] PKCS – Public Key Cryptography Standard

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Peer RSA/DSA public keys	RSA/DSA 1024-, 1536-, 2048-bit keys or DSA 1024-bit key	Imported electronically during handshake protocol	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Peer Authentication for SSH sessions
Local and CA[18] RSA public/private (local unit only) keys	RSA 1024-, 1536-, 2048-bit keys,	Externally generated and imported in encrypted form	Public key certificate exported electronically in plaintext via wireless port; private component not exported	Stored in non-volatile memory.	By Zeroize command	Establish trusted point in peer entity
SSH Key Agreement keys	Diffie-Hellman 1024-, 2048-bit exponents	Internally generated	Public exponent electronically in plaintext; private component not exported	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for SSH sessions as defined above in Section 0
TLS Key Agreement Keys	RSA 2048-bit key	Externally generated	Public exponent electronically in plaintext; private component not exported	Stored in volatile memory	Upon reboot or session termination	Key wrapping/establishment for TLS sessions as defined above in Section 0
TLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data authentication for TLS sessions
TLS Session Key	Triple-DES, AES-128, AES-192, AES-256	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data encryption for TLS sessions
SSH Session Authentication Key	HMAC-SHA1 key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data authentication for SSH sessions
SSH Session Key	Triple-DES, AES-128, AES-192, AES-256	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data encryption for SSH sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Harris Firmware Update Public Key	RSA 2048-bit public key	Externally generated and hard coded in the image	Never exits the module	Stored in non-volatile memory	Upon reboot or session termination	Verifies the signature associated with a broadband radio firmware update package
Administrator Passwords	8-character ASCII[19] string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By Zeroize command	Authentication for administrator login
User Passwords	8-character ASCII string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By Zeroize command	Authentication for user login
NIST SP 800-90 DRBG seed	256-byte random value	Internally generated	Never exits the module	Generated after reset. Stored in non-volatile memory	Overwritten (as a circular buffer) by random value	Used during FIPS-approved random number generation

2.7 Electromagnetic Interference / Electromagnetic Compatibility

The Harris RF-7800W was tested and found to be conformant to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by *Federal Communications Commission CFR*[20] *47, Parts 2 and 90 (Subpart Y) – Regulations Governing Licensing and Use of Frequencies in the 4940-4990 MHz Range*. Compliance with these regulations meets FIPS Level 3 requirements for EMI/EMC.

2.8 Self-Tests

The RF-7800W performs the following self-tests at power-up:

- Firmware integrity check using an Error Detection Code (16 bit CRC[21])
- Known Answer Tests (KATs) for the following FIPS-Approved algorithms:
  - AES
  - DSA
  - HMAC (SHA-1, SHA-256, SHA-384, SHA-512)
  - NIST SP 800-90 DRBG
  - RSA (2048 bit sign/verify)
  - SHA-1, SHA-256, SHA-384, SHA-512
  - Triple-DES

If any of the power-up tests fail, the module enters into a critical error state. An error message is logged in the System Log for the Crypto-Officer to review, and a CO must power cycle the module or reload the module image to clear the error state. A CO may initiate on demand self-tests by power cycling the module.

The RF-7800W also performs the following conditional self-tests:

- Continuous RNG Test for the NIST SP 800-90 DRBG

[19] ASCII – American Standard Code for Information Interchange
[20] CFR – Code of Federal Regulations
[21] CRC – Cyclic Redundancy Check

- DSA Pair-wise Consistency Test
- Bypass Test
- Firmware Load Test

If any of the above tests fail, the module enters a soft error state and logs an error message in the System Log.

2.9 Mitigation of Other Attacks

In a FIPS Mode of operation, the module does not claim to mitigate any additional attacks.

3 Secure Operation

The RF-7800W meets the Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for the initialization and management of the module. Please view the RF-7800W User Manual for additional information on configuring and maintaining the module. The Crypto-Officer can receive the module from the vendor via trusted delivery couriers including UPS, FedEx, and Roadway. The Crypto-Officer can also arrange for pick up directly from Harris.

Upon receipt of the module the Crypto-Officer should check the package for any irregular tears or openings. Upon opening the package the Crypto-Officer should inspect the tamper-evident labels. If the Crypto-Officer suspects tampering, he/she should immediately contact Harris.

3.1.1 Initialization

The Crypto-Officer is responsible for the Initialization of the module through the Web Interface. The Crypto-Officer must login to the module using the default username and password. Once initial authentication has completed, the Crypto-Officer must setup all Crypto-Officer and User accounts passwords (eight characters minimum) and verify via the System Configuration window that FIPS Mode is enabled. If FIPS Mode is disabled, the Crypto-Officer can enable it by performing the following steps:

1. Change the default Crypto-Officer password and default User password
2. Set the Encryption Type to None
3. Disable HTTP[22], SNMP, and Telnet
4. Enable HTTPS[23] and SSH
5. Turn FIPS Mode Flag to ON
6. Reboot
7. Load the Local RSA public/private keys and Authentication (RSA) public/private keys
8. Load the Certificate Authority's public key
9. Reboot
10. Enter the Pre-Shared Key
11. Set the Encryption Type to AES 128, AES 192 or AES 256
12. Enable wireless authentication and encryption

For additional initialization guidance, please reference the *Harris Network Administrator Manual*.

3.1.2 Management

The module can run in two different modes: FIPS-Approved for PTP connections and non-FIPS-Approved for PMP connections. In FIPS-Approved mode, only FIPS-Approved algorithms listed in Table 6 are used.

The Crypto-Officer is able to configure and monitor the module via the Web Interface over TLS and CLI over SSH. The Crypto-Officer should check the System Status and System Logs frequently for errors. If the same errors reoccur or the module ceases to function normally, then Harris customer support should be contacted.

The Crypto-Officer is able to switch between FIPS Mode and non-FIPS mode by changing the FIPS Mode Flag between ON and OFF. When the mode is changed to or from FIPS mode of operation, the files in memory are

[22] HTTP – Hypertext Transfer Protocol
[23] HTTPS – Secure Hypertext Transfer Protocol

replaced with “0”s and a reboot is forced. To prevent sharing of the FIPS mode keys in non FIPS mode or vice-versa there exists two different set of files, one for each mode. The one set that is not being used is not accessible to the user in any way.

3.2 User Guidance

The User role is able to access the module over the Ethernet port and perform basic services including: viewing general system status information and changing their own password. A list of commands available to the User role is found in Table 4. A user should check the system status information to confirm the FIPS mode flag is set to ON.

4 Acronyms

This section defines the acronyms used throughout this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BOM	Bill of Materials
CAPA	Corrective and Preventive Action
CAT	Category
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CFR	Code of Federal Regulations
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRC	Cyclic Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DC	Direct Current
DES	Digital Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GHz	Gigahertz
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol

Acronym	Definition
ID	Identification
INE	Inline Network Encryption
IP	Internet Protocol
KAT	Known Answer Test
MAC	Message Authentication Code
Mbps	Megabits per second
MHz	Megahertz
Ms	Milliseconds
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency-Division Multiplexing
OS	Operating System
PKCS	Public Key Cryptography Standard
PMP	Point-to-Multipoint
POE	Power Over Ethernet
PTP	Point-to-Point
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
VoIP	Voice-over-Internet Protocol
VSS	Visual SourceSafe