Harris Corporation
RF-7800W Integrated Radio/PA

(Hardware Versions: RF-7800W-RP50x, RF-7800W-RP47x; Firmware Version: 6.00)

FIPS 140-2
Harris RF-7800W Radio with High Power PA Non-Proprietary Security Policy

Level 2 Validation
Document Version 1.2

Harris Corporation,
Communication Systems
1680 University Avenue
Rochester, NY 14610
Phone: (585) 244-5830
Fax: (585) 242-4755
http://www.harris.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 Harris Corporation's RF-7800W Integrated Radio/PA (running firmware version 6.00). This Security Policy describes how the RF-7800W Integrated Radio/PA meets the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) 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 Integrated Radio/PA running firmware version 6.00 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 (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program) 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

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 Integrated Radio/PA

2.1 Overview

The RF-7800W Integrated Radio/PA 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 100 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 430 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 Point-to-Multipoint (PMP) mode, and center frequency specification in 0.5 MHz increments. Extremely low latency in PTP (less than 4 ms[3]), 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[4]-5 Ethernet cable.

Operating over the 4.4–5.875 GHz[5] 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 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 Integrated Radio/PA

The module is available in two different variants: RF-7800W-RP50x and RF-7800W-RP47x and two different colors: green (x=0) and tan (x=1).

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

Table 1 – RF-7800W Models and Features

Model / Feature	RF-7800W-RP50x	RF-7800W-RP47x
Frequency Band	4.4 – 5.875 GHz	4.4 – 5.0 GHz
Supported Channel Sizes	5, 10, 20, 40 MHz	5, 10, 20, 40 MHz
Supported Wireless Encryption	AES (128, 256)	AES (128, 256)
Data Smoothing,	Yes	Yes
Electronic Interference Mitigation (EIM),	Yes	Yes
X509 authentication,	Yes	Yes
Multi-Hop	Yes	Yes
GPS	Yes (optional)	Yes (optional)

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

Table 2 – 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)	2
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
- DC in port
- RF port (2 RF ports)
- GPS Antenna port
- Synchronization port
- Local console port (serial port)
- Accessories port
- Buzzer

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

Table 3 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Port/Interface
Data Input	Ethernet port, RF port, GPS Antenna port, synchronization port
Data Output	Ethernet port, RF port
Control Input	Ethernet port, RF port, console port
Status Output	Ethernet port, buzzer, console port, accessories port, synchronization port
Power	Ethernet port, DC in port

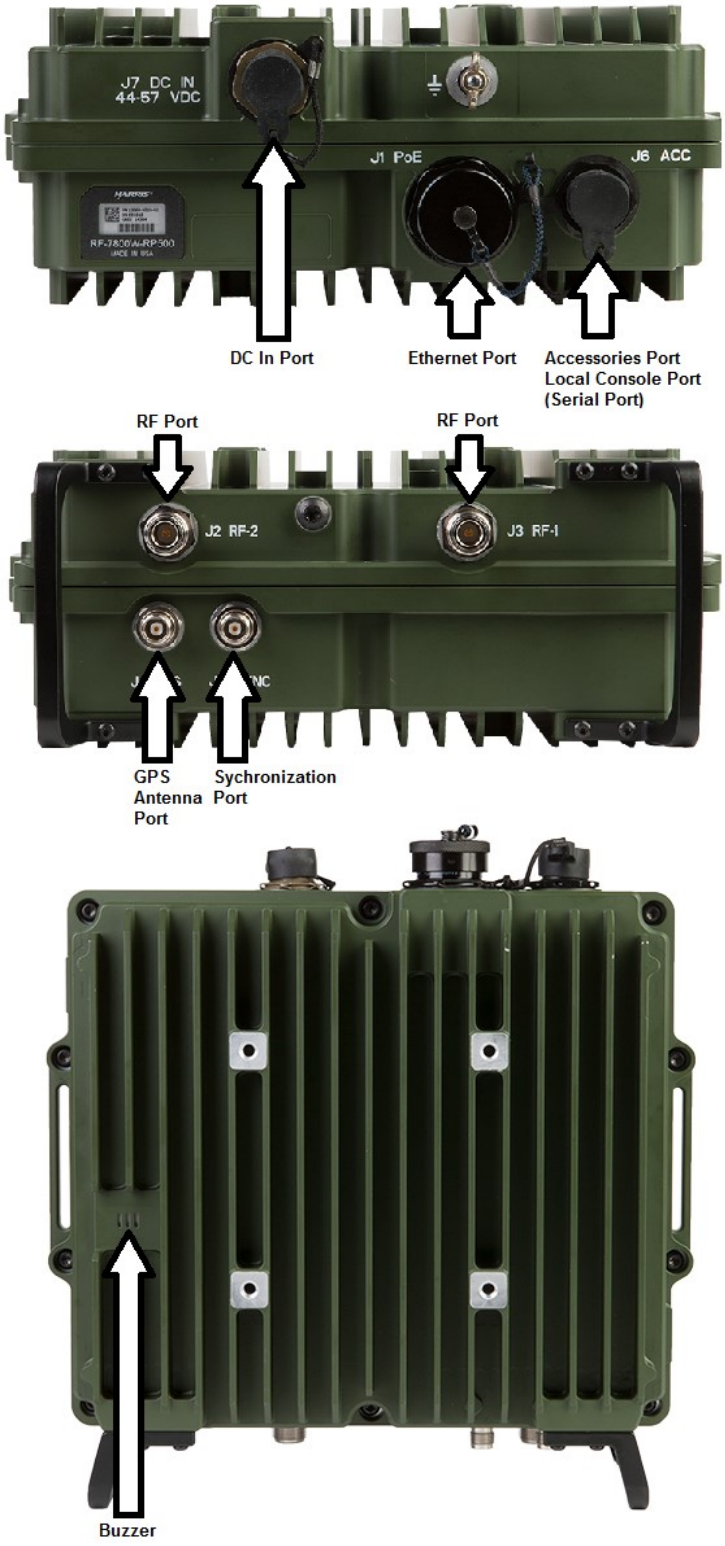

Figure 2 – Location of Physical Interfaces

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 ("Administrators" with full configuration access and "Users" with full access to all configuration parameters required for an installation including all CSPs) and a User role ("Monitor").

2.3.1 Crypto-Officer Role

The Crypto-Officer *("admin" and "user" type account)* 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

The Web Interface is Harris's proprietary web-based GUI[6] 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.

The CLI is accessed via the Ethernet port using a Secure Shell (SSH) session or via the local console port. Authentication of the CO on the CLI requires the input of a username and password. The system will drop the connection after three failed login attempts.

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 (X - Execute, R - Read, or W - Write).

Table 4 – Mapping of Crypto-Officer Role's Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Key Agreement	Used to establish keys for setting up a secure communications tunnel.	Local RSA public/private key (R/X), CA[7] RSA public key (R/X), Wireless Key Agreement Keys (R/W/X); Wireless session key encryption key (R/W) Wireless session key (R/W) TLS Key Agreement Key (R/W/X); TLS Session Authentication Key (R/W); TLS Session Key (R/W), Authentication public/private keys(R/X) SSH Key Agreement Key (R/W/X); SSH Session Authentication Key (R/W); SSH Session Key (R/W); Peer RSA/DSA public keys (R/W/X);
Authenticate	Used to log in to the module	Administrator Password (R/X) User Password (R/X);

[6] GUI – Graphical User Interface

[7] CA – Certification Authority

Service	Description	CSP and Type of Access
Enable FIPS mode	Allows Crypto-Officer to configure the module for FIPS mode.	None
Configure Bypass mode	Allows Crypto-Officer to toggle between encrypted modes and no encryption.	None
Encryption	Allows the crypto officer to enable encryption	Pre-shared Secret (R/X)
Get FIPS Status	Allows Crypto-Officer to view general System and Configuration parameters	None
Perform Self Tests	Allows Crypto-Officer to run on-demand self tests	None
View General Information	Allows Crypto-Officer to view general system identification and Configuration Settings.	None
View System Status	Allows Crypto-Officer to view system, Ethernet, and wireless statistics.	None
View System Log	Allows Crypto-Officer to view the system status messages.	None
Configure System	Allows Crypto-Officer to view and adjust configuration system, IP address, management, and wireless settings.	Pre-shared Secret (W)
Upload Firmware	Allows Crypto-Officer(administrators only) to upload new software binary file	Harris Firmware Update Public key (R/X)
User Management	Allows Crypto-Officer(administrator only) to add/delete users and modify existing login passwords.	Administrator Passwords (R/W); User Passwords (R/W); Monitor Passwords (R/W)
Spectrum Sweep	Allows Crypto-Officer to scan radio frequencies to detect additional RF sources which could be a source of interference	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 (W)
Clear	Clears commands	None
Del	Deletes an ID	None
Freq	Used to enter the frequency ranges for autoscan and dynamic frequency selection	None
Generate	Creates new RSA keys for wireless and https or RSA/DSA keys for use with SSH	SP 800-90A DRBG seed/V/C values(R/W/X) Local RSA public/private key (R/W), Authentication public/private keys(R/W)
Get	Displays statistic and parameter values	None
Load File	Initiate file download	Local RSA public/private key (W), CA[8] RSA public key (W), Authentication public/private keys(W)

[8] CA – Certification Authority

Service	Description	CSP and Type of Access
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
Ping	Ping utility	None
Reboot	Restarts the module	None
Reset	Resets the statistical values stored in the module	None
Save	Saves the selected configuration settings	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
Set	Displays system parameter values and allows modification to the displayed values	Pre-shared Secret (W)
Show	Displays configuration and additional system compound objects	None
Test	Allows configuration changes to be run for a five minute test period	None
Manage module via SNMPv3	Non security related monitoring and configuration by the CO using SNMPv3	snmpEngineId (R/W/X), SNMPv3 Session Key (R/W/X), Administrator Password (R/X); User Password (R/X);
Secure management	Allows Crypto-Officer to securely manage the module over SSH or HTTPS.	TLS Session Authentication Key (R/X); TLS Session Key (R/X), SSH Session Authentication Key (R/X); SSH Session Key (R/X);
Wireless Communication	Provides secure wireless communication between RF-7800W modules	Wireless management encryption key (R/W/X); Wireless session key (R/W/X); Wireless session key encryption key (R/W/X) SP 800-90A DRBG seed/V/C values(R/W/X)

2.3.2 User Role

The User (“monitor” type account) 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 (X - Execute, R - Read, or W - Write).

Table 5 – Mapping of User Role's Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Key Agreement	Used to establish keys for setting up a secure communications tunnel.	TLS Key Agreement Key (R/W/X); TLS Session Authentication Key (R/W); TLS Session Key (R/W), Authentication public/private keys(R/X) SSH Key Agreement Key (R/W/X); SSH Session Authentication Key (R/W); SSH Session Key (R/W); Peer RSA/DSA public keys (R/W/X);
Authenticate	Used to log in to the module	Monitor Password (R/X)
Access the Module via SNMPv3	Used to log in to the module using SNMP v3 protocol	snmpEngineId (R/X), SNMPv3 Session Key (R/W/X), Monitor Password (R/X)
General Information	Allows Users to view general system identification and Configuration Settings.	None
System Status	Allows Users to view system, Ethernet, and wireless statistics.	None
System Log	Allows Users to view the system status messages.	None
Get	Displays statistic and parameter values	None
Ping	Ping utility	None
Change Password	Allows Users to change login password	Monitor Password (R/W)
Secure management	Allows Users to securely manage the module over SSH or HTTPS.	TLS Session Authentication Key (R/X); TLS Session Key (R/X), SSH Session Authentication Key (R/X); SSH Session Key (R/X);

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, 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 6 – 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) and numeric characters can be used, which gives a total of 62 characters to choose from. With the possibility of repeating characters, the chance of a random attempt falsely succeeding is 1 in 62^8, or 1 in 218,340,105,584,896. The theoretical maximum number of attempts per minute is 750,000,000 therefore the chance of succeeding with multiple attempts in a one minute interval is 1 in 291,120.
Certificate	Certificates used as part of TLS or for wireless authentication in FIPS mode of operation are 2048 bits. The chance of a random attempt falsely succeeding is 1 in 2^{112}, or 1 in 5.1922968×10^{33}. The theoretical maximum number of attempts per minute is 29,296,875 therefore the chance of succeeding with multiple attempts in a one minute interval is 1 in $1,772,304 \times 10^{20}$.

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. There are multiple color variants:

- Green: RF-7800W-RPxx0
- Tan: RF-7800W-RPxx1

The module's enclosure is sealed using tamper-evident labels, which prevent the case from being opened without signs of tampering. All connectors are secured via structures internal to chassis which prevent them from being pulled out of or pushed into the chassis.

The location of the tamper-evident labels is indicated with the red circles 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. Although the tamper-evident labels are placed at the factory, it is the responsibility of the Crypto-Officer—during deployment or repositioning of the module—to ensure that both labels have not been tampered. In is also the responsibility of the Crypto-Officer to schedule and implement a periodic inspection routine to ensure that the tamper evident labels have not been breached.

Figure 3 – Tamper-Evident Label Locations for RF-7800W

2.5 Operational Environment

The operating system (OS) employed by the module is referred to as Wind River VxWorks version 6.8 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 7 below.

Table 7 – Certificate Numbers for Cryptographic Algorithm Implementations

Approved Security Function	Certificate Number
Symmetric Key – Encryption	
Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CBC[9], CFB128[10] modes	#5525
AES Key Wrap 256-bit	#5525
Advanced Encryption Standard (AES) 128-, 192-, 256-bit in ECB[11], CCM modes	#5526
Triple-DES[12] (3-key) in CBC mode	#2783
Asymmetric Key – Signature	
RSA[13] PKCS[14]#1 signature generation 2048-bit (FIPS 186-4)	#2963
RSA PKCS#1 signature verification 1024, 1536, 2048-bit (FIPS 186-2), 1024, 2048-bit (FIPS 186-4)	#2963
RSA Key Generation (2048-bit) (FIPS 186-4)	#2963
Digital Signature Algorithm (DSA) signature generation – 2048-bit	#1416
Digital Signature Algorithm (DSA) signature verification – 1024 / 2048-bit	#1416
Hashing	
Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512)	#4434

[9] CBC – Cipher-Block Chaining
[10] CFB – Cipher Feedback
[11] ECB – Electronic Codebook
[12] DES – Data Encryption Standard
[13] RSA – Rivest, Shamir, and Adleman
[14] PKCS – Public Key Cryptography Standard

Approved Security Function	Certificate Number
Message Authentication	
HMAC[15] using SHA-1, SHA-256, SHA-384, and SHA-512	#3679
Random Number Generators	
NIST[16] SP 800-90A DRBG[17]: Hash SHA-1 and Hash SHA-256	#2187
Key Agreement Schemes	
KAS (Diffie-Hellman)(Key establishment methodology provides 112 bits of encryption strength)	#187
Component	
Component Test (TLS (TLS1.0/1.1), SSH, SNMP)	#1969

Notes:

1. No parts of the TLS, SSH and SNMPv3 protocols, other than the key derivation functions, have been tested or reviewed by the CMVP or the CAVP.
2. KTS (AES Cert. #5525 and HMAC Cert. #3679; key establishment methodology provides between 128 and 256 bits of encryption strength).
3. KTS (Triple-DES Cert. #2783 and HMAC Cert. #3679; key establishment methodology provides 112 bits of encryption strength).

The module implements the following non-FIPS-Approved algorithms allowed in FIPS mode of operation:

- RSA 2048-bit key (key wrapping; key establishment methodology provides 112 bits of encryption strength).
- MD5 (for TLS use).
- NDRNG used as entropy source for the SP800-90A DRBG.

The module supports the following critical security parameters:

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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key	AES 128-bit CFB key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Provides secured channel for SNMPv3 management
snmpEngineID	SNMPv3 engine ID	Internally generated from the SNMP Enterprise OID and the MAC address	Exported electronically in encrypted form	Stored in volatile memory	Upon reboot	Unique ID of the SNMP v3 engine

[15] HMAC – Keyed-Hash Message Authentication Code
[16] NIST – National Institute of Standards and Technology
[17] DRBG – Deterministic Random Bit Generator

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Pre-shared Secret (key)	Shared secret	Externally generated and imported electronically in encrypted form or plaintext from a non-networked GPC[18].	Never exits the module	Stored in non-volatile memory.	Delete key	Used to derive the first KEK (key exchange) and MEK (management key)
Authentication public/private keys	RSA 2048-bit keys or DSA 2048-bit key	RSA/DSA keys are internally generated or externally generated and imported electronically into the module in encrypted form or plaintext from a non-networked GPC.	Public key exported electronically in plaintext via Ethernet or RF ports, private component not exported	Stored in non-volatile memory	By Zeroize command	Peer Authentication of SSH/TLS sessions
Peer RSA/DSA public keys	RSA/DSA 2048-bit keys	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[19] RSA public/private (local unit only) keys	RSA 2048-bit keys	Internally generated (local unit only) or externally generated and imported electronically into the module in encrypted form or plaintext from a non-networked GPC	Public key certificate exported electronically in plaintext via wireless or Ethernet port; private component not exported	Stored in non-volatile memory.	By Zeroize command	Establish trusted point in peer entity

[18] GPC – General Purpose Computer

[19] CA – Certification Authority

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Key Agreement keys	Diffie-Hellman 2048-bit public key, 256 bit private key	Internally generated	Public key exported electronically in plaintext; private key not exported	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for TLS sessions
SSH Key Agreement keys	Diffie-Hellman 2048-bit public key, 256 bit private key	Internally generated	Public key exported electronically in plaintext; private key not exported	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for SSH sessions
Wireless Key agreement keys	Diffie-Hellman 2048 bit public key, 256 bit private key	Internally generated	Public key exported electronically in plaintext, private key not exported	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for wireless link establishment
TLS Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Stored in plaintext in volatile memory	Upon reboot or session termination	Data authentication for TLS sessions
TLS Session Key	Triple-DES, AES-128, AES-256	Internally generated	Never exits the module	Stored in plaintext 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 plaintext 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 plaintext in volatile memory	Upon reboot or session termination	Data encryption for SSH sessions
Harris Firmware Update Public Key	RSA 2048-bit public key	Externally generated and hard coded in the image	Never exits the module	Stored in plaintext in non-volatile and volatile memory	N/A	Verifies the signature associated with a broadband radio firmware update package
Administrator Passwords	8-15 character ASCII[20] string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By password change command	Authentication for administrator login

[20] ASCII – American Standard Code for Information Interchange

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
User Passwords	8-15 character ASCII string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By password change command	Authentication for user login
Monitor Passwords	8-15 character ASCII string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By Zeroize command	Authentication for monitor login
NIST SP 800-90A DRBG seed	250 bytes random value	Internally generated	Never exits the module	Generated after reset. Stored in plaintext volatile memory	Overwritten (as a circular buffer) by random value	Used during FIPS-approved random number generation
NIST SP 800-90A DRBG "V" value	Internal DRBG state value	Internally generated	Never exits the module	Stored in plaintext volatile memory	Upon reboot or power cycle	Used during FIPS-approved random number generation
NIST SP 800-90A DRBG "C" value	Internal DRBG state value	Internally generated	Never exits the module	Stored in plaintext volatile memory	Upon reboot or power cycle	Used during FIPS-approved random number generation
Wireless management encryption key	AES 128-, 256-bit CCM key	Internally generated	Never exits the module	Stored in plaintext volatile memory	Upon reboot or power cycle	Used to encrypt the wireless control & management traffic
Wireless session key encryption key (KEK)	256-bit AES KW key	Internally generated	Exits the module in encrypted form during session establishment	Stored in plaintext volatile memory	Overwritten every time a new key is generated, by reboot or power cycle.	Used to encrypt wireless session keys
Wireless session key	AES 128-, 256-bit CCM key	Internally generated	Exits the module in encrypted form during session establishment	Stored in plaintext volatile memory	Overwritten every time a new key is generated, by reboot or power cycle.	Used to encrypt the user data traffic

The module performs key generation as per SP800-133 (vendor affirmed).

The module collects entropy from inside the module as per FIPS 140-2 IG 7.14 scenario 1(a) and provides a minimum of 1250 bits of entropy to the DRBG.

It is required that each validated module shall have a limit of 2^{16} encryptions with the same Triple-DES key. As Triple-DES encryption is used by the module only for management using SSH or HTTPS it is required that any management session that uses Triple-DES encryption to be limited to an interval of maximum 10 minutes.

It is recommended that all the RSA and DSA keys used be 2048 bits. Starting January 1st 2014 the following algorithms/key length combinations are disallowed or accepted only for legacy use:

- RSA1024

- SHA-1
- DSA1024

More information is available on the CMVP Web site (https://csrc.nist.gov/projects/cryptographic-module-validation-program).

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 47, Parts 2, 15, and 90 (Subpart Y) – Regulations Governing Licensing and Use of Frequencies in the 4940-4990 MHz Range. Compliance with these regulations meets FIPS Level 2 requirements for EMI/EMC.

2.8 Self-Tests

2.8.1 Power-Up 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 (encrypt - hardware)
  - AES (decrypt - hardware)
  - AES (encrypt - firmware)
  - AES (decrypt - firmware)
  - HMAC (SHA-1, SHA-256, SHA-384, SHA-512)
  - NIST SP 800-90A DRBG
  - RSA (signature generation and signature verification)
  - SHA-1, SHA-256, SHA-384, SHA-512
  - Triple-DES (encrypt)
  - Triple-DES (decrypt)
  - Diffie-Hellman Primitive "Z" Computation KAT
- Pair-wise Consistency Test:
  - DSA

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.

2.8.2 Conditional Self-Tests

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

- Continuous RNG Test for the NIST SP 800-90A DRBG
- Continuous RNG Test for the entropy source for the NIST SP 800-90A DRBG
- RSA Pair-wise Consistency Test
- DSA Pair-wise Consistency Test
- Bypass Test
- Firmware Load Test

[21] CRC – Cyclic Redundancy Check

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

2.8.3 Critical Functions Tests

The RF-7800W performs the following critical functions tests and it will enter an error state if any of these fail:

- SP800-90A DRBG Instantiate Test
- SP800-90A DRBG Generate Test
- SP800-90A DRBG Reseed Test

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.

The Module must be periodically inspected by the User for evidence of tampering. If tampering is suspected, the Crypto-Officer should assume that the module has been compromised, remove the unit from the network and contact Harris.

3.1.1 Initialization

The Crypto-Officer is responsible for the Initialization of the module through the Web Interface or CLI over SSH. The Crypto-Officer must log in to the module using the default username and password. Once initial authentication has completed, the Crypto-Officer must set up 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 ("admin" and "user" type account) password and default User ("monitor" type account) password. For a unit configured as an SC, change the STID password for all Link Templates. For a unit configured as an SS, change the STID password. The minimum password length is 8 characters and the maximum is 15 characters.
2. Make sure the Encryption Type is set to None
3. Disable HTTP[22], Telnet and RADIUS [23]
4. If SNMP is required, enable SNMPv3
5. Enable HTTPS[24] and SSH
6. Turn FIPS Mode Flag to ON
7. Save the configuration.
8. A reboot will be triggered by the step above. The reboot process can take a few minutes. A continuous "ping" can be used to determine when the unit is back up.
9. Log in using SSH or using the console port.
10. Load the Local RSA public/private keys (if X509 Authentication is used) and Authentication (RSA) public/private keys. Load the TLS certificate and private key if HTTPS will be used.
11. If X509 Authentication is used load the Certificate Authority's public key
12. Reboot (by issuing the "reboot" command)
13. Enter the Pre-Shared Secret. The pre-shared secret can have between 32 and 64 characters.
14. Set the Wireless Encryption Type to AES 128 or AES 256.
15. Enable X509 wireless authentication (optional).

[22] HTTP – Hypertext Transfer Protocol
[23] RADIUS - Remote Authentication Dial-In User Service
[24] HTTPS – Secure Hypertext Transfer Protocol

16. Check if the module is in FIPS mode using the "get fipsstatus" command (returns "ON" for FIPS mode).

For additional initialization guidance, please reference the "*Multimission HCLOS Installation/Operation Manual"*.

3.1.2 Management

In FIPS-Approved mode, only FIPS-Approved algorithms listed in Table 7 are used.

The Crypto-Officer ("admin" and "user" type account) is able to configure and monitor the module via the Web Interface over TLS and CLI over SSH or local console port. 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 appliance can be configured into an explicit FIPS mode of operation as per the instructions provided in Section 3.1.1. However, the appliance supports a non-compliant state, the initialization of which requires an explicit separate configuration. When the appliance is operating in non-compliant state, the services have access to non-Approved and non-Allowed algorithms. The logical boundary of the module is defined such that all functionality available in non-compliant state is scoped out from the module boundary. Thus, when the module is operating in FIPS Approved mode of operation, it can access only FIPS Approved or Allowed algorithms as access to non-Approved and non-Allowed algorithms are explicitly inhibited by design of the module.

The radio will be operating as a validated cryptographic module when all the steps to install, initialize and configure the radio are performed correctly. If the steps are not executed properly, the module will be operating outside the scope of the security policy and will not be operating as a validated cryptographic module.

For all zeroization operations the module is under the direct control of the Crypto Officer.

3.2 User Guidance

The User role ("monitor" type account) 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 5. 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 9 – 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
CSE	Communications Security Establishment
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
RADIUS	Remote Authentication Dial-In User Service
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