L3Harris Technologies, Inc.
RF-7800W Broadband Ethernet Radio

Hardware Versions:

RF-7800W-OU470, P/N: 12069-3000-01, Hardware P/N: 12069-3035-01, Version C
RF-7800W-OU471, P/N: 12069-3000-04, Hardware P/N: 12069-3035-02, Version C
RF-7800W-OU473, P/N: 12069-3000-08, Hardware P/N: 12069-3035-04, Version -
RF-7800W-OU492, P/N: 12069-3000-07, Hardware P/N: 12069-3035-03, Version C
RF-7800W-OU500, P/N: 12069-3000-03, Hardware P/N: 12069-3035-01, Version C
RF-7800W-OU501, P/N: 12069-3000-06, Hardware P/N: 12069-3035-02, Version C
RF-7800W-OU503, P/N: 12069-3000-09, Hardware P/N: 12069-3035-04, Version -
RF-7800W-RP470, P/N: 12069-5000-01, Hardware P/N: 12069-5010-01, Version C
RF-7800W-RP471, P/N: 12069-5000-02, Hardware P/N: 12069-5010-02, Version C
RF-7800W-RP473, P/N: 12069-5000-04, Hardware P/N: 12069-5010-04, Version C
RF-7800W-RP500, P/N: 12069-5000-21, Hardware P/N: 12069-5010-01, Version C
RF-7800W-RP501, P/N: 12069-5000-22, Hardware P/N: 12069-5010-02, Version C
RF-7800W-RP503, P/N: 12069-5000-24, Hardware P/N: 12069-5010-04, Version C

Firmware Version: 6.20

FIPS 140-2
L3Harris RF-7800W Radio Non-Proprietary Security Policy

Level 2 Validation
Document Version 2.0

L3Harris Technologies
Communication Systems
1680 University Avenue
Rochester, NY 14610
Phone: (585) 244-5830
Fax: (585) 242-4755
http://www.l3harris.com

THIS INFORMATION IS NOT EXPORT CONTROLLED

THIS INFORMATION IS APPROVED FOR RELEASE WITHOUT EXPORT RESTRICTIONS IN ACCORDANCE WITH A REVIEW OF THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR), 22CFR 120-130, AND THE EXPORT ADMINISTRATION REGULATIONS (EAR) 15 CFR 730-774.

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for L3Harris Technologies' RF-7800W Broadband Ethernet Radio (running firmware version 6.20). This Security Policy describes how the RF-7800W Broadband Ethernet Radio 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 L3Harris RF-7800W Broadband Ethernet Radio running firmware version 6.20 is referred to in this document as the RF-7800W, the cryptographic module, or the module.

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 L3Harris website (www.L3harris.com) contains information on the full line of products from L3Harris.
- 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.

1.2 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 L3Harris and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact L3Harris.

2 L3Harris Technologies RF-7800W Broadband Ethernet Radio

2.1 Overview

The RF-7800W Broadband Ethernet Radio by L3Harris Technologies 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 external Ethernet Inline Network Encryption (INE) devices.

The lightweight RF-7800W is easy to configure and deploy. Using a standard terminal application, 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 L3Harris devices and that no CSPs or user data are transmitted over this interface.

[1] Mbps – megabits per second

[2] MHz – megahertz

[3] ms – milliseconds

[4] CAT – category

[5] GHz – gigahertz

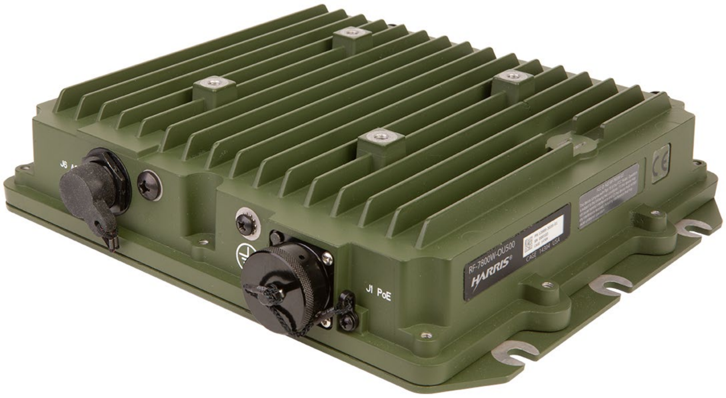

Figure 1 – L3Harris RF-7800W-OU Broadband Ethernet Radio

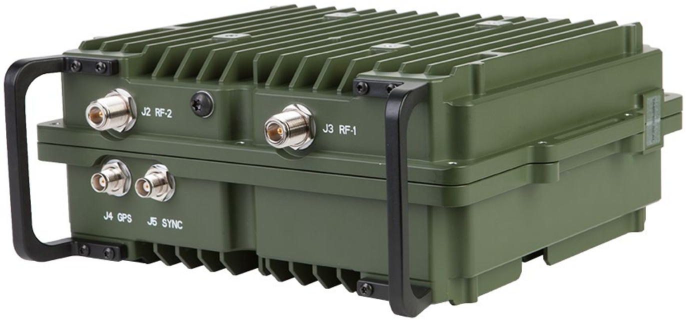

Figure 2 – L3Harris RF-7800W-RP Broadband Ethernet Radio

The module is available in the following variants:

Table 1 – RF-7800W Models

Model	Color	Part Number	Hardware Part Number	Hardware Part Number Revision
RF-7800W-OU470	Green	12069-3000-01	12069-3035-01	C
RF-7800W-OU471	Tan	12069-3000-04	12069-3035-02	C
RF-7800W-OU473	Gray	12069-3000-08	12069-3035-04	-
RF-7800W-OU492	White	12069-3000-07	12069-3035-03	C
RF-7800W-OU500	Green	12069-3000-03	12069-3035-01	C
RF-7800W-OU501	Tan	12069-3000-06	12069-3035-02	C
RF-7800W-OU503	Gray	12069-3000-09	12069-3035-04	-
RF-7800W-RP470	Green	12069-5000-01	12069-5010-01	C
RF-7800W-RP471	Tan	12069-5000-02	12069-5010-02	C
RF-7800W-RP473	Gray	12069-5000-04	12069-5010-04	C
RF-7800W-RP500	Green	12069-5000-21	12069-5010-01	C
RF-7800W-RP501	Tan	12069-5000-22	12069-5010-02	C
RF-7800W-RP503	Gray	12069-5000-24	12069-5010-04	C

Table 2 – RF-7800W Models and Features

Model / Feature	RF-7800W-OU50x and RF-7800W-RP50x	RF-7800W-OU47x and RF-7800W-RP47x	RF-7800W-OU49x
Frequency Band	4.4 – 5.875 GHz	4.4 – 5.0 GHz	5.150 – 5.875 GHz
Supported Channel Sizes	5, 10, 20, 40 MHz	5, 10, 20, 40 MHz	5, 10, 20, 40 MHz
Supported Wireless Encryption	AES (128, 256)	AES (128, 256)	AES (128, 256)
Data Smoothing	Yes	Yes	Yes (optional)
Electronic Interference Mitigation (EIM)	Yes	Yes	Yes (optional)
X509 authentication	Yes	Yes	Yes (optional)
Multi-Hop	Yes	Yes	Yes (optional)
GPS	Yes (optional)	Yes (optional)	Yes (optional)

The RF-7800W is validated at the FIPS 140-2 section Levels shown in Table 3 below.

Table 3 – 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
	Overall	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 (2 RF ports)
- GPS Antenna port
- Synchronization port
- Local console port (serial port)
- Accessories port
- Buzzer
- DC in port (only for the RF-7800W-RP models)

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

Table 4 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Port/Interface
Data Input	Ethernet port, RF port, GPS Antenna port, synchronization port, console port
Data Output	Ethernet port, RF port, console 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 (only RF-7800W-RP models)

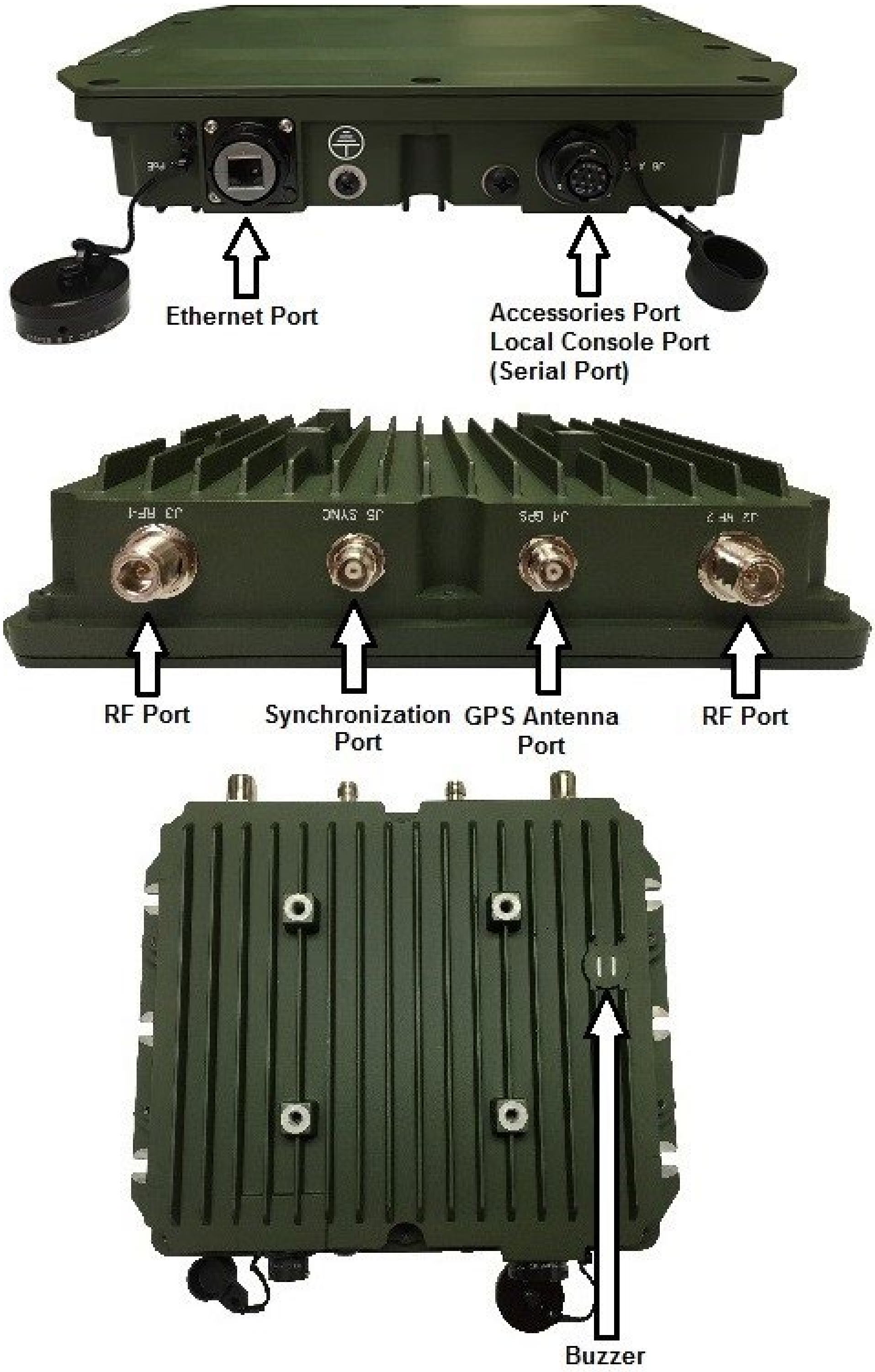

Figure 3 – Location of Physical Interfaces – RF-7800W-OU (12069-3035-xx)

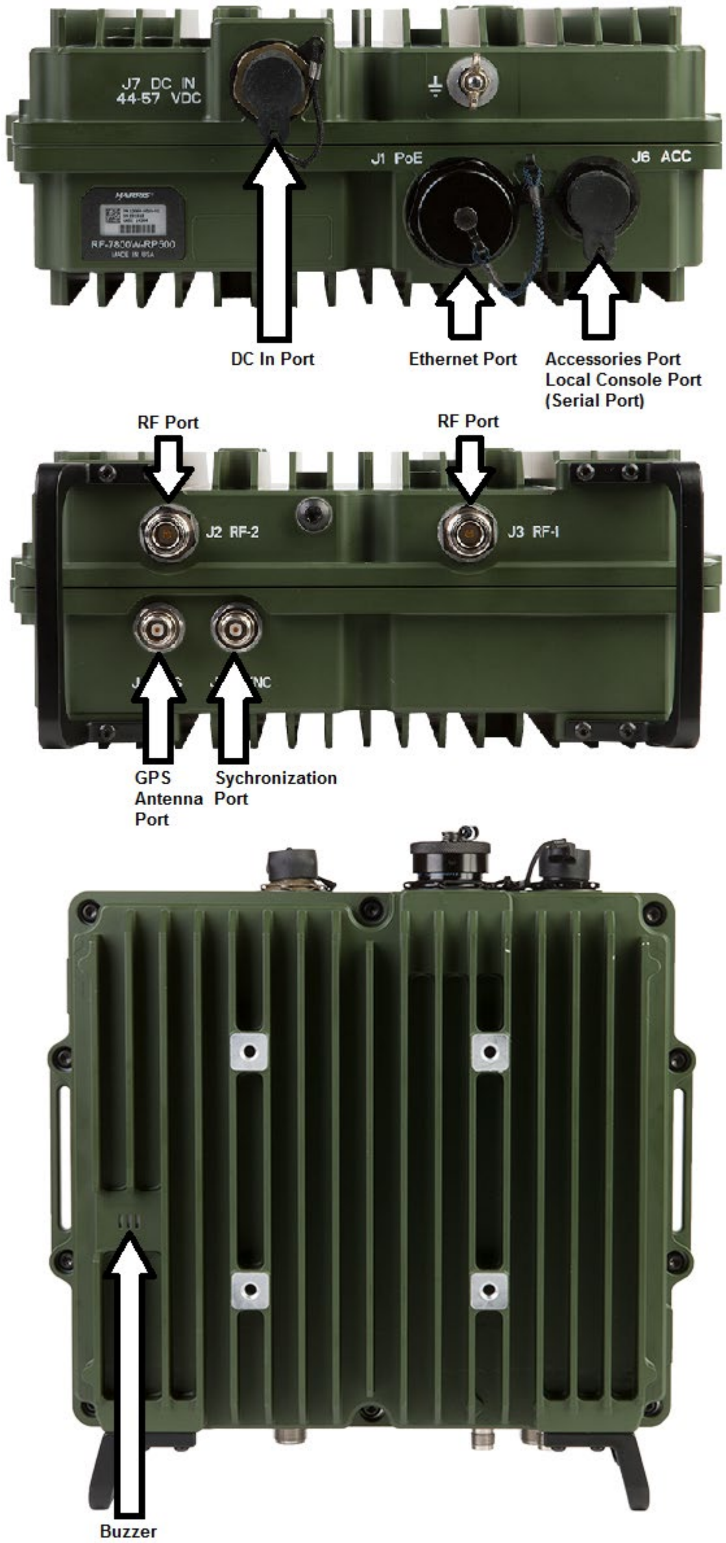

Figure 4 – Location of Physical Interfaces RF-7800W-RP (12069-5010-0x)

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").

When operating in non-FIPS mode the operators can use the following protocols for management:

- HTTP
- Telnet
- SNMPv2

Critical security parameters (CSPs) stored or used in FIPS mode are not used in non-FIPS mode and CSPs that are stored or used in non-FIPS mode are not used in FIPS mode.

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 L3Harris's proprietary web-based GUI[6] that can be accessed via the local network using a web browser. 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 which is checked against a local password database. The system will drop the connection after three failed login attempts. When connected using the local console the communication between the module and the terminal is in plaintext (IG7.7).

The SNMP agent is accessed via the Ethernet port using the SNMPv3 protocol. Each packet is encrypted and authenticated as specified by the SNMPv3 protocol.

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:

R – Read from internal memory
W – Write to internal memory
X – Performs a cryptographic operation with the CSP

[6] GUI – Graphical User Interface

Table 5 – 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);
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 firmware binary file	L3Harris Firmware Update Public key (R/X)

[7] CA – Certification Authority

Service	Description	CSP and Type of Access

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	Clear commands	None
Del	Deletes an ID	None
Freq	Used to enter the frequency ranges for autoscan and dynamic frequency selection	None
Generate	Generates 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 of cryptographic key/certificate file or language file	Local RSA public/private key (W), CA RSA public key (W), Authentication public/private keys(W)
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 (passwords and keys are not included in the configuration script).
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 (passwords and keys are not included in the configuration script).
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

Service	Description	CSP and Type of Access

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); TLS Key Agreement Private Key (R/W/X) TLS Key Agreement Public Key (R/W/X) SSH Key Agreement Private Key (R/W/X) SSH Key Agreement Public Key (R/W/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) Wireless Key Agreement Private Keys (R/W/X) Wireless Key Agreement Public Key (R/W/X) SP 800-90A DRBG seed/V/C values(R/W/X)

2.3.2 User Role

The User role (“Monitor”) has the ability to view general status information about the module, and utilize the module’s data transmitting functionalities via the Ethernet port using the web, CLI, or SNMP protocols or via local console using CLI. 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 6 – 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 SNMPv3 protocol	snmpEngineId (R/X), SNMPv3 Session Key (R/W/X), Monitor Password (R/X)
View General Information	Allows Users to view general system identification and Configuration Settings.	None
View System Status	Allows Users to view system, Ethernet, and wireless statistics.	None
View 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)
Show	Displays configuration and additional system compound objects	None

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 for the wireless interface by allowing the encryption type configuration parameter to be set to NONE, AES 128, and AES 256. The secure management (SSH, HTTPS, SNMPv3) does not provide a bypass capability. 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 and for wireless authentication of the peer module.

Table 7 – 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 x 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 x 10^{20}.

2.4 Physical Security

The L3Harris 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. All components are made of production-grade materials, and all ICs in the module are coated with commercial standard passivation.

The RF-7800W-OU radio has four color variants:

- Green: RF-7800W-OUxx0 (12069-3035-01)
- Tan: RF-7800W-OUxx1 (12069-3035-02)
- White: RF-7800W-OUxx2 (12069-3035-03)
- Grey: RF-7800W-OUxx3 (12069-3035-04)

The RF-7800W-RP radio has three color variants:

- Green: RF-7800W-RPxx0 (12069-5010-01)
- Tan: RF-7800W-RPxx1 (12069-5010-02)
- Grey: RF-7800W-RPxx3 (12069-5010-04)

The module's enclosure is sealed using tamper-evident seals, which prevent the case covers from being removed without signs of tampering. A tamper-evident pin (L3Harris part number H20-0027-309) affixes the Ethernet connector to the chassis and cannot be removed from the chassis without damaging the chassis and/or the Ethernet connector. Coaxial connectors (RF port, GPS Antenna port, and Synchronization port) are secured via structures internal to the chassis that prevent them from being pulled out of or pushed into the chassis.

The location of the tamper-evident seals is indicated with the red circles in Figure 5 to Figure 10 below. Two tamper seals on opposite sides of the module will prevent unauthorized users from gaining undetected access, even if screws not covered by tamper seals are removed. The location of the tamper-evident pin is indicated with the red circle in Figure 11 to Figure 13 below. Although the tamper-evident seals and pin are placed at the factory, it is the responsibility of the Crypto-Officer—during deployment or repositioning of the module—to ensure that both seals and the pin have not been tampered. It is also the responsibility of the Crypto-Officer to schedule and implement a periodic inspection routine to ensure that the tamper evident seals and pin have not been breached.

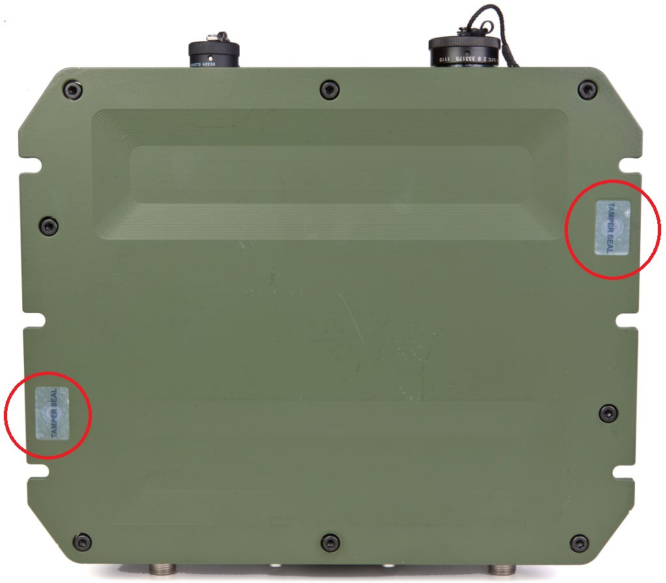

Figure 5 – Tamper-Evident Seal Locations for RF-7800W-OUxx0 (12069-3035-01)

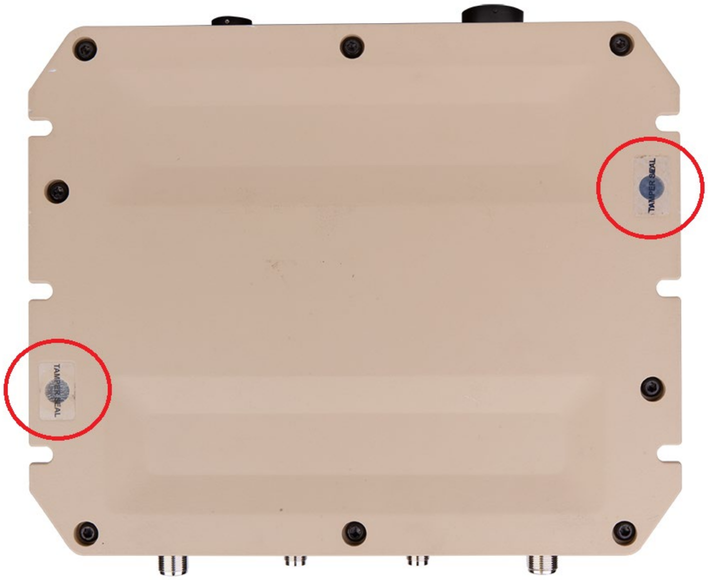

Figure 6 – Tamper-Evident Seal Locations for RF-7800W-OUxx1 (12069-3035-02)

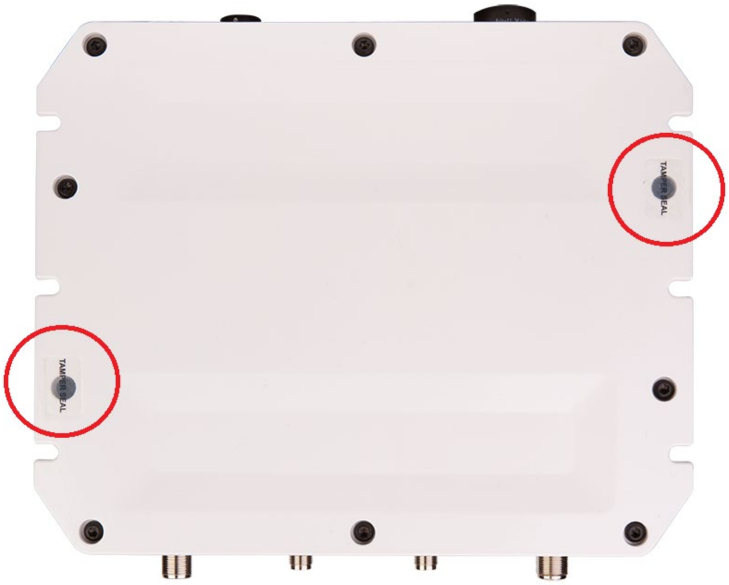

Figure 7 – Tamper-Evident Seal Locations for RF-7800W-OUxx2 (12069-3035-03)

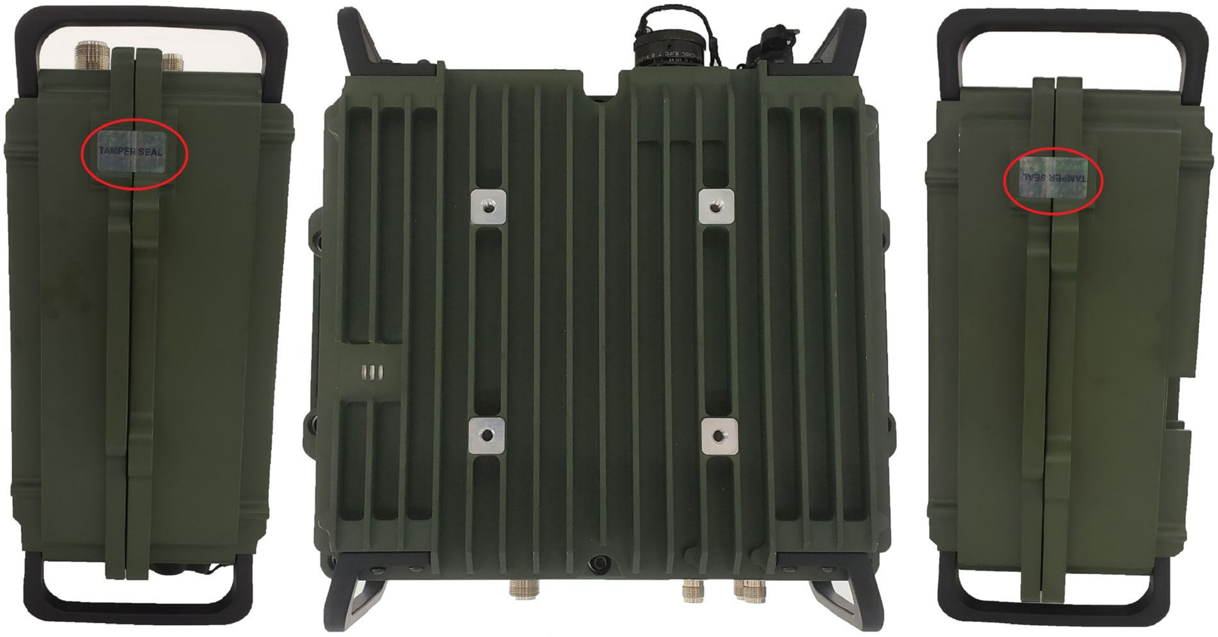

Figure 8 – Tamper-Evident Seal Locations for RF-7800W-RPxx0 (12069-5010-01)

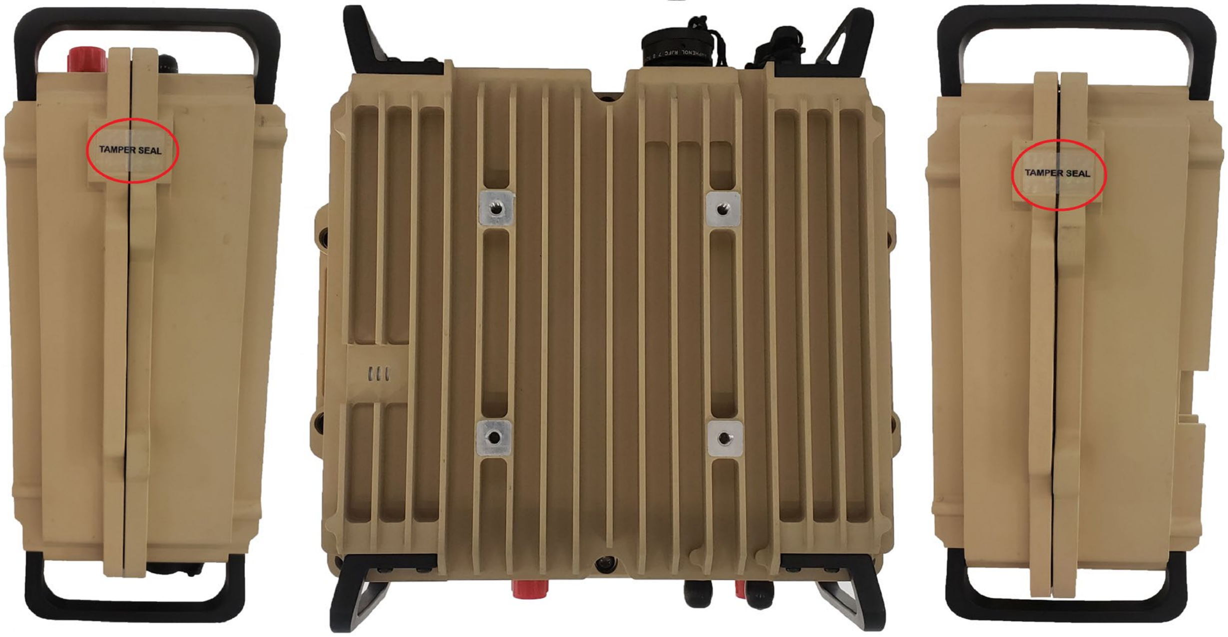

Figure 9 – Tamper-Evident Seal Locations for RF-7800W-RPxx1 (12069-5010-02)

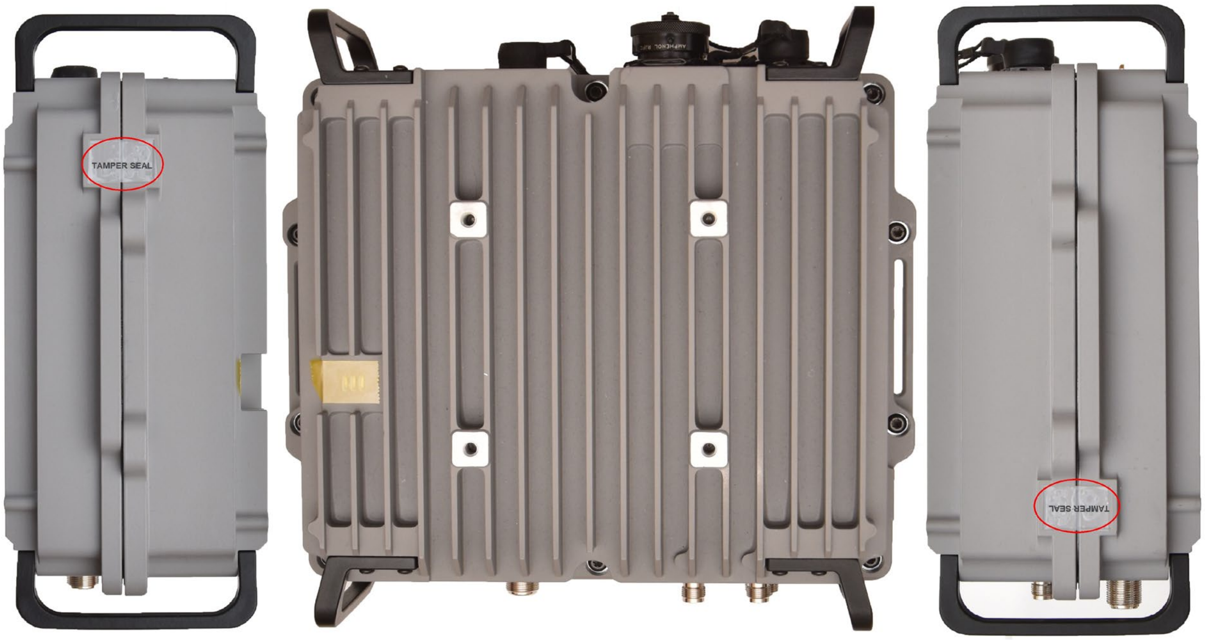

Figure 10 – Tamper-Evident Seal Locations for RF-7800W-RPxx3 (12069-5010-04)

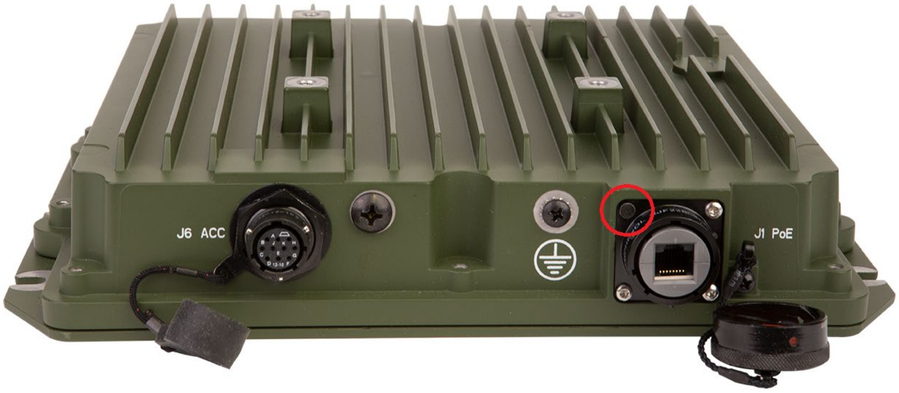

Figure 11 – Tamper-Evident Pin Location for RF-7800W-OUxx0 (12069-3035-01)

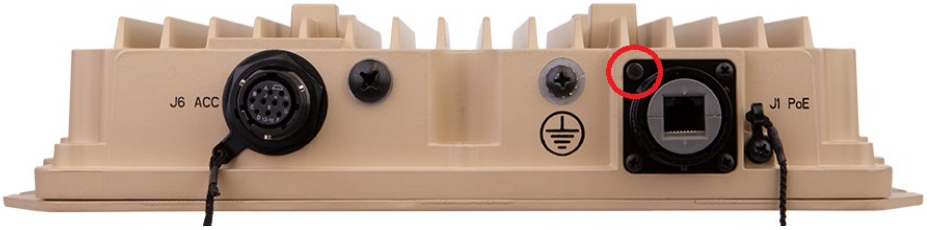

Figure 12 – Tamper-Evident Pin Location for RF-7800W-OUxx1 (12069-3035-02)

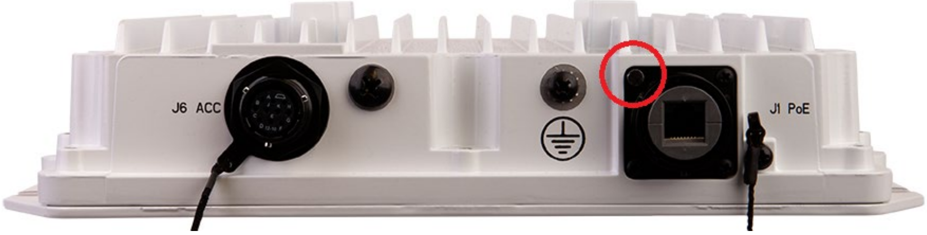

Figure 13 – Tamper-Evident Pin Location for RF-7800W-OUxx2 (12069-3035-03)

2.5 Operational Environment

The operating system (OS) employed by the module is referred to as Wind River VxWorks version 6.9 OS running on a Broadcom XLS108 network processor. 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 for 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. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

2.6 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 8 – Certificate Numbers for Cryptographic Algorithm Implementations

Cert	Algorithm	Mode	Description	Function/Caveats
C1967	AES [197]	ECB [38A]	Key Sizes: 128, 192, 256	Encrypt
		CCM [38C]	Key Sizes: 128, 192, 256 Tag Len: 64	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
C1966	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CFB128 [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		GCM/GMAC [38D]	Key Sizes: 128, 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt
A2565	AES [197]	ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
C1966	AES [197]	KW	Forward Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt
Vendor Affirmed	CKG [IG D.12]	[133] Section 5.1 Key Pairs for Digital Signature Schemes [133] Section 5.2 Key Pairs for Key Establishment [133] Section 6.1 Direct symmetric key generation using unmodified DRBG output [133] Section 6.2.2 Derivation of symmetric keys from a pre-shared key		
C1966	CVL: ECC CDH Primitive [56A]		P-256	Key Agreement Scheme provides 128 bits of encryption strength
	CVL: KAS ECC [56A]	Ephemeral Unified - Initiator	EC	
C1966	CVL: RSASP [186-4]		n = 2048	
C1966	CVL: RSADP [56B]		n = 2048	
C1966	CVL: KDF SNMP [135]		SHA-1	Key Derivation
C1966	CVL: KDF SSH [135]	V2	SHA256	Key Derivation
	CVL: KDF TLS [135]	v1.2	SHA(256, 384)	
C1966	DRBG [90A]	Hash	SHA256	Deterministic Random Bit Generation, generates 256 bits for each call
C1966	DSA [186-4]		(L = 2048, N = 224) (L = 2048, N = 256)	KeyGen

Cert	Algorithm	Mode	Description	Function/Caveats
			(L = 2048, N = 224) SHA224 (L = 2048, N = 256) SHA256	SigGen
			(L = 2048, N = 224) SHA224 (L = 2048, N = 256) SHA256	SigVer
C1966	ECDSA KeyGen [186-4]		P-256	Key Pair (Testing Candidates)
	ENT [90B]	The entropy source produces at least 4 bits of entropy per each output byte. The module uses 128 bytes from this entropy source to seed the internal SP 800-90A Hash DRBG (SHA-256) with entropy input and nonce. 128 bytes of entropy data provides at least 64 bytes of min-entropy or equivalently 512 bits of min-entropy. 512 bits of min-entropy exceeds 1.5 x 256 bits min-entropy security strength. Therefore, the entropy source in the module successfully seeds the DRBG with 256 bits of security strength.		Entropy output to seed the DRBG
C1966	HMAC [198]	SHA-256	Key Sizes: 24, 32, 64, 96, 128 bytes (192, 256, 512, 768, 1024 bits)	Message Authentication KDF Primitive
		SHA-384	Key Sizes: 128 bytes (1024 bits)	
		SHA-512	Key Sizes: 128 bytes (1024 bits)	
C1966	KAS FFC [56A]	dhEphem	FC (2048/256), Concatenation	Key Agreement Scheme provides 112 bits of encryption strength
	KTS [38F]	KW	AES Cert. #C1966	Key Transport using a 256-bit AES key
C1966	RSA [186-4]		n = 2048	KeyGen
		PKCS1_v1.5	n = 2048 SHA256	SigGen
		PKCS1_v1.5	n = 2048 SHA256	SigVer
C1966	RSA [186-2]	PKCS1_v1.5	n = 2048 SHA256	SigVer
C1966	SHS[180]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest Generation

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.

Table 9 – Non-Approved, Allowed Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman	CVL Cert. #C1966 with CVL Cert. #C1966, key agreement; key establishment methodology provides 112 bits of encryption strength.
RSA	2048-bit RSA based key encapsulation per IG D.9 (for use in TLS v1.2); key wrapping; key establishment methodology provides 112 bits of encryption strength.

Table 10 – Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Server/Host Auth	Cipher	Integrity
SNMPv3			AES-CFB-128	SHA1
SSHv2 [IG D.8 and SP 800-135]	diffie-hellman-group-exchange-sha256 (2048 bit)	RSA(2048)/DSA(2048)	AES-CBC-128/192/256	HMAC-SHA-256, HMAC-SHA-512
TLS [IG D.8 and SP 800-135]	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS v1.2			
	Ephemeral ECDH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS v1.2			
	Ephemeral ECDH	RSA	AES-CBC-256	HMAC-SHA-384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS v1.2			
	Ephemeral ECDH	RSA	AES-GCM-128	
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS v1.2			
	Ephemeral ECDH	RSA	AES-GCM-256	
	TLS_RSA_WITH_AES_128_CBC_SHA256, TLS v1.2			
	RSA	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_RSA_WITH_AES_256_CBC_SHA256, TLS v1.2			
	RSA	RSA	AES-CBC-256	HMAC-SHA-256
	TLS_RSA_WITH_AES_128_GCM_SHA256, TLS v1.2			
	RSA	RSA	AES-GCM-128	
	TLS_RSA_WITH_AES_256_GCM_SHA384, TLS v1.2			
	RSA	RSA	AES-GCM-256	

Note: The module's implementation of TLS is compatible with the TLS 1.2 specification and supports GCM ciphersuites defined by SP 800-52 rev1, Section 3.3.1. The module's AES-GCM IV generation conforms to IG A.5 Scenario #1 for TLS v1.2 (RFC5288). The counter portion of the IV is set by the module within its cryptographic boundary. The 64-bit counter portion of the 96 bit IV has 2^{64} possible values and the module will need more than 598 years for this to roll over (2^{64} / (3600*24*365*(976,562.5 pkts/sec))). In case the module's power is lost and then restored, a new key for use with the AES GCM is established. The IV's fixed field is a 32-bit random number and can have 2^{32} different values. The module was tested against an independent implementation of TLS and found to behave correctly.

2.6.1 Critical Security Parameters

The module supports the following critical security parameters:

Table 11 – 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 SNMPv3 engine
Pre-shared Secret (key)	Shared secret	Externally generated and imported electronically in encrypted form or plaintext from a non-networked GPC .	Never exits the module	Stored in non-volatile memory.	By Del service (command) to delete key	Used to derive the first KEK (key exchange) and MEK (management key)
Authentication 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.	Never exits the module	Stored in non-volatile memory	By Zeroize command	Peer Authentication of SSH/TLS sessions
Local private key	RSA 2048-bit key	Internally generated or externally generated and imported electronically into the module in encrypted form or plaintext from a non-networked GPC	Never exits the module	Stored in non-volatile memory.	By Zeroize command	Establish trusted point in peer entity
TLS Key Agreement Private Key	EC Diffie-Hellman, (P-256 curve)	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for TLS sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS pre-master secret	Shared secret	Generated using EC Diffie-Hellman key exchange or by TLS client when RSA key exchange is used.	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Used to derive the TLS master secret
TLS master secret	48 bytes	Internally generated from the TLS pre-master secret	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Used to derive TLS session keys
SSH Key Agreement Private Key	Diffie-Hellman. 256 bit private key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for SSH sessions
Wireless Key Agreement private keys	Diffie-Hellman 256 bit private key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for wireless link establishment
TLS Session Authentication Key	HMAC SHA-256 key or HMAC SHA-384 key	Internally derived	Never exits the module	Stored in plaintext in volatile memory	Upon reboot or session termination	Data authentication for TLS sessions
TLS Session Key	AES-128, AES-256 (CBC, GCM)	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-SHA256 or HMAC-SHA512 key	Internally derived	Never exits the module	Stored in plaintext in volatile memory	Upon reboot or session termination	Data authentication for SSH sessions
SSH Session Key	AES-128, AES-192, AES-256 (CBC)	Internally generated	Never exits the module	Stored in plaintext in volatile memory	Upon reboot or session termination	Data encryption for SSH sessions
Administrator Passwords	8-15 character ASCII[8] string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By password change command or by Zeroize command	Authentication for administrator login
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 or by Zeroize command	Authentication for user login

[8] ASCII – American Standard Code for Information Interchange

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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	128 bytes of entropy data with at least 64 bytes of min-entropy	Internally generated	Never exits the module	Generated after reset. Stored in plaintext in 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 in 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 in volatile memory	Upon reboot or power cycle	Used during FIPS-approved random number generation
Wireless management encryption key (MEK)	AES 128-, 256-bit CCM key	Internally derived	Never exits the module	Stored in plaintext in 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 or derived	Exits the module in encrypted form during session establishment The current KEK is used to encrypt the new KEK.	Stored in plaintext in 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 in 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 Rev2 (vendor affirmed). See Table 8 row 5 that shows each section from SP800-133 Rev2 that is implemented by the module.

2.6.2 Public Keys

The table below provides a complete list of Public Keys used within the module:

Table 12 – List of Public Keys

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Authentication public 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	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 RSA public 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	Stored in non-volatile memory.	By Zeroize command	Establish trusted point in peer entity
TLS Key Agreement Public Key	EC Diffie-Hellman, (P-256 curve)	Internally generated	Public key exported electronically in plaintext	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for TLS sessions
SSH Key Agreement Public Key	Diffie-Hellman 2048-bit public key	Internally generated	Public key exported electronically in plaintext	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for SSH sessions
Wireless Key Agreement public key	Diffie-Hellman 2048 bit public key	Internally generated	Public key exported electronically in plaintext	Stored in volatile memory	Upon reboot or session termination	Key agreement/establishment for wireless link establishment
L3Harris 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

2.7 Electromagnetic Interference / Electromagnetic Compatibility

The L3Harris 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.

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[9])
- Known Answer Tests (KATs) for the following FIPS-Approved algorithms:
    - AES (Cert. #C1967) encrypt – hardware, AES-256 CCM[10]
    - AES (Cert. #C1967) decrypt – hardware, AES-256 CCM
    - AES (Cert. #C1966) encrypt – firmware, AES-256 GCM[11]
    - AES (Cert. #C1966) decrypt – firmware, AES-256 GCM
    - AES (Cert. #A2565) encrypt – firmware, AES-256 ECB
    - AES (Cert. #A2565) decrypt – firmware, AES-256 ECB
    - HMAC (SHA-256, SHA-384, SHA-512)
    - NIST SP 800-90A Hash_DRBG (SHA-256)
    - RSA (signature generation and signature verification)
    - SHA1, SHA-256, SHA-384, SHA-512
    - KAS FFC Primitive "Z" Computation KAT (IG 9.6 Self-Test)
    - KAS ECC Primitive "Z" Computation KAT
    - Entropy source start-up tests:
        - Repetition Count Test (RCT)
        - Adaptive Proportion Test (APT)

- Pair-wise Consistency Test:
    - DSA key pair generation

If any of the power-up self-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.

[9] CRC – Cyclic Redundancy Check

[10] Per IG 9.4, the AES-256 CCM KAT tests the forward cipher function. The AES ECB (Cert. #C1967) encrypt does not also need its own separate KAT.

[11] Per IG 9.4, the AES-256 GCM KAT tests the forward cipher function. The AES CFB (Cert. #C1966) mode does not also need its own separate KAT. AES CFB utilizes the forward cipher function for both encrypt and decrypt.

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 Health Test for the entropy source for the NIST SP 800-90A DRBG:
    - Repetition Count Test (RCT)
    - Adaptive Proportion Test (APT)
- RSA Pair-wise Consistency Test
- 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.

2.8.3 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 L3Harris.

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 seals. If the Crypto-Officer suspects tampering, he/she should immediately contact L3Harris.

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 L3Harris.

3.1.1 Initialization

The Crypto-Officer is responsible for the Initialization of the module through the Web Interface or CLI over SSH or local console port. The Crypto-Officer must log in to the module using the default username (“admin”) and password (“admin”). 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 in the system configuration. 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, Telnet, and RADIUS.
4. If SNMP is required, enable SNMPv3.
5. Enable HTTPS 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).
16. Check if the module is in FIPS mode using the "get fipsstatus" command (returns "ON" for FIPS mode).

To transition out of the FIPS compliant mode of operation the Crypto-Officer should perform the following steps:

1. Delete the Local RSA public/private keys (if X509 Authentication is used) and Authentication (RSA) public/private keys. Delete the TLS certificate and private key if HTTPS was used.
2. Turn FIPS Mode Flag to OFF.
3. Set the Encryption Type to None.
4. Save the configuration.
5. A reboot will be triggered by the step above. The reboot process can take a few minutes. After reboot the unit will operate as a non-FIPS module.

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 8 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 the 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 L3Harris 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 other management protocols can be used (HTTP and telnet). 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 6. A monitor should check the system configuration information to confirm the FIPS mode flag is set to ON.

4 Acronyms

This section defines the acronyms used throughout this document.

Table 13 – 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
RADIUS	Remote Authentication Dial-In User Service
ID	Identification

Acronym	Definition
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

5 References

Table 14 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, June 29, 2020*
[133r2]	*NIST Special Publication 800-133 Rev. 2, Recommendation for Cryptographic Key Generation, June 2020*
[135r1]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186-4]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*

Abbreviation	Full Specification Name
[198-1]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180-4]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, October 2016*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, August 2007*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Br2]	*NIST Special Publication 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, March 2019*
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
SSH	*Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", RFC 4252/4253/4254, Internet Engineering Task Force, January 2006.* *D. Bider, "Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol", RFC 8332, Internet Engineering Task Force, March 2018.*
TLS	*Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2". RFC 5246, Internet Engineering Task Force, August 2008.*