FastIron ICX™ 7850 Series Switch/Router

FIPS 140-2 Non-Proprietary Security Policy Level 1

Document Version 1.7

May 12, 2023

Ruckus Networks (formerly known as Ruckus Wireless) is a brand of wired and wireless networking equipment and software owned by CommScope Technologies LLC.

Table of Contents:

Table of Tables:

Table of Figures:

1 Introduction

ICX7850 switch is targeted to enhance the existing ICX (FastIron) core and aggregation solutions, as well as to increase ICX market share with 100GE, 10GE LRM and 256b MACSEC support. With the 40/100GE links, 48 port SFP28 models with the support of 10G LRM optics, 256b MACSEC, ICX7850 caters to emerging markets that require massive bandwidth. The support of 25GE transceivers, as well the break out 100G link to either a 4*10G or 4*25G enables the future proofing of the campus requirements. This environment is a multi-chip standalone cryptographic module.

2 Overview

The FIPS 140-2 validation includes hardware devices running the firmware version presented in Table 1. The module meets an overall FIPS 140-2 compliance of Security Level 1 with Design Assurance Level 1. The cryptographic boundary is represented by the opaque enclosure.

Table 2 list the devices included in this evaluation.

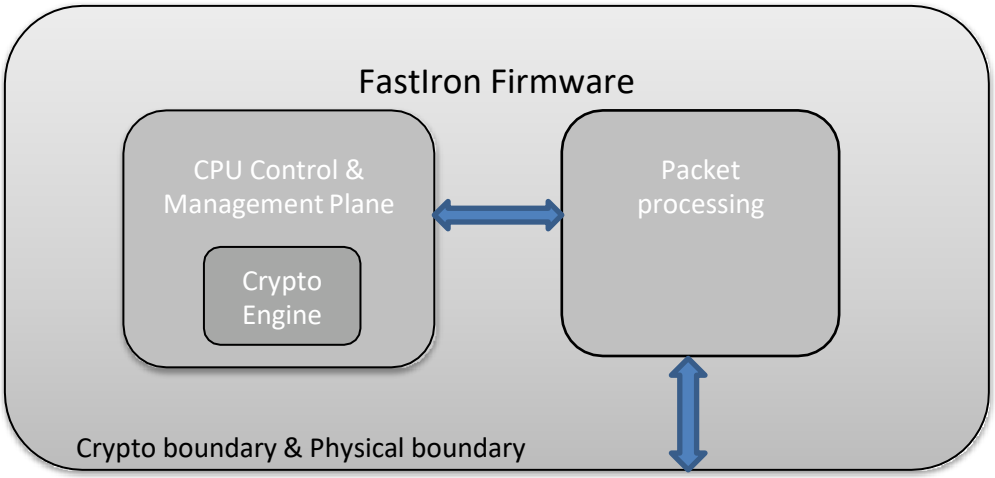

Figure 1 - Block diagram

3 FastIron Firmware

Each of the ICX series runs a different firmware image which is built from the same source code. This firmware image includes the cryptographic functionality described under Section 6. The firmware can be built as an “S” (switch) or an “R” (router) version. The “R” image has Router functionality in addition to the functionality in the “S” image. The source code for cryptographic module on both images is identical and is compiled identically.

Firmware Version
IronWare R08.0.95g

Table 1 - Firmware Version

4 ICX 7850 Series

SKU	MFG Part Number	Brief Description
ICX7850-32Q	HW P/N 84-1003423-01, Version 0300	32x100G (fiber) • Each 100G QSFP28 port supports 40G operation • Each 100G QSFP28 port supports 4x25G break-out • Use 12 of 32 ports for uplink/stacking
ICX7850-48F	HW P/N 84-1003425-01, Version 0300	48x25G (fiber) + 4x100G (fiber uplink) + 4x100G (stacking) • Each 25G SFP28 port supports 10G and 1G operation • Each 100G QSFP28 port supports 4x25G break-out modular slot. bundle includes one 1000W AC power supply and one fan, front to back airflow, port modules sold separately.
ICX7850-48FS	HW P/N 84-1003424-01, Version 0200	48x10G (fiber, MACSec, LRM) + 4x100G (fiber uplink) + 4x100G (stacking) • Each 10G SFP+ port supports 10G and 1G operation • Each 100G QSFP28 port supports 4x25G break-out • PHY-less design for QSFP28 ports • Each 10G client port support 256-bit MACSec and LRM up to 220 meters - modular slot bundle includes one 1000W AC power supply and one fan, front to back airflow, port modules sold separately

Table 2 - ICX 7850 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 2 illustrates the ICX7850-32Q, ICX7850-48F, ICX7850-48FS.

Figure 2 - ICX 7850 (Front)

5 Ports and Interfaces

5.1 ICX 7850 Series

An ICX 7850 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7850 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7850 device has one RJ-45 network management port, one mini USB serial management port, and one USB storage port on the front panel

Table 3 shows the correspondence between the physical interfaces of an ICX 7850 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
QSFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
DC socket	Power
Console Port	Data input, Control input, Status output
Out of band management port	Data input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 3 - ICX 7850 Port Mapping to Logical Interface

6 Modes of Operation

ICX 7850 devices have two (2) modes of operation: FIPS Approved mode and non-Approved mode. Section 6.3 describes services and cryptographic algorithms available in FIPS-Approved mode. In non-FIPS Approved mode, the module runs without these FIPS policy rules applied. Section 8.3 FIPS Approved Mode describes how to invoke FIPS Approved mode. Before the module has been invoked into the FIPS Approved mode for the first time, the module is in an initial non-compliant state. Power-on Self-Tests (POSTs), other than the Firmware Integrity Test, do not run in this initial state. Once the FIPS Approved mode is invoked, self-tests will continue to run in both the FIPS Approved mode and non-FIPS Approved mode.

6.1 Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 1 with Design Assurance Level 1

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 4 - Security Requirements and Levels

6.2 Roles

In FIPS Approved mode, the cryptographic modules support four (4) roles: Crypto Officer, Port Configuration Administrator, User Role, MACsec Peer:

1. Crypto Officer Role (Super User): The Crypto Officer Role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode. The Crypto Officer Role has complete access to the system. The Crypto Officer is the only role that can perform firmware loading.

2. Port Configuration Administrator Role (Port Configuration): The Port Configuration Administrator Role on the device in FIPS Approved mode is equivalent to a port configuration user in non- FIPS Approved mode. Hence, the Port Configuration Administrator Role has read-and-write access for configuring specific ports but not for global (system-wide) parameters.

3. User Role (Read-Only): The User Role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

4. MACsec Peer - A peer device which establishes a MACsec connection with the cryptographic module using AES GCM 128-bit pre-shared key.

The User role has read-only access to the cryptographic module while the Crypto Officer Role has access to all device commands. The cryptographic modules do not have a maintenance interface or maintenance role.

Section 7.2 describes the authentication policy for user roles.

6.3 Cryptographic Functionality

Table 5 summarizes the available FIPS Approved cryptographic functions.

Table 6 lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

Label	Cryptographic Algorithms	Cert.
AES	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB (128,192,256 bits)*, CBC (128,192,256 bits), CMAC (128 bits), CFB (128 bits), and CTR (128,192,256 bits) *Tested only as a prerequisite for other algorithms. Please note that AES-KW has been tested for AES #5023, but it is not used.	5023
AES implemented for MacSec in BCM82756	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB (128,256 bits)*, GCM (128,256 bits) *Tested only as a prerequisite for other algorithms. Please note that other operations have been tested for AES #4550 but are not used.	4550
CVL	[SP 800-135] Application Specific Key Derivation Functions SNMPv3 KDF, SSHv2 KDF, *TLSv1.0/1.1 KDF, *TLSv1.2 KDF Please note that the CAVP and CMVP do not examine this module's implementations of the above protocols. *Tested but not used in the approved mode of operation.	1568
DRBG	[SP 800-90A] Deterministic Random Bit Generators Variants: CTR DRBG with AES-256 (with PR and DF) Please note that HASH DRBG was tested but is not used.	1838
DSA	[FIPS 186-4] Digital Signature Algorithm Key Generation* Size: DSA-2048 *DSA-2048 Key Generation was tested only as a prerequisite to Diffie Hellman key exchange (see "DH KA" in the table below). Please note that other operations have been tested but are not used. (Please refer to DSA Cert. #1319 for details.)	1319

HMAC	[FIPS 198-1] Keyed-Hash Message Authentication code MAC Generate & Verify Variants: HMAC-SHA-1 (96, 160-bit tag) HMAC-SHA-256 (128, 192, 256-bit tags) HMAC-SHA-384 (192-bit tag)				3337
KAS	(KAS-SSC Cert. #A2310, CVL Cert. #1568)				KAS-SSC #A2310, CVL #1568
KAS-FFC-SSC	Diffie Hellman based shared secret computation adhering to SP800-56A rev3 dhEphem with FC, MODP-2048 L = 2048, N = 224, s = 112				#A2310
KBKDF	[SP800-108] Key-Based KDF Variant: KDF in Counter Mode, using AES-128-CMAC as PRF				167
KTS	[SP800-38F §3.1] Functions: Key Wrap, Key Unwrap Variants: AES-128-CTR and HMAC-SHA-1 AES-256-CTR and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-256 AES-256-CBC and HMAC-SHA-1 AES-256-CBC and HMAC-SHA-256				AES #5023; HMAC #3337
RSA	[FIPS 186-4] Rivest Shamir Adleman Signature Algorithm	Key Generation	Size: RSA-2048	* SHA-1 is used for protocol-specific signature generation and legacy signature verification only.	2708
	X9.31	Signature Generation	Size: RSA-2048	Hashes: *SHA-1, SHA-256,	
		Signature Verification	Sizes: RSA-1024, RSA-	Hashes: *SHA-1, SHA-256,	

			2048	SHA-384, SHA-512	
	PKCS 1.5	Signature Generation	Size: RSA-2048	Hashes: *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	

		Signature Verification	Sizes: RSA-1024, RSA-2048	Hashes: *SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
	PSS	Signature Generation	Size: RSA-2048	Hashes: *SHA-1, SHA-256	
		Signature Verification	Sizes: RSA-1024, RSA-2048	Hashes: *SHA-1, SHA-256	
SHS	[FIPS 180-4] Secure Hash Algorithm (SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512) Used for signature operations, as a component of other algorithms (e.g. HMAC, DRBG), password obfuscation, and other purposes *SHA-1 is only used for legacy signature verification, and for protocol-specific signature generation.				4082

Table 5 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode

Table 6 below lists all FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode.

Label	Cryptographic Algorithms
RSA Key Wrapping	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
MD5 (no security claimed)	MD5 is used for: • RADIUS obfuscated password output during operator authentication (this function is not exposed to the operator) • RADIUS server authenticity check (this function is not exposed to the operator)
NDRNG	Generation of seeds for DRBG with an estimated entropy rate of 6.77 bits/ 8 bits and 128 bytes per function call

Table 6 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode

6.4 Roles and Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a power-cycle. They can also view the module status by entering CLI "`fips show`" command.

For all other services, an operator must authenticate to the device as described in Section 7.2 Authentication. The cryptographic modules provide services for remote communication (SSHv2, SNMPv3 and Console) for management and configuration of cryptographic functions. The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSP) associated with the service.

Table 7 below, lists Roles, FIPS non-Approved Cryptographic Functions, Protocols, and Services only available in non-FIPS Approved Mode

Role	Service / Function	Description
This is not a user accessible service	HTTPS Cipher Suites	Hyper Text Transport Protocol in secure connection mode, using non-Approved cipher suites
Crypto Officer Role, User Role	HTTP	Hyper Text Transport Protocol (plaintext; no cryptography)
Crypto Officer Role, User Role	SSHv2	2-key Triple-DES (non-compliant), 3-key Triple-DES (non-compliant)
Crypto Officer Role, User Role	SNMP { Simple Network Management Protocol v1, v2 and v3 with MD5 / DES, AES (non-compliant) / SHA-1 (non-compliant) }	MD5 and DES, AES (non-compliant) / SHA-1 (non-compliant), SNMPv1, SNMPv2c and SNMPv3 (non-compliant) in noAuthNoPriv, authNoPriv modes Modes: DES in authPriv mode for SNMPV3 (non-compliant) Key sizes: DES 56 bits, AES-128 (non-compliant)
Crypto Officer Role	TFTP (Trivial File Transfer Protocol)	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Role	Service / Function	Description
This is not a user accessible service	“Two-way encryption”	Base64
This is not a user accessible service	MD5	Message Digest 5 algorithm is used as cryptographic hash function to check for verification of data integrity and wide variety of cryptographic applications Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	Syslog	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Syslog output is transmitted in plaintext. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VSRP	Virtual Switch Redundancy Protocol Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VRRP/VRRP-E	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	MSTP	Multiple Spanning Tree Protocol Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	NTP (Authentication using MD5)	Network Time Protocol Modes: MD5 and SHA-1 (non-compliant) for authentication Key sizes: 20 bytes

Role	Service / Function	Description
Crypto Officer Role, User Role	BGP	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	AES-192 (non-compliant)	AES-192 (non-compliant) encryption/decryption is only available in non-FIPS mode
This is not a user accessible service	DSA (non-compliant)	DSA (non-compliant) digital signature generation/verification only available in non- FIPS mode

Table 7 - Roles, FIPS non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode

Note: In addition to Table 7, all algorithms in Tables 5 and 6 are available in the non-Approved mode but are not compliant with the usual applicable standards.

6.5 User Role Services

6.5.1 SSHv2

This service provides a secure session between the cryptographic module and an SSHv2 client using SSHv2 protocol. The cryptographic module authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface.

The cryptographic modules support three kinds of SSHv2 client authentication: password, client public key and keyboard interactive. For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The cryptographic module authenticates operator with passwords stored on the device, or on a RADIUS server. Section 7.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one step ahead. It allows multiple challenges to be issued by the cryptographic module, using the backend RADIUS server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the cryptographic module.

SSHv2 supports Diffie-Hellman (DH) to configure the modulus size on the SSHv2 server for the purpose of key- exchange.

Maximum number of concurrent SSHv2 user sessions supported is five (5).

The following encryption algorithms are available for negotiation during the key exchange with an SSHv2 client:

- AES-CTR with a 128-bit key (aes128-ctr),
- AES-CTR with a 256-bit key (aes256-ctr),

All secure hashing is done with HMAC-SHA-1.

The following MAC algorithms are available for negotiation during the key exchange with an SSHv2 client: HMAC-SHA1 (digest length = key length = 20 bytes)

In User role access, the client is given access to three (3) commands: *enable*, *exit* and *terminal*. The enable command allows user to re-authenticate using a different role. If the role is the same, based on the credentials given during the *enable* command, the user has access to a small subset of commands that can perform *ping traceroute* in addition to *show* commands.

6.5.2 SNMP

SNMPv1 and SNMPv2 services are disabled in FIPS mode and the SNMPv3 service with authentication as HMAC-MD5 and privacy as DES are also disabled (only HMAC-SHA-1 and AES-CFB are used). The SNMPv3 service within User role allows read-only access to the SNMP MIB within the FastIron device. The device does not provide SNMP MIB access to CSPs when operating in FIPS Approved mode. All other MIB objects are made available for use in approved FIPS mode. These other MIB objects provide capability to monitor the various functional entities in the module which are non-security relevant.

6.5.3 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about a Ruckus cryptographic module and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available is the same as the list mentioned in the SSHv2 service.

6.5.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

6.6 Port Configuration Administrator Role Services

6.6.1 SSHv2

This service is described in Section 6.4.1 above.

The Port Configuration Administrator will have seven (7) commands, which allows this user to run show commands, run ping or trace route. The enable command allows the user to re-authenticate as described in section 6.4.1. Within the configuration mode, this role provides access to all the port configuration commands, e.g., all sub-commands within “interface eth 1/1” command. This operator can

transfer and store firmware images and configuration files between the network and the system and review the configuration.

6.6.2 SNMP

The SNMP service is not available for a Port Configuration Administrator Role Service.

6.6.3 Console

This service is described in Section 6.4.3 above. Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. EXEC commands. The list of commands available is the same as those mentioned in the SSHv2 service.

6.6.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

6.7 Crypto Officer Role Services

6.7.1 SSHv2

In addition to the two methods of authentication, password and keyboard interactive, described in Section 6.4.1, SSHv2 service in this role supports RSA public key authentication, in which the device stores a collection of client public keys. Only clients with a private key that corresponds to one of the stored public keys can gain access to the device using SSHv2. After a client presents a public key which matches one of the stored CO SSHv2 public keys, and provides a corresponding signature, the device will give Crypto Officer access to the entire module.

The Crypto Officer can perform configuration changes to the module (including enabling and disabling MACsec on a per-port basis, which configures alternating bypass). This role has full read and write access to the cryptographic module.

When firmware download is desired, the Crypto Officer shall download firmware download in the primary image and secondary image.

The Crypto Officer can perform zeroization by invoking the firmware command "`fips zeroize all`" or session termination.

6.7.2 SCP

This is a secure copy service. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary Images can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and MAC algorithm configured for SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on the cryptographic modules is to copy user digital certificates and host public-private key pairs to the device in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

6.7.3 SNMP

This service is described in Section 6.4.2 above. The SNMP service within Crypto Officer Role allows read- write access to only Non-Security Relevant elements of the SNMP MIB within the FastIron device.

6.7.4 Console

Logging in through the CLI service is described in Section 6.4.3 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the cryptographic module. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access; afterwards the operator may securely import additional pairs of RSA host keys as needed over a secured SSHv2 connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSHv2 connection) and enable the HTTPS server.

NOTE: The cryptographic module “does not” support DSA key generation in FIPS mode, except as part of Diffie Hellman.

6.7.5 NTP

The NTP [same as NTPv4] Network Time Protocol can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server. Symmetric key scheme is supported for authentication.

NTPv4 specification (RFC-5905), allows any one of possibly 65,534 message digest keys (excluding zero), each distinguished by a 32-bit key ID, to authenticate an association. The servers and clients involved must agree on the key ID, key type and key to authenticate NTP packets.

NTP service with MD5 key authentication is disabled in FIPS mode.

NTPv4 service with SHA1 key authentication is available upon configuration in FIPS mode.

6.8 MACsec Peer Role Services

6.8.1 MACsec

Establishes and maintains MACsec sessions with the cryptographic module using AES 128-bit pre-shared keys.

7 Policies

7.1 Security Rules

The cryptographic module’s design corresponds to the cryptographic module’s security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 1 security requirements. After configuring a FastIron device to operate in FIPS Approved mode, the Crypto Officer can execute the “fips self-tests” command to perform algorithm self-tests. If an error is detected during the self-test, the module is reloaded once and comes back in the initial non-

compliant state. The Crypto Officer has an opportunity to fix the error conditions. Once “fips self-tests” command runs successfully without any error, the Crypto Officer can save the configuration and reload the module. Once the module enters FIPS approved mode, these self-tests are always executed during POST, even if the module later runs in non-Approved mode.

1) The cryptographic module provides role-based authentication.

2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSPs).

3) The module does not perform MACsec encryption by default. MACsec has to be enabled via configuration. The MACsec configuration can be used to enable Alternating Bypass or full encryption.

4) The cryptographic module performs the following tests:

    a) Power up Self-Tests:

        i) Cryptographic Known Answer Tests (KAT):

            (1) AES-128,192,256-bit key sizes KAT (encrypt) in CBC, ECB, CTR and CFB modes*

            (2) AES-128,192,256-bit key sizes KAT (decrypt) in CBC, ECB, CTR and CFB modes*

            (3) AES-CMAC KAT*

            (4) SHA-1,256,384,512 KAT (Hashing)

            (5) HMAC-SHA-1,256 KAT (Hashing)

            (6) RSA 2048-bit key size KAT (encrypt)

            (7) RSA 2048-bit key size KAT (decrypt)

            (8) RSA 2048-bit key size, SHA-256,384,512 Hash KAT (signature generation)

            (9) RSA 2048-bit key size, SHA-256,384,512 Hash KAT (signature verification)

            (10) DRBG KAT (CTR_DRBG) and Health Tests

            (11) SP800-135 SSHv2 KDF KAT (CVL #1568)

            (12) SP800-135 SNMPv3 KDF KAT (CVL #1568)

            (13) SP800-108 KBKDF KAT

            (14) AES-GCM KATs for MACsec (#4550)

            (15) KAS-FFC-SSC (SP800-56Ar3 compliant) KATs

            *All AES self-tests are for AES #5023, unless otherwise specified.

ii) Firmware Integrity Test (CRC 32) [run in FIPS mode and non-FIPS mode]

iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

```
Crypto module initialization and Known Answer Test (KAT) Passed
```

iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

```
Crypto Module Failed < Reason String >
```

b) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on NDRNG

ii) Continuous Random Number Generator test – performed on DRBG

iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

v) DSA 2048 SHA- 256 Pairwise Consistency Test (Sign/Verify)

vi) Firmware Load Test: RSA 2048 bit, SHA-256 Signature Verification

vii) Alternating Bypass Test

viii) Manual Key Entry Test: N/A

ix) KAS-FFC-SSC Pairwise Consistency Test

5) At any time, the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the "`fips self-tests`" command.

6) Data output to services defined in Section 6.3 Services is inhibited during key generation, self-tests, zeroization, and error states.

7) Status information does not contain CSPs or sensitive data that if used could compromise the module.

8) As per FIPS 140-2 Implementation Guidance D.11, Ruckus hereby states that the following protocols have not been reviewed or tested by the CAVP or CMVP:
   a) SSHv2
   b) SNMPv3

9) The module acts as authenticator within the MACsec protocol. The module should only be used together with other CMVP-validated modules to provide a peer to authenticator connection. The link between peer and authenticator should be secured to prevent the possibility for an attacker to

introduce foreign equipment into the LAN. The module creates IV's for MACsec in compliance with IEEE 802.1AE and its applicable amendments.

7.1.1 FIPS Fatal Cryptographic Module Failure

When POST is successful, the following messages will be displayed on the console:

```
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.

Crypto module initialization and Known Answer Test (KAT) Passed.
```

In order to operate a cryptographic module securely, an operator should be aware of the following rules for FIPS Approved mode of operation:

External communication channels / ports are not available before initialization of the cryptographic module.

The cryptographic module uses a FIPS Approved random number generator, CTR_DRBG.

The cryptographic modules shall use FIPS Approved key generation methods:

1) RSA public and private keys in accordance with [ANSI X9.31]

The cryptographic modules shall use Approved (or allowed) key establishment techniques:

1) Diffie-Hellman
2) RSA Key Encapsulation
3) AES Key Wrapping

The cryptographic modules shall restrict key entry and key generation to authenticated roles.

The cryptographic modules shall not display plaintext secret or private keys. The device shall display "…" in place of plaintext keys.

The cryptographic module only performs "get" operations using SNMP.

7.2 Authentication

The cryptographic modules support role-based authentication. A device can perform authentication and authorization (that is, role selection) using RADIUS and local configuration database. Moreover, the cryptographic modules support multiple authentication methods for each service.

For first-time access, an operator can authenticate without a password. To implement one or more authentication methods for securing access to the device, an operator in the Crypto Officer Role configures authentication-method lists that set the order in which a device consults authentication methods). In an authentication-method list, an operator specifies an access method (Console, SSHv2,Web and SNMP) and the order in which the device tries one or more of the following authenticationmethods:

1) Line Password Authentication,

2) Enable Password Authentication,

3) Local User Authentication,

4) RADIUS Authentication with exec authorization and command authorization, and

5) Pre-shared keys

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a RADIUS server) the device tries the next method until a method in the list is available or all methods have been tried.

The cryptographic modules allow multiple concurrent operators through SSHv2 and the console, only limited by the system resources.

7.2.1 Line Password Authentication Method

The Line Password Authentication method uses the Telnet password to authenticate an operator.

To use Line Password Authentication, a Crypto Officer must set the Telnet password. Please note that when operating in FIPS mode, Telnet is disabled, and Line Password Authentication is not available.

7.2.2 Enable Password Authentication Method

The Enable Password Authentication Method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-config password to select the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use Enable Password Authentication, a Crypto Officer must set the password for each privilege level.

7.2.3 Local Password Authentication Method

The Local Password Authentication Method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The cryptographic modules assign the role associated with the user name to the operator when authentication is successful.

To use Local Password Authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

7.2.4 RADIUS Authentication Method

The RADIUS Authentication method uses one or more RADIUS servers to verify user names and passwords. The cryptographic modules prompt an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server

does not respond, the cryptographic module will send the user name and password information to the next configured RADIUS server.

However, while the actual password verification occurs on the RADIUS server, this is still treated as password-based authentication to the module.

The cryptographic modules support additional command authorization with RADIUS Authentication. The following events occur when RADIUS command authorization takes place.

1) A user previously authenticated by a RADIUS server enters a command on the cryptographic module.
2) The cryptographic module looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3) If the command belongs to a privilege level that requires authorization, the Ruckus cryptographic modules looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the cryptographic module. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the cryptographic module.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings.

7.2.5 Strength of Authentication

This section describes the strength of each authentication method.

7.2.5.1 MACsec Peer Role (only)

The MACsec Peer Role is assumed implicitly as follows:

Specifically, in reference to MACsec Peer Role only, the probability of a successful random guess of the AES 128-bit pre-shared key is 1/ 2^128 for a random attempt, which is less than 1/1,000,000. The module only supports a maximum of 60 attempts during a one-minute period due to the timing of the protocol. This means that the probability of false authorization with multiple consecutive random attempts during a one-minute period is 60 / 2^128, which is less than 1/100,000.

7.2.5.2 All other roles (except MACsec Peer Role)

All other users except for the MACsec Peer Role can utilize all other available authentication techniques for the purpose of authentication.

The cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000. The minimum length also applies to the RADIUS secret.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one-minute period is 60/80^8 which is less than 1/100,000.

The probability of a successful random guess of a RADIUS password during a one-minute period is less than three (3) in 1,000,000 which is less than 1/100,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

For the SNMPv3 secret used for authentication, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^8 which is less than 1/100,000.

For the SNMPv3 secret used for privacy, the module supports minimum 12-character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^12 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^12 which is less than 1/100,000.

For the NTP secret, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^8 which is less than 1/100,000.

7.2.6 Pre-shared keys Method

The MACsec Peer role establishes and maintains MACsec sessions using AES 128-bit pre-shared keys that are configured by the Crypto Officer.

7.2.7 Access Control Policy and CSP & Public Key access

Table 8 and Table 9 summarize the access operators in each role have to critical security parameters. The table entries have the following meanings:

1) r – Operator can read the value of the item,
2) w - Operator can write a new value for the item,
3) x - Operator can use the value of the item without direct access (for example encrypt with an encryption key)
4) d - Operator can delete the value of the item (zeroize).

Note that many protocol services are managed from an SSH terminal, which is why protocol, appear to be accessed from the SSH service.

Roles & Services / CSPs & Public Keys	User Role				Port Configuration Administrator				Crypto Officer Role				
	SSHv2	SNMP	Console	NTP	SSHv2	SNMP	Console	NTP	SSHv2	SCP	SNMP	Console	NTP
SSHv2 Host RSA Private Key (2048 bit)	x				x				xwd	x		wd	
SSHv2 DH Private Key (2048 bit)	x				x				xwd	x		wd	
SSHv2 DH Shared Secret Key (2048 bit)	x				x				wxd	x		wxd	
SSHv2/SCP Session Keys (128 and 256 bit AES-CTR)	x				x				wxd	x		wxd	
SSHv2/SCP Authentication Key (160-bits HMAC-SHA-1)	x				x				wxd	x		wxd	
SSHv2 KDF Internal State	x				x				wxd	x		wxd	
DRBG Entropy Input	x				x				wxd	x		wxd	
CTR_DRBG Internal State	x	x	x		x	x	x		wxd	x	x	x	
User Password	x	x	x						xrwd	xrwd		xrwd	
Port Administrator Password					x	x	x		xrwd	xrwd		xrwd	
Crypto Officer Password									xrwd	xrwd	x	xrwd	
RADIUS Secret	x		x		x		x		xrwd	xrwd		xrwd	
SNMPv3 secret	r	r	r		r	r	r		rwd	rwd	r	rwd	
NTP secret	r			r	r		r	r	rwd	rwd	r	rw	rwd
CAK									rwd	rwd		rwd	
CKN									rwd	rwd		rwd	
ICK									d			d	
KEK									d			d	
SAK									dx			dx	
SP800-108 KDF Internal State									rwd			rwd	
Firmware Integrity / Firmware Load RSA Public Key								xd	x				
SSHv2 Host RSA Public key	rx				rx				xrwd	xrw		rwd	

Roles & Services / CSPs & Public Keys	User Role				Port Configuration Administrator				Crypto Officer Role				
	SSHv2	SNMP	Console	NTP	SSHv2	SNMP	Console	NTP	SSHv2	SCP	SNMP	Console	NTP
SSHv2 Client RSA Public Key	rx				rx				xrwd	xrwd		xrwd	
SSHv2 DH Public Key	rx				rx			xd	xrwd				
SSHv2 DH Peer Public Key	wx				wx			xd	xrwd				

Table 8 - Access Control Policy and CSP & Public Key Access

Service / CSPs	MACsec Service
CAK	xd
CKN	xd
x`	xd
KEK	xd
SAK	rwxd
SP800-108 KDF Internal State	xd

Table 9 - Access Control Policy and CSP Access for MACsec Peer Role

7.2.8 CSP Zeroization

All CSPs can be zeroized by executing the "`fips zeroize all`" command. This command can be executed via the Console and SSHv2 service.

8 Description of FIPS Approved Mode

This section describes:

A. FIPS Approved mode, Section 8.1, describes:
   - This section describes required actions before you can use the module in FIPS Approved mode of operation
   - The nature of operational conditions in the module while operating in FIPS Approved mode.

B. Displaying mode status, Section 8.2, provides details on how to examine the status for the module's mode of operation.
C. Invoking FIPS approved mode, Section 8.3, describes the required steps in order to invoke the FIPS approved mode on the module.

8.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that places a Ruckus cryptographic module in FIPS Approved mode.

FIPS Approved mode disables the following:

1) Telnet access including the telnet server command
2) Command `ip ssh scp disable`
3) TFTP access
4) SNMP access to CSP MIB objects
5) Access to all commands within the monitor mode
6) Port 280
1) Entering or leaving the FIPS Approved mode also requires that an operator zeroize all CSPs.

FIPS Approved mode enables:

1) SCP

8.2 Displaying Mode Status

The cryptographic modules provide the *fips show* command to display status information about the device's FIPS mode. This command displays information about the policy settings. This information includes the status of administrative commands for security policy, the status of security policy enforcement and security policy settings.

The *fips enable* command changes the status of administrative commands; see also Section 8.1, FIPS Approved Mode.

The following example shows the output of the *fips show* command before an operator enters the *fips enable* command. Displayed status information indicates that administrative commands for security policy are unavailable (Administrative Status is OFF) and the device is not enforcing a security policy (Operational Status is OFF).

```
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

The following example shows the output of the *fips show* command after an operator enters the *fips enable* command. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) but the device is not enforcing a security policy yet (Operational Status is OFF).

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be fips
compliant and has to be zeroized. The system needs to be reloaded to operate
in FIPS mode.
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords: Clear
SSHv2 RSA Host Keys: Clear
```

The following example shows the output of the *fips show* command after the device reloads successfully in the default strict FIPS mode. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) and the device is enforcing a security policy (Operational Status is ON).

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:    Clear
SSHv2 RSA Host Keys: Clear
```

8.3 Invoking FIPS Approved Mode

Crypto Officer may use "FastIron FIPS and Common Criteria Configuration Guide" documentation on ruckuswireless.com for configuration of these devices.

To invoke the FIPS Approved mode of operation, perform the following steps:

1) Assume Crypto Officer role.
2) Enter command: *fips enable*

   The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.

3) Enter command: *fips zeroize all*

   The device zeros out the shared secrets used by various networking protocols including host access passwords, SSHv2 host keys, and HTTPS host keys with the digital signature. This will delete all the users.

4) Enter command: *no web-management hp-top-tools*

   The device will turn off access by HP ProCurve Manager via port 280.

5) Generate the SSHv2 Host RSA Private Key (2048 bit) and SSHv2 Host RSA Public Key.

   a) Use CLI command: *crypto key generate*

6) Copy signature files of all the affected images to the flash memory.

a) Use CLI command: *copy scp*

7) Create a new user

   a) Use user command: *user <username> password <password>*

8) Enter command: *write memory*.

   The device saves the running configuration as the startup configuration.

9) Enter command: *reload*

   The device resets and begins operation in FIPS Approved mode.
   (**NOTE**: Do not press B as the module is reloading).

10) Enter command: *fips show* (This command displays the FIPS-related status, which should confirm the security policy is the default security policy.)

9 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DF	Derivation Function (for SP800-90A DRBG)
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
GbE	Gigabit Ethernet
GCM	Galois/Counter Mode symmetric key cryptographic
GMAC	Galois Message Authentication Code (GMAC): an authentication-only variant of the GCM
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
MACsec	MAC Security standard
Mbps	Megabits per second
NDRNG	Non-Deterministic Random Number Generator
POE	Power over Ethernet
POE+	High Power over Ethernet
PR	Prediction Resistance (for SP800-90A DRBG)
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

Table 10 - Glossary

10 Appendix A: Critical Security Parameters

The module supports the following CSPs and public keys:

10.1 SSHv2 & SCP

1. SSHv2 Host RSA Private Key (2048 bit)
   - Description: Used to authenticate SSHv2 server to client
   - Type: RSA-2048 Private Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
   - Key-to-Entity: Process
   - Zeroization: "fips zeroize all" command

2. SSHv2 DH Private Key (2048 bit)
   - Description: Used in SCP and SSHv2 to establish a shared secret
   - Type: DH-2048 Private Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process
   - Zeroization: Session termination and "fips zeroize all" command

3. SSHv2 DH Shared Secret Key (2048 bit)
   - Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
   - Type: DH Shared Secret
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

4. SSHv2/SCP Session Keys (128 and 256-bit AES-CTR)
   - Description: AES encryption key used to secure SSHv2/SCP
   - Type: AES-128-CTR or AES-256-CTR Key

- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

5. SSHv2/SCP Authentication Key (160 bits HMAC-SHA-1)
   - Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
   - Type: HMAC-SHA-1
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

6. SSHv2 KDF Internal State
   - Description: Used to generate Host encryption and authentication key
   - Type: KDF
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

10.2 Random Number Generation

7. DRBG Entropy Input
   - Description: Entropy Input for the SP800-90A CTR_DRBG
   - Type: DRBG Seed material
   - Generation: internally generated; raw random data from NDRNG
   - Establishment: N/A
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process
   - Zeroization: Power cycle and "fips zeroize all" command

8. DRBG Internal States

- Description: Internal State of SP800-90A CTR_DRBG (V and Key)
- Type: SP800-90A DRBG State
- Generation: SP800-90A DRBG State modification (instantiate, generate, etc.)
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Power cycle and "fips zeroize all" command

10.3 Passwords & Related Secrets

9. User Password
   - Description: Password used to authenticate User (8 to 48 characters)
   - Type: Authentication data
   - Generation: N/A
   - Establishment: N/A
   - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
   - Output: MD5 hashed in configuration, output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
   - Storage: MD5 digest in plaintext in Compact Flash
   - Key-to-Entity: User
   - Zeroization: "fips zeroize all" command

10. Port Administrator Password
    - Description: Password used to authenticate Port Configuration Administrator (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

11. Crypto Officer Password
    - Description: Password used to authenticate Crypto Officer (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

12. RADIUS Secret
    - Description: Used to authenticate the RADIUS server (8 to 64 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, MD5 hashed in RADIUS message output encrypted/authenticated over SSHv2 session
    - Storage: Plaintext in RAM, Ruckus proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash
    - Key-to-Entity: Process
    - Zeroization: "fips zeroize all" command

10.4 Miscellaneous

13. SNMPv3 secret
    - Description: Used for authentication (SHA1, Password is 8 to 16 characters long) and for privacy (AES-CFB 128-bit, Password 12 to 20 characters)
    - Type: Authentication data and privacy
    - Generation: N/A - generated outside of the module
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
    - Storage: SHA1 digest and AES are stored in Compact Flash
    - Key-to-Entity: Process: User
    - Zeroization: Session termination and "fips zeroize all" command

14. PKI SCEP Enrollment RSA 2048-bit Private Key
    - Description: One-time key: SCEP protocol signing. Generated during certificate enrollment
    - Type: RSA key pair
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Temporarily stored in memory not Flash
    - Key-to-Entity: Process
    - Zeroization: Key is destroyed/zeroized as soon as the SCEP enrollment is complete.

15. NTP secret
    - Description: Authentication (SHA1, Password is 8 to 16 characters long)
    - Type: Authentication data
    - Generation: N/A - generated outside of the module
    - Establishment: N/A
    - Entry: Configured by the operator, entered authenticated over SSHv2 session
    - Output: SHA1 hashed in configuration, output authenticated over SSHv2 session

- Storage: SHA1 digest is stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

16. CAK
    - Description: Connectivity association key - main master key; Pre-shared key; 128 bits in length
    - Type: KDF Input
    - Generation: N/A - generated outside of the module
    - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in configuration file (Flash); Save configuration
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

17. CKN
    - Description: Connectivity key name; pre-shared key; 128 bits in length)
    - Type: KDF input
    - Generation: N/A - generated outside of the module
    - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in configuration file (Flash); Save configuration
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

18. ICK
    - Description: Integrity checksum key; 128 bits. This is the ICV key used to verify the integrity of MKPDUs
    - Type: AES CMAC 128
    - Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

19. KEK
    - Description: Key encryption key; 128 bits
    - Type: AES Key Wrap

- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

20. SAK
    - Description: Secure association key; 128 bits
    - Type: GCM Key
    - Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
    - Establishment: Key transport: AES Encrypted with the KEK (KTS)
    - Entry: Input AES encrypted by the KEK
    - Output: Output AES encrypted by the KEK
    - Storage: Plaintext in RAM and Plaintext in Marvell chip
    - Key-to-Entity: Process: MACsec
    - Zeroization: Session termination and "fips zeroize all" command

21. SP800-108 KDF Internal State
    - Description: SP800-108 KDF
    - Type: SP800-108 (AES 128 CMAC in Counter Mode)
    - Generation: SP800-108 KDF
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

11 Public Keys

11.1 Firmware

1. Firmware Integrity / Firmware Load RSA Public Key
   - Description: RSA 2048-bit public key used to verify signature of firmware of the module
   - Type: RSA Public Key
   - Generation: N/A, Generated outside the module
   - Establishment: N/A
   - Entry: Through firmware update
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

11.2 SSHv2

1. SSHv2 Host RSA Public Key
   - Description: (2048 bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: Plaintext
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

2. SSHv2 Client RSA Public Key
   - Description: (2048 bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: N/A, generated outside the module
   - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

3. SSHv2 DH Public Key
   - Description: (2048-bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Public Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A

- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

4. SSHv2 DH Peer Public Key
   - Description: (2048-bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Peer Public Key
   - Generation: N/A
   - Establishment: N/A
   - Entry: Plaintext
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process