R610-F Access Point

R710 Access Point

R720 Access Point

T610 Access Point

T610s Access Point

T710 Access Point

T710s Access Point

E510 Access Point

FIPS 140-2 Level 2 Non-Proprietary Security Policy

Document Version Number: 1.7
Date: July 7, 2021

Ruckus Wireless, Inc.

Table of Contents

List of Tables

List of Figures

1. Module Overview

The access point provides the connection point between wireless client hosts and the wired network. Once authenticated as trusted nodes on the wired infrastructure, the access points provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the wireless controller for management purposes. The management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted using AES SSH.

The APs have an RF interface and an Ethernet interface, and these interfaces are controlled by the software executing on each AP. The APs vary by the antenna support they offer; however, the differences do not affect the security functionality claimed by the module.

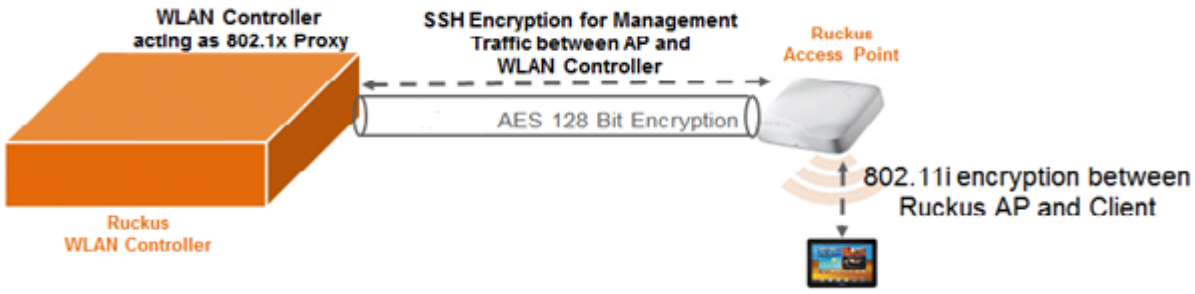

Figure 1: Encryption between AP and Controller

FIPS 140-2 conformance testing was performed at Security Level 2 on the following modules:

Table 1: Module Configurations

Module Name	HW P/N and Revision	Firmware version
R610-F Access Point	9F1-R610-US00, rev A	5.1.1.3*
R710 Access Point	9F1-R710-US00, rev A	
R720 Access Point	9F1-R720-US00, rev A	
T610 Access Point	9F1-T610-US01, rev B4	
T610s Access Point	9F1-T610-US51, rev A	
T710 Access Point	9F1-T710-US01, rev A	
T710s Access Point	9F1-T710-US51, rev A	
E510 Access Point	9F1-E510-US01, rev A	
Ruckus Tamper-Evident Seal	XBR-000195	N/A

* 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

The Cryptographic Module meets FIPS 140-2 Level 2 requirements.

Table 2: Module Security Level Statement

FIPS Security Area	Security Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module is the enclosure that contains components of the module. The enclosure of the cryptographic module is opaque within the visible spectrum. The module uses tamper evident seals to provide the evidence of tampering.

R610-F Access Point

Figure 2: R610-F Access Point

R710 Access Point

Figure 3: R710 Access Point

R720 Access Point

Figure 4: R720 Access Point

T610 and T610s Access Point

Figure 5: T610 and T610s Access Point

T710 and T710s Access Point

Figure 6: T710 and T710s Access Point

Figure 8: E510 Access Point

Figure 7: E510 Access Point

2. Modes of Operation

When received, the module is not initialized and shall be configured in the FIPS Approved Mode of operation by enabling the FIPS mode. Please see paragraph below for configuration instructions in the Approved Mode of operation. Once configured, the module is intended to always operate in the FIPS Approved Mode (refer to the first provision in Section 8 of this Security Policy); however, a provision is made to disable FIPS mode via configuration by using the **set fips-mode disable command**:

- If this provision is used, the command "zeroize –all csp" shall be executed. This requires that the module must be returned to the factory to regain operational capacity.

Access to the mode of operation selection implies that the command line interface is open and the Cryptographic Officer, shown in Figure 8 below as 'super' user, authenticates to the module. The FIPS mode state is displayed when the module is logged in as shown in the Figure 8 below. When a FIPS SKU AP joins a FIPS SKU SmartZone controller, it adopts the mode of the controller by default. Therefore, when an AP in FIPS mode joins a controller with a disabled FIPS mode, the FIPS mode in the AP is also disabled, and vice versa. If the AP and controller are running the same mode, then the AP mode remains unchanged. This implies that only a FIPS SKU AP can join a FIPS SKU controller.

Note: default credentials for first-time access are username: "super" and password: "sp-admin"

```
Please login: super
password :
Copyright(C) 2018 Ruckus Wireless, Inc. All Rights Reserved.

** FIPS SKU Ruckus R720 Multimedia Hotzone Wireless AP : 451606000024
** FIPS mode is DISABLED
```

Figure 8: FIPS Mode Displayed at Login

Enable FIPS with the **set fips-mode enable** command as shown in the Figure 9 below. When prompted, enter **y** to confirm the change or **n** to cancel. After enabling FIPS mode, the AP reboots and power on self-tests are performed. In addition to following these steps, the procedural rules defined in Section 8 shall be adhered to.

```
rkscli: set fips-mode enable
AP will reboot for toggling fips mode
Do you want to do this (y/n) :
```

Figure 9: Set FIPS mode to enabled

Please note that a FIPS mode AP with FIPS mode disabled must be manually approved in the SmartZone UI as shown in the following figure, whether or not **Auto approval** is enabled or disabled on SmartZone.

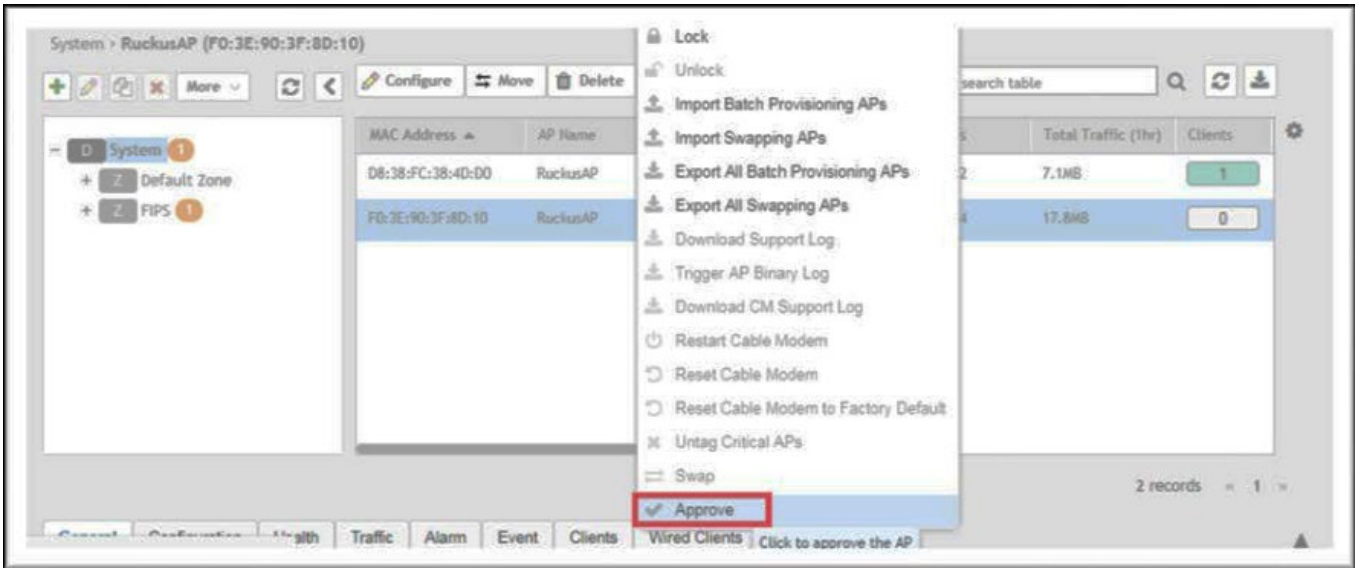

Figure 10: Set Auto Approval mode in SmartZone UI

Refer to the Ruckus FIPS Configuration Guide for more detailed information.

2.1 Approved Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation. Note that in some cases, more algorithms/ modes of operation have been tested than are utilized by the Module. Only implementations that are used are shown in the table below.

Table 3: Approved Cryptographic Functions

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
HW AES					
5312	AES	FIPS 197, SP 800-38A, SP 800-38C	ECB, CCM **Note: ECB is only used as a prerequisite to CCM*	128, 256* **Note: 256-bit is CAVP certified but not used by this module*	Data Encryption/ Decryption
5312	KTS	SP 800-38F	CCM	128, 256* Key establishment methodology provides 128 bits of encryption strength **Note: 256-bit is CAVP certified but not used by this module*	Key Transport
Linux Kernel					
C708	AES	FIPS 197, SP 800-38A	CBC	128, 192, 256	Data Encryption/ Decryption
C708	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 256, 384, 512	Message Authentication
C708	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest
OpenSSL/OpenSSH					
C710	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, CFB128, CTR, GCM*	128, 192*, 256 **Note: 192-bit is CAVP certified but is not used by this module.*	Data Encryption/ Decryption
(Vendor Affirmed)	CKG	SP 800-133	Section 6.1 Asymmetric		Key Generation

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
			signature key generation using unmodified DRBG output		
			Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
			Section 7.1 Direct symmetric key generation using unmodified DRBG output		
			Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
C710	CVL	SP 800-135	SNMP, TLSv1.2, SSH, IKEv2		Key Derivation
		SP 800-56A	ECC CDH	P-224/256//384/521 **Note: There is a Power Up-Self Test for P-224, however curve is not evoked by, or associated with, any cryptographic service or function implemented in the module*	Key Agreement
C710	DRBG	SP 800-90A	CTR_DRBG use_df	256	Deterministic Random Bit Generation
C710	DSA	FIPS 186-4	Key Generation, Signature Verification	Key Generation: (L=2048, N=224) (L=2048, N=256) (L=3072, N=256) Signature Verification: (L=1024, N=160) (L=2048, N=224) (L=2048, N=256)	Diffie-Hellman Key Generation*, Signature Verification **Note: DH uses RFC3526 safe primes referenced in*

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
				(L=3072, N=256) w/ SHA-1/224/256/384/512 (operator defined; (L=1024, N=160) and SHA-1 are acceptable for legacy-use only)	*SP 800-56Arev3, however key pair generation for N > 256, where N = len(q) is not testable.*
C710	ECDSA	FIPS 186-4		Key Generation: - P-256/384/521 Signature Generation: - P-384 w/ SHA-384 - P-224 w/ SHA-512 - K-233 w/ SHA-512 **Note: There is a Power Up-Self Test for P-224 and K-233, however these curves are not evoked by, or associated with, any cryptographic service or function implemented in the module* Signature Verification: - P-192/224/256/384/521, B-163/233/283/409/571, or K-163/233/283/409/571 w/ SHA-1/224/256/384/512 (operator defined; P-192, B-163, K-163 and SHA-1 are acceptable for legacy-use only) *Approved per IG A.14:* *any non-testable ECDSA curve generated in*	Key Generation, Digital Signature Generation and Verification

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
				compliance with Section 6.1.1 of FIPS 186-4 and providing at least 112 bits of strength.	
C710	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 256, 384, 512	Message Authentication
C710	KBKDF	SP 800-108	Counter, HMAC-SHA-1	256	Key Derivation
C710	KTS	SP 800-38F	AES-GCM	128, 256 Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport
C710	KTS	SP 800-38F	AES-CBC/ CTR with HMAC SHA-1/256/384/512	AES: 128, 256 HMAC: 160, 256, 384, 512 Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport
C710	RSA	FIPS 186-4	PKCS1 v1.5, ANSI X9.31, PSS	Signature Generation: - 3072-bit w/ SHA-224/256/384/512 Signature Verification: - 1024/2048/3072-bit w/ SHA-1/224/256/384/512 (operator defined; RSA 1024 and SHA-1 are acceptable for legacy-use only) *Approved per IG A.14:* *any non-testable RSA modulus greater than 2048 bits*	Digital Signature Generation and Verification
C710	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256		Message Digest

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
			SHA-384 SHA-512		

* AES GCM IV:

- SSH: The IV is only used in the context of the AES GCM mode encryptions within the SSHv2 protocol. The module is compliant with RFCs 4252, 4253 and RFC 5647. The AES GCM IV satisfies the following conditions:
    - If the invocation counter reaches its maximum value 2^64 – 1, the next AES GCM encryption is performed with the invocation counter set to either 0.
    - No more than 2^64 – 1 AES GCM encryptions may be performed in the same session. The SSH session is reset for both the client/server after one GB of data (2^23 block encryptions) or one hour whichever comes first.
    - When a session is terminated for any reason, a new key and a new initial IV are derived.
- TLS: The module is compatible with TLSv1.2 and the module supports acceptable GCM cipher suites from SP 800-52 Rev 1, Section 3.3.1. The cipher suites are listed in Table 5. The 64-bit nonce of the IV is deterministic. It will take 2^64 increments for the IV invocation field to wrap. The module does not enter an error state if wrapping occurs because it is inconceivable that this value can wrap around. Assuming a time of 1ns per generation operation (several orders of magnitude faster than currently possible) it would take over 584 years to wrap around.

2.2 Non-FIPS Approved but Allowed Cryptographic Functions.

The following non-FIPS approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 4: Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
Diffie-Hellman	Provides between 112 and 200 bits of encryption strength using MODP 2048 to 8192.	Used during SSHv2 and IKEv2/ IPsec handshake
EC Diffie-Hellman (CVL Cert. #C710)	Provides between 128 and 256 bits of encryption strength using P-256, P-384, or P-521 curves.	Used during TLS, SSHv2 and IKEv2/ IPsec handshake
MD5	No security claimed	Supplements the existing RSA-4096 w/ SHA-384 verification performed as part of the FW integrity test and FW load test
NDRNG	Provides a 256-bit seed to the SP 800-90A DRBG	Used to seed the SP 800-90A DRBG
RSA Key Wrapping	Provides 128 bits of encryption strength using MODP 3072.	Used during TLS handshake

2.3 Non-FIPS Approved Cryptographic Functions.

The following non-FIPS approved cryptographic algorithms are used only in the non-Approved mode of operation.

Table 5: Algorithms/ Protocols Available in the Non-Approved Mode

Algorithm	Use
DH MODP 768/1024/1536	IPSec
PBKDF2/RC4	WPA/WEP
ECDH anon TLS PSK	TLS
MD5, DES	SNMP
MD5, DES, RC4, Triple-DES, RSA*, DSA*, ECDSA*, SHA-1** * Signature verification with keys having less than 112 bits of strength ** Used in non-legacy signature verification	OpenSSL
N/A	Can enable Telnet used to access AP cli similar to SSH
N/A	HTTP/TFTP for firmware upgrade
N/A	Can configure TACACS PLUS client configuration

2.4 Protocols Used in the Approved Mode

The following protocols are used in the Approved mode of operation.

Table 6: Protocols Available in the Approved Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
IKEv2 [IG D.8 and SP 800-135]	MODP2048 MODP3072 MODP4096 MODP6144 MODP8192 ECP384	RSA 3072 Pre-Shared Key	AES CBC 128/192/256	HMAC-SHA1-96 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
IPsec ESP	MODP2048 MODP3072 MODP4096 MODP6144 MODP8192 ECP384	IKEv2	AES-CBC-128/192/256	HMAC-SHA1-96 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
SSHv2 (OpenSSH_7.9) [Compliant to RFC 4252, 4253, and 5647]	ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group14-sha1	ssh-rsa, ecdsa-sha2-nistp384	aes128-ctr, aes256-ctr	hmac-sha2-256, hmac-sha2-512, hmac-sha1
			aes256-gcm	aes256-gcm
SNMPv3	NA	HMAC-SHA1-96	AES-CFB-128	NA
WPA2 (IEEE 802.11i)	N/A	Pre-Shared Secret	AES-CCM-128	AES-CCM-128

TLS	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLSv1.2			
	Ephemeral ECDH	RSA	AES-GCM-256	AES-GCM-256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-GCM-256	AES-GCM-256

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLSv1.2			
	Ephemeral ECDH	RSA	AES-CBC-256	HMAC-SHA-384
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-CBC-256	HMAC-SHA-384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLSv1.2			
	Ephemeral ECDH	RSA	AES-CBC-256	HMAC-SHA-1
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-CBC-256	HMAC-SHA-1
	TLS_RSA_WITH_AES_256_GCM_SHA384 TLSv1.2			
	RSA		AES-GCM-256	AES-GCM-256
	TLS_RSA_WITH_AES_256_CBC_SHA256 TLSv1.2			
	RSA		AES-CBC-256	HMAC-SHA-256
	TLS_RSA_WITH_AES_256_CBC_SHA TLSv1.2			
	RSA		AES-CBC-256	HMAC-SHA-1
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLSv1.2			
	Ephemeral ECDH	RSA	AES-GCM-128	AES-GCM-128
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-GCM-128	AES-GCM-128
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLSv1.2			
	Ephemeral ECDH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-CBC-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLSv1.2			
	Ephemeral ECDH	RSA	AES-CBC-128	HMAC-SHA-1
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLSv1.2			
	Ephemeral ECDH	ECDSA	AES-CBC-128	HMAC-SHA-1
	TLS_RSA_WITH_AES_128_GCM_SHA256 TLSv1.2			

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
	RSA		AES-GCM-128	AES-GCM-128
	TLS_RSA_WITH_AES_128_CBC_SHA256 TLSv1.2			
	RSA		AES-CBC-128	HMAC-SHA-256
	TLS_RSA_WITH_AES_128_CBC_SHA TLSv1.2			
	RSA		AES-CBC-128	HMAC-SHA-1
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV TLSv1.2			

Note: Customer shall only use MODP2048 and above DH groups for IKEv2 and ESP to be FIPS compliant even though other groups are supported. No parts of these protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3. Ports and interfaces

The following tables describes physical ports and logical interfaces of the module.

R610-F Access Point

Table 7: Port and Interfaces--R610-F Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Power Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output

R710 Access Point

Table 8: Ports and Interfaces--R710 Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Power Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output

R720 Access Point

Table 9: Ports and Interfaces-- R720 Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Power Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output

T610 Access Point / T610s Access Point

Table 10: Ports and Interfaces-- T610 Acess Point / T610s Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Power Output
LEDs	5	Status Output
Reset Button	1	Control Input

T710 Access Point / T710s Access Point

Table 11: Ports and Interfaces T710 Access Point / T710s Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input, Power Output
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
SFP port	1	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output

E510 Access Point

Table 12: Ports and Interfaces-- E510 Access Point

Port Name	Count	Interface(s)
Ethernet Ports	1	Data Input, Data Output, Control Input, Status Output, Power Input
RF interfaces	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Power Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output

4. Roles, Services and Authentication

The module supports a Crypto Officer role and a User (Wireless Client) Role. The Crypto Officer installs and administers the module. The User uses the cryptographic services provided by the module. The module provides the following services.

Table 13: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Reboot/ Self-test (physical access)	Unauthenticated	Keys in RAM are zeroized
Reboot/ Self-test (authenticated)	Crypto Officer	Keys in RAM are zeroized
Zeroization	Crypto Officer	All: Z except write protected Ruckus Public Key CA chains
Firmware update	Crypto Officer	Firmware update key: R TLS Keys: R, W DRBG seed: R, W
Show status	Crypto Officer	N/A
GRE Tunnel	Crypto Officer	IPsec Keys: R, W
SSH Tunnel	Crypto Officer	Password: R, W SSH Keys: R, W DRBG seed: R, W
IPSec Tunnel	Crypto Officer	Password: R, W IPsec Keys: R, W DRBG seed: R, W
Login	Crypto Officer	Password: R, W SSH Keys: R, W TLS Keys: R, W DRBG seed: R, W
Logout	Crypto Officer	N/A
Secure Wireless connection for Clients	User	802.11i keys: R, W 802.11i PSK: R, W
Configure module parameters	Crypto Officer	Password: R, W SSH Keys: R, W DRBG seed: R, W
Secure Mesh	User	802.11i keys: R, W
SNMPv3	Crypto Officer	SNMPv3 passphrases: R SNMPv3 keys: R

While in a non-Approved mode, the module supports all the services in Table 13 above and additionally supports the services in Table 14 below. Note that the key access in Table 14 is not intended to suggest that the same keys/ CSPs are shared between the Approved and non-Approved modes, only to indicate what types of keys are accessed.

Table 14: Roles and Services in the Non-Approved Mode

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Firmware update	Crypto Officer	Firmware update key: R DRBG seed: R, W Firmware update allowed over FTP/HTTP/TFTP
SNMPv2	Crypto Officer	Configurable parameters from SZ: R
IPsec Tunnel	Crypto Officer	Password: R, W IPsec Keys: R, W DRBG seed: R, W IPsec tunnel established using DH MODP 768/1024/1536
Secure Wireless connection for Clients	User	802.11i keys: R, W 802.11i PSK: R, W If the PSK is less than 64 hex characters, PBKDF2 is used (non-storage application)
Diagnostics	N/A	All keys/ CSPs: R, W Intended for manufacturing use only; the module requires zeroization by the CO if enabled.

The module supports the following authentication mechanisms.

Table 15: Authenthication Mechanisms

Role	Authentication Mechanisms	Authentication Strength
User	802.11i Pre-Shared Secret/ Pairwise Master Key Note: For FIPS compliance, the secret configured shall be 64 hex characters (the maximum length the module supports is 64)	The length of the Pre-Shared Secret/ Pairwise Master Key must be 64 characters in hexadecimal format, therefore the probability of successfully authenticating to the module through random attempts is 1/16^64. The module's processor can run, at most, at 1.7GHz. The probability of successfully authenticating to the module within a one-minute period through random attempts is (1.7 * 10^9 * 60)/16^64.

Crypto Officer	Passwords (Minimum eight (8) characters)	The module enforces a minimum password length of eight (8) characters, and each character can be one of 93 possibilities: 26 lowercase, 26 uppercase, 10 numeric, and 31special characters (*~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ' " , . < > / ?*). Therefore, the probability of successfully authenticating to the module through random attempts is 1/93^8. The AP can optionally be configured to enforce a limit on the number of authentication attempts before locking out an operator, however assuming a limit is not configured, the module can process approximately 244 failed authentication attempts within a one-minute period. Therefore, the probability of successfully authenticating to the module within a one-minute period through random attempts is 244/93^8.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 16: Cryptographic Keys and CSPs

Key	Description/Usage
TLSv1.2	
TLS Client RSA Private Key	RSA-3072 key used in TLSv1.2 for signature generation
TLS Client RSA Public Key	RSA-3072 key used to authenticate to a TLSv1.2 host
TLS Host RSA Public Key	RSA-3072 key used to encrypt the TLS Pre-Master Secret in an RSA key exchange or verify a signature in an ECDH key exchange
TLS RSA Pre-Master Secret	384-bit secret value used to derive the TLS Master Secret in an RSA key exchange
TLS ECDH Pre-Master Secret	256/ 384/ 521-bit secret value used to establish the TLS Master Secret in an ECDH key exchange
TLS Master Secret	384-bit secret used to derive the TLS Encryption Keys and TLS Authentication Keys
TLS Client ECDH Private Key	Ephemeral P-256/ 384/ 521 ECDH key used to establish the TLS Pre-Master Secret in an ECDH key exchange
TLS Client ECDH Public Key	Ephemeral P-256/ 384/ 521 ECDH key sent to the host to establish the TLS Pre-Master Secret in an ECDH key exchange
TLS Host ECDH Public Key	Ephemeral P-256/ 384/ 521 ECDH public key sent from the host to the client to establish the TLS Pre-Master Secret in an ECDH key exchange
TLS Encryption Keys	AES-CBC 128/ 256-bit or AES-GCM 128/ 256-bit keys used to encrypt TLS session data
TLS Authentication Keys	256/ 384-bit keys used in HMAC SHA-256/ 384 respectively to authenticate TLS session data
DRBG	
DRBG Entropy Input	Entropy Input for the SP 800-90A CTR DRBG

DRBG Internal State	V and Key Values of the SP 800-90A CTR DRBG internal state
SSHv2	
SSHv2 Host RSA/ ECDSA Private Key	RSA-3072 or ECDSA P-384 key used in SSHv2 for signature generation
SSHv2 Host RSA/ ECDSA Public Key	RSA-3072 or ECDSA P-384 key used to authenticate the SSHv2 host (the AP) to an SSHv2 client
SSHv2 Client RSA/ ECDSA Public Key	RSA or ECDSA key (length is operator defined) used to authenticate the SSHv2 client to host (AP)
SSHv2 SZ/ vSZ Client RSA Private Key	RSA-3072 key used for signature generation when the AP acts as an SSHv2 client to an SZ or vSZ. Note: this is the same key as the IKEv2/ IPsec Client RSA Private Key
SSHv2 SZ/ vSZ Host RSA Public Key	RSA-3072 key used to authenticate the SSHv2 host (an SZ or vSZ) to the client (the AP)
SSHv2 SZ/ vSZ Client RSA Public Key	RSA-3072 key sent to the SSHv2 host (an SZ or vSZ) to authenticate the SSHv2 client (the AP). Note: this is the same key as the IKEv2/ IPsec Client RSA Public Key
SSHv2 DH/ ECDH Host Private Key	2048-bit ephemeral DH or P-256/ 384/ 521 ephemeral ECDH key used to derive SSHv2 Session and Authentication Keys
SSHv2 Host DH/ ECDH Public Key	2048-bit ephemeral DH or P-256/ 384/ 521 ephemeral ECDH key sent from the host to the client
SSHv2 Client DH/ ECDH Public Key	2048-bit ephemeral DH or P-256/ 384/ 521 ephemeral ECDH key sent from the client to the host
SSHv2 Session Key	AES-CTR 128/ 256-bit or AES-GCM 256-bit encryption key used to encrypt/ decrypt SSHv2 session data
SSHv2 Authentication Key	160/ 256/ 384-bit key used in HMAC SHA-1/ 256/ 384 respectively to authenticate SSHv2 session data
IKEv2/ IPsec	
IKEv2/ IPsec Encryption Key	AES-CBC 128/ 192/ 256-bit key used to encrypt IKEv2/ IPsec session data
IKEv2/ IPsec Authentication Key	160/ 256/ 384-bit key used in HMAC SHA-1-96/ 256/ 384/ 512 respectively to authenticate IKEv2/ IPsec session data
IKEv2/ IPsec Client DH/ ECDH Private Key	2048/ 3072/ 4096/ 6144/ 8192-bit ephemeral DH or P-384 ephemeral key used to derive IKEv2/ IPsec Session and Authentication Keys
IKEv2/ IPsec DH/ ECDH Host Public Key	2048/ 3072/ 4096/ 6144/ 8192 ephemeral DH or P-384 ephemeral ECDH key sent from the client to the host
IKEv2/ IPsec DH/ ECDH Client Public Key	2048/ 3072/ 4096/ 6144/ 8192 ephemeral DH or P-384 ephemeral ECDH key sent from the host to the client
IKEv2/ IPsec Pre-Shared Key	Eight (8) character minimum ASCII string used to the authenticate peers to each other
IKEv2/ IPsec Client RSA Private Key	RSA-3072 key used in IKEv2/ IPsec for signature generation. Note: this is the same key as the SSHv2 SZ/ vSZ Client RSA Private Key
IKEv2/ IPsec Host RSA Public Key	RSA-3072 key sent from the host to the client. Note: this is the same key as the SSHv2 SZ Client RSA Public Key
IKEv2/ IPsec Client RSA Public Key	RSA-3072 key sent from the client to the host
SNMPv3	
SNMPv3 Passphrases	Eight (8) character minimum passphrases used derive SNMPv3 Authentication and Privacy keys
SNMPv3 Authentication Key	160-bit HMAC SHA-1 key used for SNMPv3 session authentication

SNMPv3 Privacy Key	AES-CFB 128-bit key used for SNMPv3 session data encryption/ decryption
802.11i	
802.11i Pre-Shared Secret/ Pairwise Master Key	64 hexadecimal character secret used to derive the 802.11i Pairwise Transient Key (PTK)
802.11i Pairwise Transient Key (PTK)	384-bit key used to derive the 802.11i Temporal Key, EAPOL Key Confirmation Key and EAPOL Key Encryption Key
802.11i EAPOL Key Confirmation Key	AES-CCM 128-bit key used to perform an integrity check on an EAPOL key message
802.11i EAPOL Key Encryption Key	AES-CCM 128-bit key used to wrap the Group Temporal Key (GTK) in key transport
802.11i Temporal Key	AES-CCM 128-bit key used to encrypt/ decrypt and authenticate unicast 802.11i session data
802.11i Group Master Key (GMK)	256-bit key used to derive the 802.11i Group Transient Key (GTK)
802.11i Group Transient Key (GTK)	256-bit key used to derive the 802.11i Group Temporal Key
802.11i Group Temporal Key	AES-CCM 128-bit key used to encrypt/ decrypt and authenticate multicast 802.11i session data
Certificate Chain	
Custom CA Certificate Chain	RSA/ ECDSA/ DSA (operator defined) keys used to verify TLS certificate chains in the case that an operator chooses to use their own custom certificates.
Ruckus CA Certificate Chain	RSA-4096 keys used to verify signatures on certificates chains. There are two separate instances of Ruckus CA certificate chains: (1) those used during FW loading, and (2) those used in TLS connections if a Custom CA Certificate Chain hasn't been loaded.
Miscellaneous	
Crypto Officer Password	Password used to authenticate the Crypto Officer (at least eight (8) characters)
Firmware Upgrade Key	RSA-4096 public key used to verify signatures as part of the FW integrity and FW load tests

6. Self-Tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation, and an operator needs to power cycle the module to recover. Note that Triple-DES is self-tested, but not otherwise used.

The following table describes power-up self-tests implemented by the module.

Table 17: Self-Tests

Algorithm	Test
HW AES	
CCM	128/256 KAT (encryption/ decryption) * Note that AES-CCM-256 isn't used by the module
Linux Kernel	
AES	CBC 128/192/256 KAT (encryption/ decryption)
HMAC	HMAC SHA-256 KAT
SHS	SHA-1/ 224/ 256/ 384/ 512 KAT * Note that SHA-224 isn't used by the module
OpenSSL/ OpenSSH	
AES	AES-128-CBC AES-192-CBC AES-256-CBC AES-128-ECB AES-256-CTR KAT (encryption/decryption) * Note that AES-ECB isn't used by the module
GCM	128/ 192/ 256 KAT (authenticated encryption/ authenticated decryption) * Note that AES-GCM-192 isn't used by the module
Triple-DES (not used)	DES-EDE3-CBC DES-EDE3-ECB KAT (encryption/decryption)
SHS	SHA-1 KAT
HMAC	HMAC SHA1/224/256/384/512 KAT * Note that HMAC SHA-224 isn't used by the module
KBKDF	Counter HMAC SHA-1/256 KAT

Algorithm	Test
	* Note that KBKDF HMAC SHA-256 isn't used by the module
SP800-90A DRBG	DRBG AES-256-CTR DF DRBG AES-256-CTR (not used) DRBG SHA256 (not used) DRBG HMAC-SHA256 (not used) KAT (inclusive of instantiate, generate and reseed health tests)
DSA	(L=2048, N=256) with SHA-384 KAT (signature generation/ verification) * Note that DSA signature generation isn't used by the module
RSA	2048 with SHA1 (verification only) 2048 with SHA224 2048 with SHA256 2048 with SHA384 2048 with SHA512 KAT (signature generation/ verification)
Firmware integrity	RSA 4096 w/ SHA-384(Legacy MD5 checksum during bootup still exists); applied over all code/ firmware, inclusive of the kernel
ECDSA	Signature ECDSA P-224 with SHA512 Signature ECDSA K-233 with SHA512 (verification only) KAT (Generation/Verification)
ECC CDH	P-224 KAT

The table below describes the conditional self-tests performed by the module. Note that an RSA pairwise consistency test has not been listed because the module does not generate RSA keys. A DSA pairwise consistency test has not been listed because the module does not generate DSA keys, only DH keys.

Table 18: Conditional Self-Tests

Algorithm	Test
DRBG	Continuous Random Number Generator test
	Periodic generate function health test
ECDSA	Pairwise Consistency Test
Firmware update	RSA 4096 w/ SHA-384 (Legacy MD5 checksum during bootup still exists)
NDRNG	Continuous Random Number Generator test

7. Physical Security

The cryptographic module is a multi-chip standalone embodiment consisting of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum. The removable covers are protected with tamper-evident seals. The tamper-evident seals can be ordered when ordering the module (Part # XBR-000195 includes 120 tamper evident seals). Tamper-evident seals shall be installed as indicated in this section for the module to operate in a FIPS Approved mode of operation. The tamper-evident seals must be checked periodically by the Crypto Officer; it is up to the Crypto Officer to decide how often. Any unused seals shall remain in control of the Crypto-Officer at all times. The Crypto Officer shall be in direct control and, must observe any changes to the module such as reconfigurations where the tamper-evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module.

[Instruction on surface/device preparation and seal application]
For all seal applications, Crypto Officer ensures that the following instructions are observed:

• All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
• Do not cut, trim, punch, or otherwise alter the TEL.
• Do not use bare fingers to handle the labels. Slowly peel the backing from each seal, taking care not to touch the adhesive.
• Use very firm pressure across the entire seal surface to ensure maximum adhesion.
• Allow a minimum of 24 hours for the adhesive to cure. Tamper evidence might not be apparent until the adhesive cures.

R610-F Access Point- Three (3) Tamper-Evident Seals

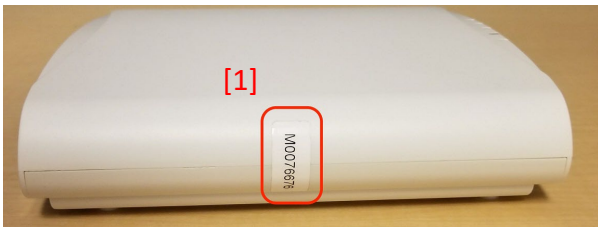

Figure 11: Left Side Tamper Seal Location

Figure 12: Right Side Tamper Seal Location

Figure 13: Bottom Tamper Seal Location

R710 Access Point- Two (2) Tamper-Evident Seals

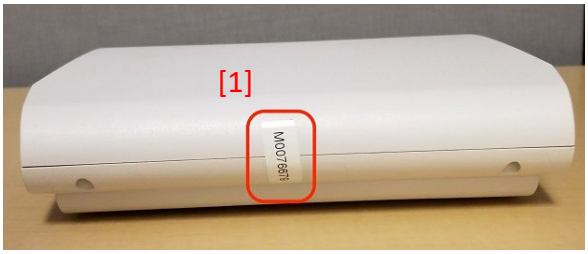

Figure 14: Left Side Tamper-Evident Seal Location

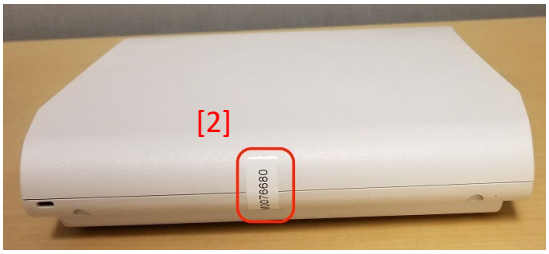

Figure 15: Right Side Tamper-Evident Seal Location

R720 Access Point- Two (2) Tamper-Evident Seals

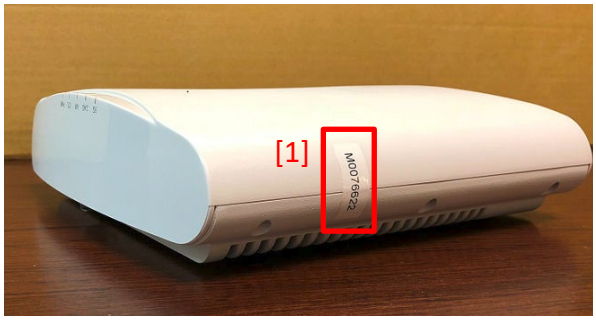

Figure 16: Right Side Tamper-Evident Seal Location

Figure 17: Left Side Tamper-Evident Seal Location

T610 Access Point/T610S Access Point- Three (3) Tamper-Evident Seals

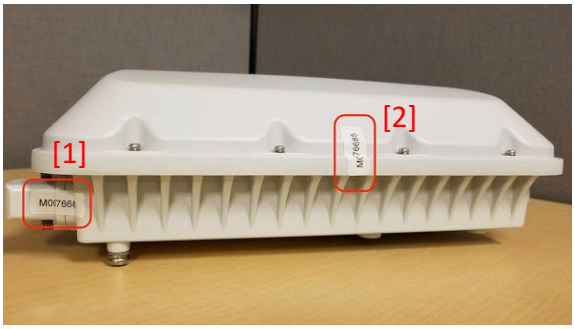

Figure 18: Left Corner and Left Side Two (2) Tamper-Evident Seal Locations

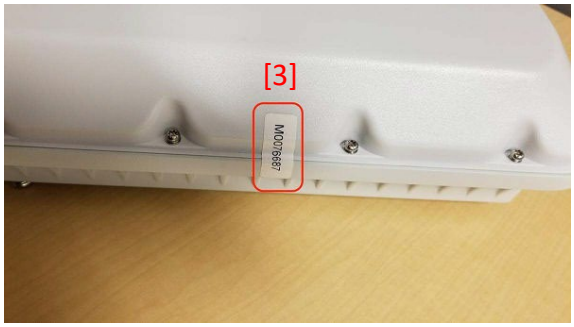

Figure 19: Right Side Tamper-Evident Seal Location

T710 Access Point/T710S Access Point- Three (3) Tamper-Evident Seals

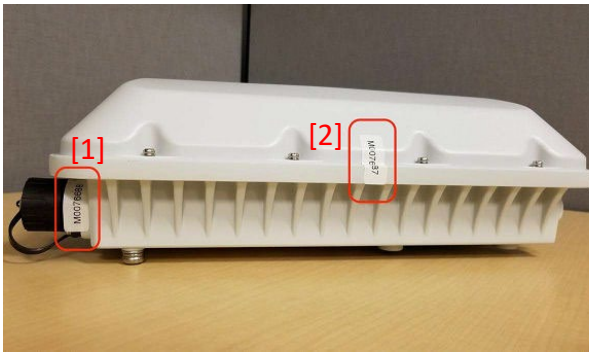

Figure 20: Front Corner and Left Side Tamper-Evident Seal Locations

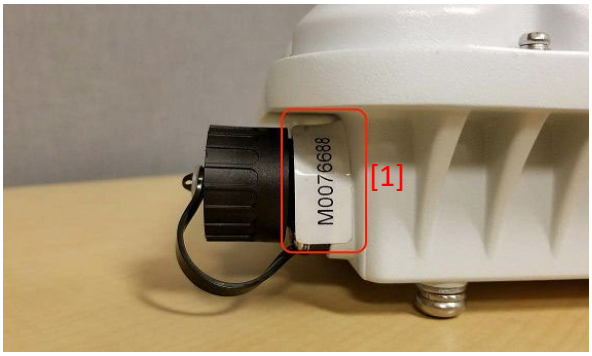

Figure 21: Close-up of Front CornerTamper-Evident Seal Location

Figure 22: Right Side Tamper-Evident Seal Location

E510 Access Point- Two (2) Tamper-Evident Seals

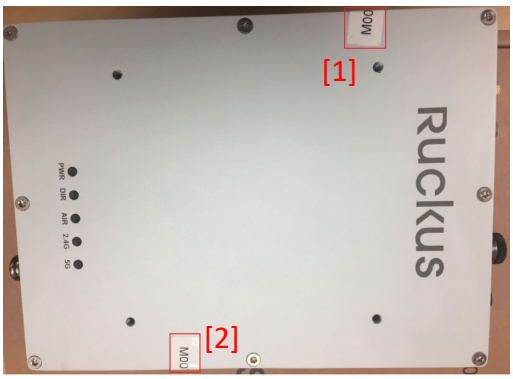

Figure 23: Left & Right Side Tamper-Evident Seal Location

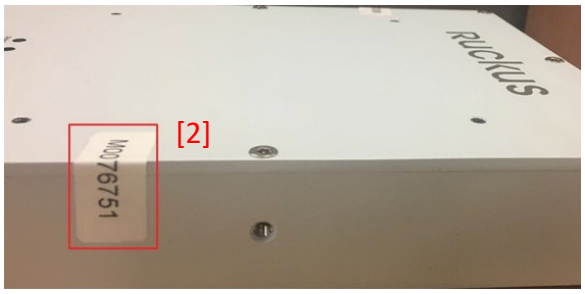

Figure 24: Close-up of Right Side Tamper-Evident Seal Location

8. Procedural Rules

The following procedural rules must be maintained by the operator in order to remain in the Approved mode.

- An operator shall immediately initialize the module to an Approved mode upon delivery, and thereafter never leave the Approved mode by ensuring the module only connects to SZ and vSZ controllers configured in the Approved mode.
- Approved lengths are used by default; however, the operator is capable of loading their own TLS certificates signed with non-Approved RSA/ ECDSA/ DSA key lengths and SHA sizes. Only Approved key lengths / curves and SHA sizes specified in Table 3 shall be used for certificate signature verification.
- The operator shall not authorize access to the Diagnostics service while in the Approved mode. Upon receiving the module, the CO shall verify that the Diagnostics service has not been enabled in the SmartZone UI, and if so, shall issue the zeroize command and return module to manufacturer.
- IKEv2/ IPsec support DH groups MODP 768, MODP 1024 and MODP1536; these groups shall not be used in the Approved mode.
- The tamper evident seals identified in Table 1 shall be installed as indicated in Section 7 for the module to operate in the approved mode of operation.
- An operator shall ensure an 802.11i Pre-Shared Secret/ Pairwise Master Key used in the Approved mode is at least 64 hex characters

Table 19: Acronyms

Acronym	Meaning
AP	Access Point
SZ	SmartZone
VSZ	Virtual SmartZone
SKU	Stockkeeping Unit