R650-US Access Point, R650-WW Access Point, R750 Access Point, R850 Access Point, T750SE Access Point, T750 Access Point, and T750-WW Access Point

FIPS 140-2 Level 2 Non-Proprietary Security Policy

by CommScope Technologies LLC

Firmware Version: 5.2.1.3
Documentation Version Number: 1.4
July 18, 2022

Table of Contents

List of Tables 2
1. Module Overview 3
2. Modes of Operation 5
2.1 Approved Cryptographic Algorithms 5
2.2 Non-FIPS Approved but Allowed Cryptographic Algorithms. 8
2.3 Non-FIPS Approved Cryptographic Algorithms. 8
3. Ports and interfaces 9
4. Roles, Services and Authentication 11
5. Operational Environment 14
6. Cryptographic Keys and CSPs 14
7. Self-Tests 20
8. Physical Security 21
9. Procedural Rules 25
9.1 Module Initialization 26
10. References 28

List of Tables

Table 1: Module Configurations 3
Table 2: Module Security Level Statement 4
Table 3: Approved Cryptographic Algorithms 6
Table 4: Non-FIPS Approved But Allowed Cryptographic Algorithms 8

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 via the 802.11i secure service. The APs also communicate directly with the wireless controller for management purposes. The management traffic between Ruckus AP and Ruckus Wireless Controller is protected by SSHv2 secure tunnel.

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.

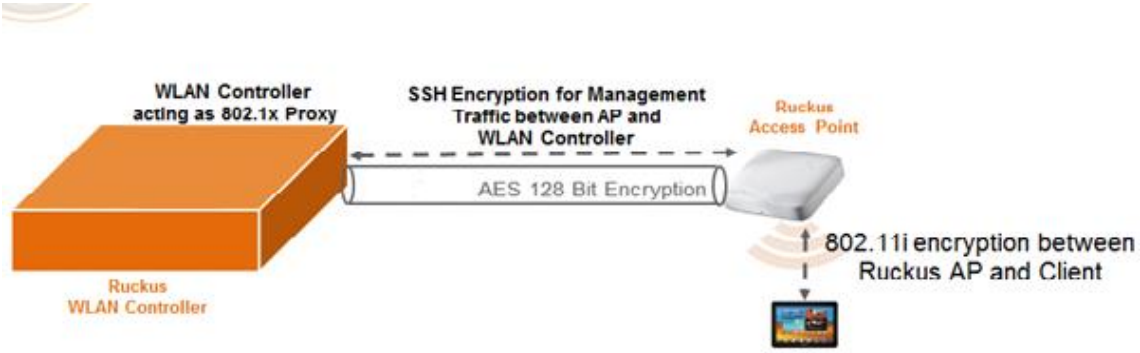

Figure 1: Encryption between AP and Controller

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
R650-US Access Point	9F1-R650-US00, revA	5.2.1.3
R650-WW Access Point	9F1-R650-WW00, revA	
R750 Access Point	9F1-R750-US00, revA	
R850 Access Point	9F1-R850-US00, revA	
T750SE Access Point	9F1-T750-US51, revA	
T750 Access Point	9F1-T750-US01, revA	
T750 -WW Access Point	9F1-T750-WW01, revA	
Tamper Evident Label Kit	902-FTEL-0040	N/A

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 module is a multi-chip standalone module. 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.

Figure 2: R650 Access Point

Figure 3: R750 Access Point

Figure 4: R850 Access Point

Figure 5: T750SE/T750/T750-WW Access Point

2. Modes of Operation

The module is intended to always operate in the FIPS approved mode. However, a provision is made to disable/enable FIPS mode via configuration. Please refer to RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3, Published on 2021-04-14 with the documentation Part Number 800-72735-001 RevA, https://support.ruckuswireless.com/documents/3509 for more information.

2.1 Approved Cryptographic Algorithms

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 Algorithms

CAVP Cert	Algorithm	Standard	Model/ Method	Use
Wi-Fi HW Algorithm Implementation				
5664	AES	FIPS 197, SP 800-38A, SP 800-38C	ECB, CCM	Authenticated Data Encryption/ Decryption
Ruckus Access Point Crypto – Kernel Algorithm Implementation				
C2092	AES	FIPS 197, SP 800-38A	ECB, CBC	Data Encryption/ Decryption
C2092	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Message Authentication
C2092	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512	Message Digest
Ruckus Access Point Crypto - OpenSSL/OpenSSH Algorithm Implementation				
C2093	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, CFB128, CTR, GCM	Data Encryption/ Decryption
Vendor affirmed	CKG	SP 800-133rev2	N/A	Key Generation
C2093	CVL	SP 800-135	SNMPv3, TLSv1.2, SSHv2, IKEv2	Key Derivation
A2459	KAS-FFC-SSC	SP800-56Arev3	dhEphem ffdhe2048, ffdhe3072, MODP-2048, MODP-3072	Key establishment methodology provides 112 or 128 bits of encryption strength
A2459	KAS-ECC-SSC	SP800-56Arev3	ephemeralUnified P-256, P-384, P-521	Key establishment methodology provides between 128 and 256 bits of encryption strength
A2459	KAS (FFC) KAS (ECC)	SP 800-56Arev3 SP 800-135rev1	Diffie-Hellman dhEphem ffdhe2048, ffdhe3072, MODP-2048, MODP-3072; EC Diffie-Hellman P-256, P-384 and P-521; with SSHv2, TLSv1.2, IKEv2 and SNMPv3 KDF	Key Agreement Scheme per SP 800-56Arev3 with key derivation per SP 800-135rev1

CAVP Cert	Algorithm	Standard	Model/ Method	Use
C2093	DRBG	SP 800-90A	CTR_DRBG (AES-256)	Deterministic Random Bit Generation
C2093	ECDSA	FIPS 186-4	Key Generation: - Curves: P-256/384/521 SigGen/SigVer: - Curves: P-256/384/521 with SHA-256/384/512	Key Generation, Digital Signature Generation and Verification
C2093	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Message Authentication
C2093	KBKDF	SP 800-108	Counter, HMAC-SHA-1	Key Derivation
C2093	KTS	FIPS PUB 197 FIPS PUB 198-1	AES (128, 192, 256 bits) with HMAC-SHA-1/256/384/512	Key Transport by using AES and HMAC
C2093	KTS	SP 800-38D	AES-GCM (128, 256 bits)	Key Transport by using GCM
C2093	RSA	FIPS 186-2 FIPS 186-4 Note: only FIPS 186-2 RSA 4096 bits was used in FIPS mode	FIPS 186-4 RSA Key Generation: - Key Generation Mode: B.3.3 - 2048/3072-bits FIPS 186-4 RSA SigGen/SigVer: - PKCSv1.5 - 2048/3072-bits with SHA-256/384/512 FIPS 186-2 RSA SigVer: - PKCSv1.5 - 4096-bits with SHA-1/256/384/512	Key Generation, Digital Signature Generation and Verification
A2459	Safe Primes	SP800-56Arev3	KeyGen/KeyVer; ffdhe2048, ffdhe3072, MODP-2048, MODP-3072	KAS-FFC-SSC Domain Parameters Generation with SafePrimes groups
C2093	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512	Message Digest

Notes:

- There are some algorithm modes that were tested but not used by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLSv1.2 and RFCs 4252, 4253 and RFC 5647 for SSHv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. The module is also compatible with SSHv2 and provides support for the acceptable GCM cipher suites from Section 7.1 of RFC 5647. The IV consist of a 4-byte fixed field and an 8-byte invocation counter. If the invocation counter reaches its maximum value 2^64 – 1, the next AES GCM encryption is performed with the invocation counter set to 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.

- No parts of the SSH, TLS, SNMP and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP.

- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP800-133. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG.

2.2 Non-FIPS Approved but Allowed Cryptographic Algorithms.

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 Algorithms

Algorithm	Caveat	Use
NDRNG		Used to seed the SP 800-90A DRBG

2.3 Non-FIPS Approved Cryptographic Algorithms.

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

Notes

- In addition to the FIPS mode of operation, the cryptographic module can also be operated in a non-FIPS mode of operation. Table 5 lists the non-approved/non-allowed the algorithms and services are available to both the User role and CO role in the module. Prior to using any of the Non-Approved services with the associated non-approved/non-allowed algorithms listed in Table 5 above, the Crypto Officer must zeroize all CSPs, which would put the module into the non-FIPS mode of operation.
- Neither the User nor the Crypto Officer are allowed to operate any of these services listed in table 5 above while in FIPS mode of operation.
- To put the module back into the FIPS mode from the non-FIPS mode, the CO must zeroize all Keys/CSPs used in non-FIPS mode, and then strictly follow up the steps in section 9 of this document to put the module into the FIPS mode.
  In addition, all available services supported by the module can be found at RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3, Published on 2021-04-14 with the documentation Part Number 800-72735-001 RevA, https://support.ruckuswireless.com/documents/3509.

3. Ports and interfaces

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

R650-US/R650-WW Access Point

Table 6: R650-US/R650-WW Access Point Ports and Interfaces

Physical Ports/Interfaces	Count	Logical Interface(s)
Ethernet Interfaces	2	Data Input, Data Output, Control Input, Status Output
RF Interfaces	2	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input

LEDs	5	Status Output
USB Port	1	Disabled

R750 Access Point

Table 7: R750 Access Point Ports and Interfaces

Physical Ports/Interfaces	Count	Logical Interface (s)
Ethernet Interfaces	2	Data Input, Data Output, Control Input, Status Output
RF Interfaces	2	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output
USB Port	1	Disabled

R850 Access Point

Table 8: R850 Access Point Ports and Interfaces

Physical Ports/Interfaces	Count	Logical Interface(s)
Ethernet Interfaces	2	Data Input, Data Output, Control Input, Status Output
RF Interfaces	2	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output
USB Port	1	Disabled

T750SE Access Point

Table 9: T750SE Access Point Ports and Interfaces

Physical Ports/Interfaces	Count	Logical Interface(s)
Ethernet Interfaces	2	Data Input, Data Output, Control Input, Status Output
RF Interfaces	2	Data Input, Data Output, Control Input, Status Output
SFP Interface	1	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output
USB Port	0	Disabled
N-Type Antenna Connectors	4	Data Input, Data Output, Control Input, Status Output

T750/T750-WW Access Point

Table 10: T750/T750-WW Access Points Ports and Interfaces

Physical Ports/Interfaces	Count	Logical Interface(s)
Ethernet Interfaces	2	Data Input, Data Output, Control Input, Status Output
RF Interfaces	2	Data Input, Data Output, Control Input, Status Output
SFP Interface	1	Data Input, Data Output, Control Input, Status Output
Power Receptacle	1	Power Input
Reset Button	1	Control Input
LEDs	5	Status Output
USB Port	1	Disabled

4. Roles, Services and Authentication

The module supports role-based authentication mechanism. Each role is authenticated by the module upon initial access to the module. There are two roles supported by the module: Crypto Officer role and User role (Wireless Client). The Crypto Officer installs and administers the module. The User role uses the cryptographic services provided by the module.

The User role or Crypto Officer role password as well as all other shared secrets must each be at least eight (8) characters long, including at least one alphabet, one numeric character, one special character (note: The special character ` cannot be used in the password and the special characters combination '$(' cannot be used in the password). Given these restrictions, we have 52 x 10 x 31 x 93 ^ 5 = 112,144,965,131,160 password combinations. If the '$(' combination was chosen in the password, then it would have 1 x 52 x 10 x 93^4 = 38,898,704,520 combinations, resulting the final correct password combinations are 112,144,965,131,160 - 38,898,704,520 = 112,106,066,426,640. Thus, the probability of a successful random attempt is approximately is one (1) in 112,106,066,426,640, which is less than the 1 in 1,000,000 required by FIPS 140-2. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total.

In addition, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, if an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 112,106,066,426,640 = 1/1,868,434,440, which is less than 1 in 100,000 required by FIPS 140-2.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 3072 bits, thus providing 128 bits of strength, which means an attacker would have a 1 in 2^128 chance of randomly obtaining the key, which is much stronger than the one in a million chances required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 2.04x10^40 (2^128 /60 = 2.04 x 10^40) attempts per second, which far exceeds the operational capabilities of the module to support.

Table 10 below lists the complete services and the associated types of access to the Keys/CSPs access supported by each role.

Table 11: 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 (authenticated)	Crypto Officer	All (not including instances in Flash Storage): Z
Zeroization	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R TLS Keys: R, W DRBG related Keys: R, W

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Show status	Crypto Officer	N/A
GRE over IPSec/IKEv2 Tunnel	Crypto Officer	IPsec/IKEv2 Keys: R, W
TLSv1.2 Tunnel	Crypto Officer	TLS Keys: R, W DRBG related Keys: R, W
SSHv2 Tunnel	Crypto Officer	Password: R, W SSH Keys: R, W DRBG related Keys: R, W
IPSec/IKEv2 Tunnel	Crypto Officer	Password: R, W IPsec Keys: R, W DRBG related Keys: R, W
Login	Crypto Officer	Password: R, W SSH Keys: R, W TLS Keys: R, W DRBG related Keys: 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 related Keys: R, W
Secure Mesh	User	802.11i keys: R, W
SNMPv3	Crypto Officer	SNMPv3 passphrases: R SNMPv3 keys: R

Notes:

1. Crypto Officer is the only role to conduct the firmware update service. Prior to the firmware update operation, the module shall perform the firmware load test by verifying the signature of the updated firmware image. Please note that the updated firmware shall be validated by CMVP prior to loading to maintain validation. For firmware load test, please refer to section 7 in this document.
2. For the services and algorithms supported by the module while in non-approved mode of operation, please refer to section 2.3 in this document for more information

Unauthenticated Services

The module also supports the unauthenticated services, including the view to the status output from the module's LED, the reset to the module and the cycling to the power.

5. Operational Environment

The module is a hardware module. The module's operating system is nonmodifiable operating system. Thus, the requirements from FIPS 140-2 level 2, section 4.6.1, are not applicable to the module.

6. Cryptographic Keys and CSPs

The entropy source (NDRNG) within the module provides at least 256 bits of entropy to seed SP800-90a DRBG for use in key generation. The table below describes cryptographic keys and CSPs used by the module.

Table 12: Cryptographic Keys and CSPs

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
DRBG Entropy Input	SP800-90A CTR_DRBG (AES-256)	384 bits	This is the entropy for SP 800-90A CTR_DRBG, used to construct the seed.	DRAM (plaintext)	Power cycle the device
DRBG Seed	SP800-90A CTR_DRBG (AES-256)	384 bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR_DRBG (AES-256)	128 bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG Key	SP800-90A CTR_DRBG (AES-256)	256 bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Crypto Officer Password	Password	At least eight characters	Password used to authenticate the Crypto Officer (CO). The password was hashed by SHA-384, and stored in the flash memory in ciphertext format. The CO input it into the module.	Flash (ciphertext)	Procedurally erase the password
Firmware Upgrade Verification Key	RSA (FIPS 186-2)	4096 bits	RSA public key used to verify the signature for Firmware Upgrade/Load Integrity Test or the Firmware Load Test. The key	Flash (plaintext)	Zeroized by erasing the

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
			was pre-installed on the system for signature verification. Note that the public key is a cryptographic key, but not considered as CSP.		firmware image
Firmware Integrity Test Key	RSA (FIPS 186-2)	4096 bits	RSA public key used to verify the signature for Firmware Integrity Test or the Firmware Integrity Test. The key was pre-installed on the system for signature verification. Note that the public key is a cryptographic key, but not considered as CSP.	Flash (plaintext)	Zeroized by erasing the firmware image
TLSv1.2 Protocol Keys and CSPs					
TLS DH/ ECDH Private Key	KAS-FFC/ECC-SSC (DH /ECDH) [SP800-56Arev3]	256 bits / P-384 curve	DH or ECDH private key used to establish the TLSv1.2 DH/ECDH shared secret. This key was generated by calling FIPS approved DRBG.	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS DH/ ECDH Public Key	KAS-FFC/ECC-SSC (DH /ECDH) [SP800-56Arev3]	3072 bits / P-384 curve	DH or ECDH public key used in TLSv1.2 handshakes. Note that the public key is a cryptographic key, but not considered a CSP	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS DH/ECDH Shared Secret	KAS-FFC/ECC-SSC (DH/ECDH) [SP800-56Arev3]	3072 bits	The shared secret used in TLSv1.2 DH/ECDH exchange. This key was derived per the DH/ECDH key agreement scheme.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS RSA Private Key	RSA (FIPS 186-4)	3072 bits	RSA private key used to sign the authentication certificate during the TLSv1.2 handshakes. This key was generated by calling FIPS approved DRBG.	Flash (plaintext)	Zeroization by RSA Keypair delete command
TLS RSA Public Key	RSA (FIPS 186-4)	3072 bits	RSA public key used for authentication during the TLSv1.2 handshakes. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	Flash (plaintext)	Zeroization by RSA Keypair delete command

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
TLS Pre-Master Secret	keying material	At least eight characters	Keying material used in TLSv1.2 handshakes. This key was used to derive TLSv1.2 Master Secret.	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS Master Secret	keying material	48 bytes	Keying material used to derive TLS Encryption Key and TLS Authentication Key. The master secret was derived from TLS pre-master secret during the TLS session establishment.	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS Encryption Key	AES-CBC or AES-GCM	AES 128/256 bits	This key is used to encrypt/decrypt the data throughout the TLSv1.2 session. This key was derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS Authentication Key	HMAC-SHA256 HMAC-SHA384	256 bits 384 bits	This key is used to protect the data integrity throughout the TLSv1.2 session. This key is derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated.
SSHv2 protocol Keys/CSPs					
SSHv2 DH/ECDH Private Key	KAS-FFC/ECC-SSC (DH/ECDH) [SP800-56Arev3]	224 bits/P-256, P-384 and P-521 curves	DH/ECDH private key, used to derive SSHv2 DH/ECDH Shared Secret during the SSHv2 handshakes. This key was generated by calling FIPS approved DRBG.	DRAM (plaintext)	Automatically when SSH session is terminated.
SSHv2 DH/ECDH Public Key	KAS-FFC/ECC-SSC (DH/ECDH) [SP800-56Arev3]	2048 bits/P-256, P-384 and P-521 curves	DH/ECDH public key, used in SSHv2 DH/ECDH exchange. This key is established per the DH/ECDH key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Automatically when SSH session is terminated.
SSHv2 DH/ECDH Shared Secret	KAS-FFC/ECC-SSC (DH/ECDH) [SP800-56Arev3]	2048 bits/P-256, P-384, P521 curves	The shared secret used in SSHv2 DH/ECDH exchange. This key was derived per the DH/ECDH key agreement scheme.	DRAM (plaintext)	Power cycle the device.

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
SSHv2 RSA/ ECDSA Private Key	RSA/ECDSA	3072 bits/P-384 curve	RSA or ECDSA private key, used to sign the authentication certificate during the SSHv2 handshakes. The key was generated by calling SP800-90A DRBG.	Flash (plaintext)	Zeroization by RSA Keypair delete command
SSHv2 RSA/ ECDSA Public Key	RSA/ECDSA	3072 bits/P-384 curve	RSA or ECDSA public key, used for authentication during the SSHv2 handshake. This key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	Flash (plaintext)	Zeroization by RSA Keypair delete command
SSHv2 Session Key	AES-CTR or AES-GCM	CTR mode: 128/256 bits GCM mode: 256 bits	This key is used to encrypt/decrypt the data throughout the SSHv2 session. This key is derived from key derivation function defined in SP800-135 KDF (SSHv2).	DRAM (plaintext)	Automatically when SSH session is terminated.
SSHv2 Authentication Key	HMAC-SHA1 HMAC-SHA256 HMAC-SHA512	160 bits 256 bits 512 bits	This key is used to protect the data integrity throughout the TLSv1.2 session. This key is derived from key derivation function defined in SP800-135 KDF (SSHv2).	DRAM (plaintext)	Automatically when SSH session is terminated.
IPSec/IKEv2 Keys and CSPs					
IKEv2 ECDH Private Key	KAS-ECC-SSC (ECDH) [SP800-56Arev3]	P-384 curve	ECDH private key, used to sign the authentication certificate signature verification Used during the IKEv2 handshakes. This key was generated by calling FIPS approved DRBG.	DRAM (plaintext)	Automatically when IPsec session is terminated.
IKEv2 ECDH Public Key	KAS-ECC-SSC (ECDH)	P-384 curve	ECDH public key, used in IKEv2 EC Diffie-Hellman (DH) exchange. This key is established per the ECDH key agreement. Note that the public key is a cryptographic key, but not considered a CSP	DRAM (plaintext)	Automatically when IPsec session is terminated.
IKEv2 ECDH Shared Secret	KAS-ECC-SSC (ECDH)	P-384 curve	The shared secret used to in IKEv2 ECDH exchange. This key	DRAM (plaintext)	Power cycle the device.

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
			was derived per the ECDH key agreement scheme.		
IKEv2 RSA/ECDSA Private Key	RSA/ECDSA	RSA:3072 bits ECDSA: P-256, P384, P-521 curves	RSA or ECDSA private key used for authentication during the IKEv2 protocol handshake. This key was generated by calling FIPS approved DRBG.	Flash (plaintext)	Zeroization by RSA/ECDSA Keypair delete command
IKEv2 RSA/ECDSA Public Key	RSA/ECDSA	RSA: 3072 bits ECDSA: P-256, P384, P-521 curves	RSA or ECDSA public key used for authentication during the IKEv2 protocol handshake. The key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	Flash (plaintext)	Zeroization by RSA/ECDSA Keypair delete command
IKEv2 Pre-Shared Key	Shared Secret	8-63 characters	Used to authenticate IPsec peers to each other. This key is configured by the Crypto Officer.	Flash (plaintext)	Configuration changes or zeroization by mode change
SKEYSEED	Keying material	160 bits	Keying material used to derive the IKEv2 session key. It was derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec/IKE session is terminated
IKEv2 Encryption Key	AES-CBC	128/192/256 bits	This key is used to encrypt/decrypt the data throughout the IKEv2 session. This key was derived by key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPsec session is terminated.
IKEv2 Authentication Key	HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	256 bits 384 bits 512 bits	This key is used to protect the data integrity of data throughout the IKEv2 session. This key is derived by key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPsec session is terminated.
IPsec Encryption Key	AES-CBC	128/192/256 bits	This key is used to encrypt/decrypt the data throughout the IPSec session. This key is derived by key	DRAM (plaintext)	Automatically when IPsec

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
			derivation function defined in SP800-135 KDF (IKEv2).		session is terminated.
IPsec Authentication Key	HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	256 bits 384 bits 512 bits	This key is used to protect the data integrity of data throughout the IPSec session. This key is derived by key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPsec session is terminated.
SNMPv3 Keys and CSPs					
SNMPv3 Passphrase	Shared Secret	8-63 characters	Shared secret used for SNMPv3 authentication. The key is configured by the Crypto Officer.	Flash (plaintext)	Procedurally erase the shared secret
SNMPv3 Authentication Key	HMAC-SHA-1	160 bits	This key is used to protect the data integrity of data throughout the SNMPv3 session. This key is derived by key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Automatically when SNMPv3 session is terminated.
SNMPv3 Session key	AES-CFB-128	128 bits	This key is used to encrypt/decrypt the data throughout the SNMPv3 session. This key is derived by key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Automatically when SNMPv3 session is terminated.
802.11i Keys and CSPs					
802.11i Pre-Shared Secret	Shared secret	64-hex characters	Used to authenticate the User. This key was entered into the module by the CO.	Flash (plaintext)	Procedurally erase the shared secret
802.11i Pairwise Master Key (PMK)	Keying material	256 bits	Used to derive the 802.11i PTK. This key was transported into the module over an IPSec/IKEv2 secure tunnel.	DRAM (plaintext)	Automatically when session is terminated.
802.11i Pairwise Transient Key (PTK)	Keying material	384 bits	Used to derive the 802.11i Temporal Key. This key was derived from 802.11i PMK.,	DRAM (plaintext)	Automatically when session is terminated.
802.11i Temporal Key (TK)	AES-CCM	128 bits	Used to protect the 802.11i session traffic. This key was derived during 802.11i 4-way	DRAM (plaintext)	Automatically when session is terminated.

Name	CSP Type	Size	Description/Usage	Storage	Zeroization
			handshakes by using the KDF defined in SP800-108.		
802.11i Group Master Key (GMK)	Keying material	256 bits	Used to derive 802.11i Group Transient Key (GTK). It was generated by calling DRBG in the module.	DRAM (plaintext)	Automatically when session is terminated.
802.11i Group Temporal Key (GTK)	AES-CCM	128 bits	Used to protect the 802.11i group traffic. This key was derived from 802.11i GMK by using the KDF defined in SP800-108.	DRAM (plaintext)	Automatically when session is terminated.
Certificate Chain					
Ruckus CA Certificate Chain	FIPS 186-2 RSA (signature verification only)	4096 bits	RSA-4096 bits used to verify signatures on certificates chains. Generated outside the module during AP manufacture. Note that the public key is a cryptographic key, but not considered a CSP	Flash (plaintext)	Zeroized by erasing the firmware image

7. 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, the access point must be returned back to manufacturer for recovery. The following table describes power-up self-tests implemented by the module.

Table 13: Power-Up Self-Tests

Algorithm	Power On Self-Test
Wi-Fi HW Chip	
AES-ECB	AES-ECB KAT (encryption)
CCM	AES-CCM KAT (authenticated encryption)
Ruckus Access Point Crypto – Kernel	
AES	AES-ECB KATs (encryption/ decryption)
HMAC	HMAC SHA-1/256/384/512 KAT
SHS	SHA-1/256/384/512 KATs

Algorithm	Power On Self-Test
Ruckus Access Point Crypto - OpenSSL/OpenSSH	
AES	AES-CBC KATs (encryption/ decryption)
GCM	AES-GCM KATs (authenticated encryption/authenticated decryption)
SHS	SHA-1 KAT
HMAC	HMAC SHA-1/256/384/512 KAT
KBKDF (SP800-108 KDF)	KBKDF KAT
SP800-90A DRBG	CTR DRBG KAT (DRBG health tests per SP 800-90A Section 11.3)
RSA (FIPS 186-4)	RSA KATs (separate KAT for signing; separate KAT for verification)
Firmware Integrity Test	FIPS 186-2 RSA 4096 bits with SHA-384 for signature verification
ECDSA	ECDSA Pairwise Consistency Test (Sign and Verify)
KAS-FFC-SSC	KAS-FFC-SSC Primitive "Z" computation KAT
KAS-ECC-SSC	KAS-ECC-SSC Primitive "Z" computation KAT

Table 14: Conditional Self-Tests

Algorithm	Test
SP800-90A DRBG	Continuous Random Number Generator test
NDRNG	Continuous Random Number Generator test
RSA	Pairwise Consistency Test
ECDSA	Pairwise Consistency Test
Firmware Load Test	FIPS 186-2 RSA 4096 bits with SHA-384 for signature verification.

8. 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 shall be installed as indicated in this section for the module to operate in a FIPS Approved mode of operation. The following table shows the Tamper Evident Labels (TELs) that shall be installed on each module to operate in a FIPS approved mode of operation. The TELs must be checked periodically by the Crypto Officer; it is up to the Crypto Officer to decide how often. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module. The Crypto Officer is responsible for using, securing and having control at all times of any unused tamper evident labels.

[Instructions 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.

There are 4 TELs (Part number: 902-FTEL-0040) that need to be placed on each module. To seal the system, apply tamper-evidence labels as depicted in the figures below.

R650 Access Point- Four (4) Tamper-Evident Seals

Figure 6: R650-US/R650-WW Front

Figure 7: R650-US/R650-WW Back

Figure 8: R650-US/R650-WW Left

Figure 9: R650-US/R650-WW Right

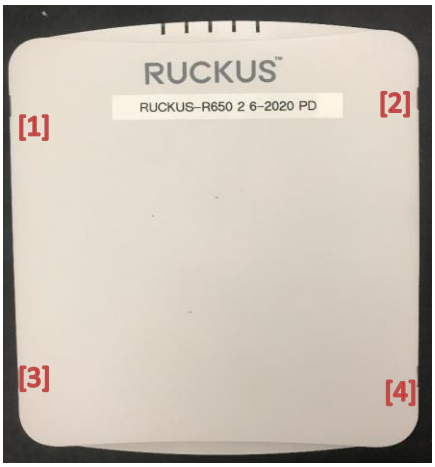

Figure 10: R650-US/R650-WW Top

Figure 11: R650-US/R650-WW Bottom

R750 Access Point- Four (4) Tamper-Evident Seals

Figure 12: R750 Front

Figure 13: R750 Back

Figure 14: R750 Left

Figure 15: R750 Right

Figure 16: R750 Top

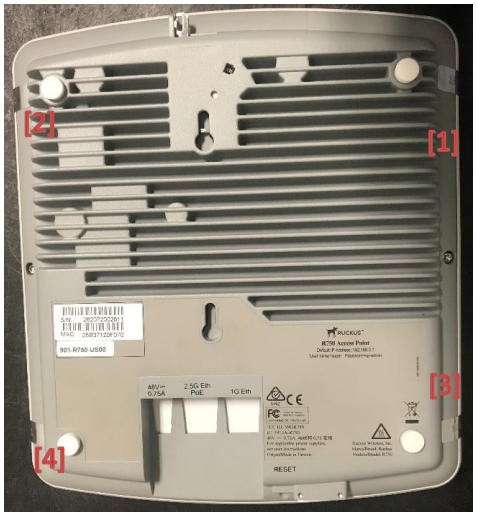

Figure 17: R750 Bottom

R850 Access Point- Four (4) Tamper-Evident Seals

Figure 18: R850 Front

Figure 19: R850 Back

Figure 20: R850 Left

Figure 21: R850 Right

Figure 22: R850 Top

Figure 23: R850 Bottom

T750SE Access Point- Four (4) Tamper-Evident Seals

Figure 24: T750SE Front

Figure 25: T750SE Back

Figure 26: T750SE Left

Figure 27: T750SE Right

Figure 28: T750SE Top **Figure 29: T750SE Bottom**

T750/T750-WW Access Point- Four (4) Tamper-Evident Seals

Figure 30: T750/T750-WW Front

Figure 31: T750/T750-WW Back

Figure 32: T750/T750-WW Left

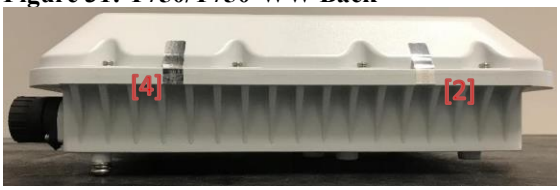

Figure 33: T750/T750-WW Right

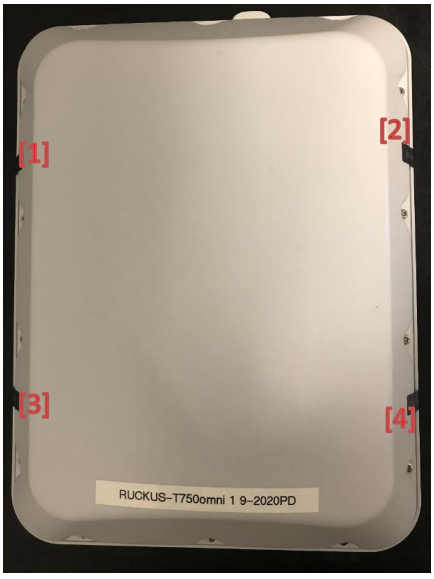

Figure 34: T750/T750-WW Top

Figure 35: T750/T750-WW Bottom

9. Procedural Rules

The module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is shipped in Vendor's boxes with Vendor's adhesive. Follow the instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings prevents the module from being placed into FIPS approved mode of operation. The module was validated with firmware version 5.2.1.3 in FIPS-approved mode of operation

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. The operator is capable of loading their own TLS certificates. Only Approved key lengths / curves and algorithms 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.
- 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.
- The CO needs to change the default login and passwords.
- The CO needs to make sure the passwords and all other shared secrets used by the module must each be at least eight (8) characters long, including at least one alphabet, one numeric character, one special character (note: The special character ` cannot be used in the password and the special characters combination '$(' cannot be used in the password).
- The User shall ensure an 802.11i Pre-Shared Secret used in the Approved mode is at least 64 hex characters.

9.1 Module Initialization

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. 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 36 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 36 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.

```
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
```

Figure36: FIPS Mode Displayed at Login

Enable FIPS with the **set fips-mode enable** command as shown in the Figure 37 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) :
```

Figure37: 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.

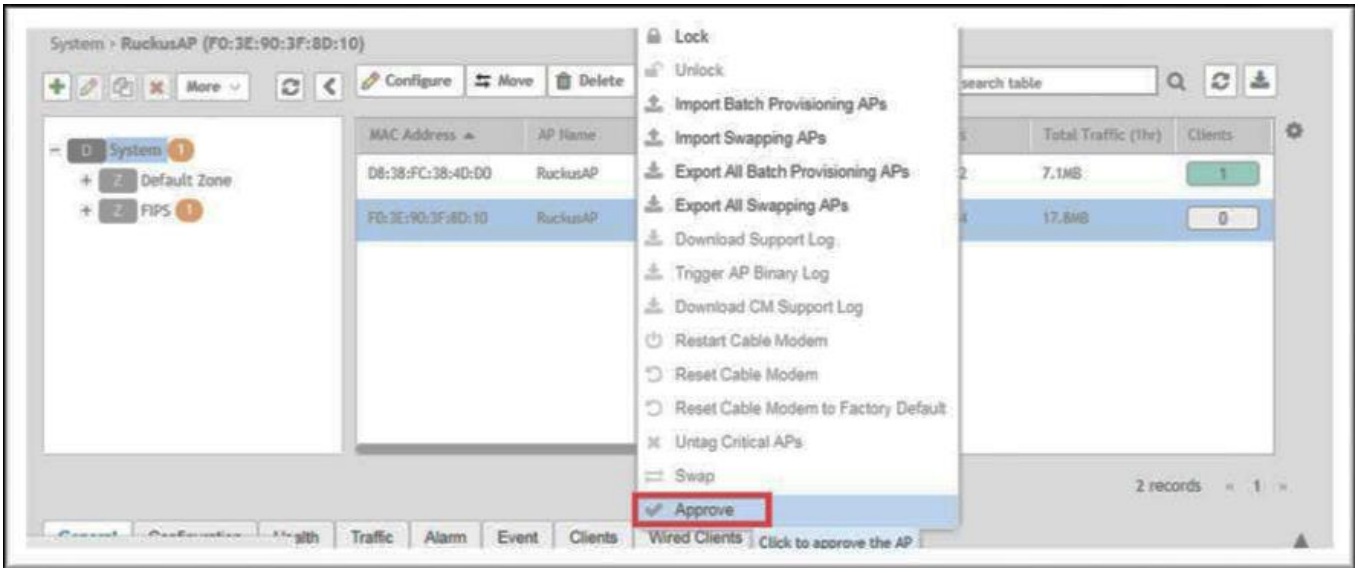

Figure 38: Set Auto Approval mode in SmartZone UI

In addition, please refer to RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3, Published on 2021-04-14 with the documentation Part Number 800-72735-001 RevA, https://support.ruckuswireless.com/documents/3509 for more configuration related information. .

10. References

Table 15: Acronyms

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