Ruckus Networks SmartZone 104 (SZ-104), SmartZone 124 (SZ-124) and SmartZone 300 (SZ-300) WLAN Controllers

FIPS 140-2 Level 1 Non-Proprietary Security Policy

by Ruckus Wireless, Inc.

Version Number: 1.3

Table of Contents

List of Tables

List of Figures

1. Module Overview

SmartZone 104 (SZ-104) and SmartZone 124 (SZ-124) are scalable, resilient, and high performing wireless LAN controllers within the Ruckus family of WLAN controllers. They manage up to 1,024 ZoneFlex Smart Wi-Fi access points, 2,000 WLANs, and 25,000 clients per device.

The SmartZone 300 (SZ-300) Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The Carrier Grade platform supports comprehensive integrated management functionality, high performance operations and flexibility to address many different implementation scenarios. The SZ-300 supports up to 10,000 AP and 100,000 Clients per unit.

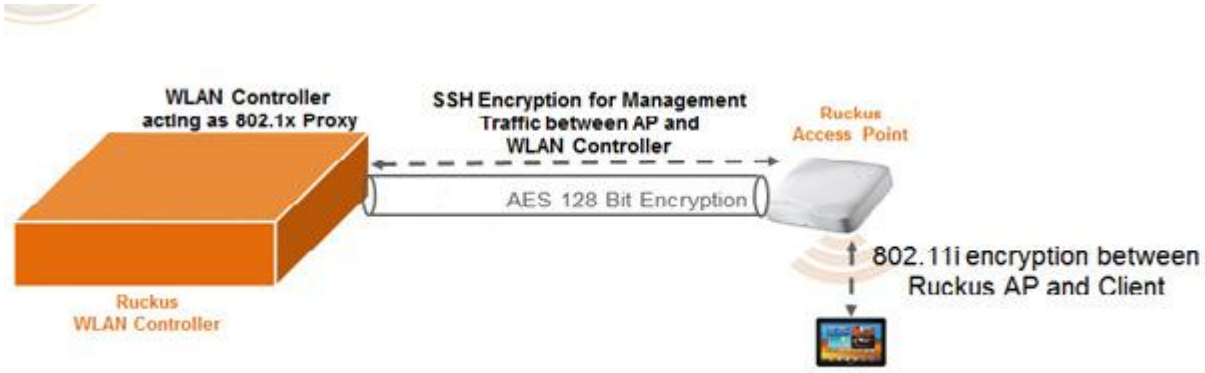

Figure 1: **Encryption between AP and Controller**

FIPS 140-2 conformance testing was performed at Security Level 1. The following configurations were tested by the lab.

Table 1: Configurations

Module Name and Version	HW P/N and Revision	Firmware version
SmartZone 104 SmartZone 124	PF1-S104-US00, RevA PF1-S124-US00, RevA	5.1.1.3 5.1.1.3
SmartZone 300	PF1-S300-WW00, RevA PF1-S300-WW10, RevA	5.1.1.3 5.1.1.3

The Cryptographic Module meets FIPS 140-2 Level 1 requirements.

Table 2: Module Security Levels

FIPS Security Area	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
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.

Figure 2: SmartZone 104

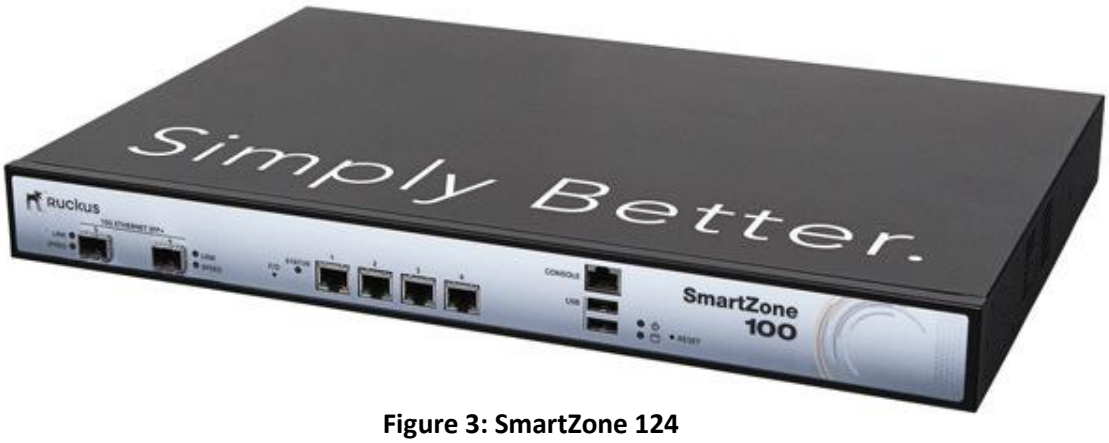

Figure 3: SmartZone 124

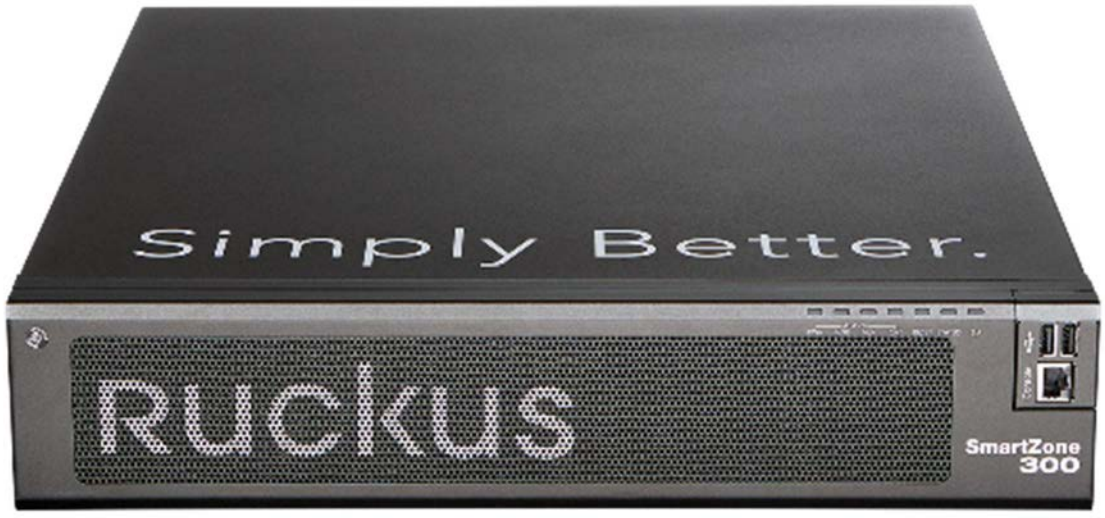

Figure 4: SmartZone 300

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 (Login CLI -> enabled mode -> fips enable/disable). In addition to running the fips enable cmd, an operator must ensure to follow the procedural rules specified in Section 8 to remain in the Approved mode. Refer to the Ruckus FIPS Configuration Guide for more 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. Implementations in **black** text are used, whereas gray text shows tested but not used configurations in the table below.

Table 3: Approved Cryptographic Functions[4]

CAVP Cert	Algorithm	Standard	Model/Method	Key Lengths, Curves or Moduli	Use
Linux Kernel					
C707	AES	FIPS 197, SP 800-38A	CBC	128, 192, 256	Data Encryption/ Decryption
C707	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	80, 96, 128, 160 128, 192, 256 192, 256, 320, 384 256,320,384,448, 512	Message Authentication
C707	SHA	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest
OpenSSL/ OpenSSH					
5097	AES	FIPS 197, SP 800-38A, SP 800-38D	CBC, CFB1, CFB128, CFB8, CTR, ECB, GCM[1], OFB	128, 192, 256	Data Encryption/ Decryption

(vendor affirmed)	CKG	SP 800-133	Section 6.1 Asymmetric signature key generation using unmodified DRBG output Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		Key Generation[3]
1647	CVL	SP 800-135	SSH TLSv 1.2	SHA-1 / 224 / 256 / 384 / 512 SHA-256 / 384 / 512 See Table 6 for protocol information.	Key Derivation[2]
1778	CVL	SP 800-135	SNMPv3	See Table 6 for protocol information.	Key Derivation[2]
C706	CVL	SP 800-135	IKEv2	See Table 6 for protocol information.	Key Derivation[2]
		SP 800-56A rev1	ECC CDH	- B-233/283/409/571 - K-233/283/409/571 - P-224/256/384/521 * P-224 is only used to meet power-up self-test requirements	Key Agreement
		SP 800-135	RSADP		Key Derivation[2]
1903	DRBG	SP 800-90A	Counter Hash HMAC	Counter: 128, 192, 256 Hash: SHA-1, 224, 256, 384, 512 HMAC: SHA-1, 224, 256, 384, 512	Deterministic Random Bit Generation
C846	DSA	FIPS 186-4	Key Generation	L=2048, N=224, 256 L=3072, N=256	Diffie-Hellman Key Generation
1322	ECDSA	FIPS 186-4		Key Generation: - B-233/283/409/571 - K-233/283/409/571 - P-224/256/384/521	Key Generation, Digital Signature Generation and Verification

				Signature Generation: - P-256* w/SHA-224/256/384/512 - P-384 w/ SHA-224/256/384/512 - P-224/521, K-233/283/409/571, B-233/283/409/571 w/SHA-224/256/384/512 Signature Verification: - P-224/256/384/521 B-233/283/409/571 or K-233/283/409/571 w/ SHA-224/256/384/512 (operator defined) Approved per IG A.14: any non-testable ECDSA curve generated in compliance with Section 6.1.1 of FIPS 186-4 and providing at least 112 bits of strength. * P-256 signature generation is only used for power-up self-tests	
3399	HMAC	FIPS 198-1	HMAC-SHA1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	80, 96, 128, 160 112,128,160,192,224 128, 192, 256 192, 256, 320, 384 256, 320, 384,448, 512	Message Authentication
5097 3399	KTS	SP 800-38F	AES with HMAC SHA-1/256/384/512	AES: 128, 192, 256 HMAC: 160, 256, 384, 512 Key establishment method provides between 128 and 256 bits of encryption strength	Authenticated Encryption, Authenticated Decryption
5097	KTS	SP 800-38F	AES-GCM	AES: 128, 192, 256 Key establishment method provides 128	Authenticated Encryption, Authenticated Decryption

				or 256 bits of encryption strength	
2759	RSA	FIPS 186-2 FIPS 186-4	ANSI X9.31 PKCSPSS PKCS1 v1.5	Key Generation: (186-2) - 2048, 3072, 4096-bit (186-4) - 2048, 3072-bit Signature Generation: (186-2) - 4096-bit w/SHA-224, 256, 384, 512 (186-4) - 2048*, 3072-bit w/ SHA-224, 256, 384, 512 * RSA-2048 signature generation is only used for power-up self-tests Signature Verification: (186-2 and 186-4) -1024/1536/2048/ 3072/4096-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	Key Generation Digital Signature Generation and Verification
4145	SHS	FIPS 180-4	SHA1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest

[1] AES GCM IV IG A.5 Compliance:

- 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 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 ciphersuites from SP 800-52 Rev 1, Section 3.3.1. The ciphersuites are listed in Table 6. 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]No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[3]The module directly uses the output of the DRBG

[4]The module implements only the modes, data size, and key sizes in the Approved algorithm table. Gray text indicates which moduli, sizes, or modes are tested, but not implemented.

2.2 Non-FIPS Approved but Allowed Cryptographic Functions

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

Table 4: Non-FIPS Approved but Allowed Cryptographic Functions

Algorithm	Caveat	Use
Diffie Hellman (CVL Cert. #1647) – TLS v1.2	Provides between 112 and 128 bits of encryption strength	Used during TLS handshake
EC Diffie Hellman (CVL Cert. #C706 with CVL Cert. #C706) – IKEv2 EC Diffie Hellman (CVL Cert. #C706 with CVL Cert. #1647) - SSH EC Diffie Hellman (CVL Cert. #C706 with CVL Cert. #1647) - TLS v1.2	Provides 192 bits of encryption strength Provides 192 bits of encryption strength Provides between 128 and 256 bits of encryption strength	Used during SSH, IKEv2/ IPsec and TLS handshake. See Table 6 for curve sizes used in each protocol.
HMAC-MD5	No security claimed per IG 1.23	Used in RADsec
NDRNG	The module generates cryptographic keys whose strength is modified by available entropy. The SZ100 provides 112 bits of security, and the SZ300 provides 128 bits of security.	Used to seed the SP 800-90A DRBG. (Provides a 256-bit seed)

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
chacha20-poly1305@openssh.com, umac-64@openssh.com,hmac-ripemd160,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com DSA, ED25519	OpenSSH
EAP-Cisco, EAP-SIM, EAP-AKA, EAP-MSCHAP-V2, EAP-AKA, MD5-Challenge	Radius
MD5, DES	SNMP
MD5, DES TDES*	OpenSSL
AES CBC* TLSv1.2 Key Derivation* RSASP* DRBG* HMAC* RSA PKCS1 v1.5* SHS*	OpenJDK AAA Test Suite

*TDES and OpenJDK library are non-compliant. OpenJDK algorithm power-up tests are performed but are not used except for testing communication with external AAA server. Using the OpenJDK AAA Test Suite constitutes exiting the FIPS Approved Mode, as stated in Section 8.

2.4 Protocols Used in the Approved Mode

Table 6: Protocols Available in the Approved Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
IKEv2 [IG D.8 and SP 800-135]	Oakley 20 (P-384)	RSA 3072 Pre-shared secret ECDSA P-384	AES CBC 128/192/256	HMAC-SHA-1 HMAC-SHA-2-256 HMAC-SHA-2-384 HMAC-SHA-2-512
IPsec ESP	Oakley 20 (P-384)	IKEv2	AES-CBC-128/192/256	HMAC-SHA-1 HMAC-SHA-2-256 HMAC-SHA-2-384 HMAC-SHA-2-512
SSHv2 [IG D.8 and SP 800-135]	ECDH-sha2-nistp256, ECDH-sha2-nistp384, ECDH-sha2-nistp521	ECDSA P-384 RSA 3072	AES-CTR-128/256 AES256-GCM@openssh.com	HMAC-SHA-1-96, HMAC-SHA-2-256, HMAC-SHA-2-512
TLS [IG D.8 and SP 800-135]	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			TLS v1.2
	Ephemeral ECDH	RSA	AES-GCM-256	HMAC-SHA-384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256			TLS v1.2
	Ephemeral ECDH	RSA	AES-GCM-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256			TLS v1.2
	Ephemeral ECDH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384			TLS v1.2
	Ephemeral ECDH	RSA	AES-CBC-256	HMAC-SHA-384
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256			TLS v1.2
	Ephemeral DH	RSA	AES-CBC-128	HMAC-SHA-256
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256			TLS v1.2
	Ephemeral DH	RSA	AES-CBC-256	HMAC-SHA-256
SNMPv3	N/A	N/A	AES-CFB-128	HMAC-SHA1
NTP	N/A	SHA-1	N/A	N/A
RADIUS (only used within RADsec)	N/A	HMAC-MD5	N/A	N/A
EAP	N/A	PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-TLS EAP-TTLS	N/A	N/A

2.5 Approved Certificate Sizes

The Crypto Officer is able to upload their own certificates and the only approved certificate sizes are loaded into the module in the approved mode.

3. Ports and Interfaces

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

Table 7: Ports and Interfaces

SmartZone 104 / 124

Port Name	Count	Interface(s)
Ethernet Ports: 4- 1GbE 2- 10GbE (SZ-124 only)	6 (SZ-124) 4 (SZ-104)	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	2	Power Output (No data interface is available while in FIPS Approved mode)
Power Receptacle	1	Power Input
Reset Button	1	Control Input
F/D Button	1	Control Input
LEDs	15 (SZ-124) 11 (SZ-104)	Status Output

SmartZone 300

Port Name	Count	Interface(s)
Ethernet Ports: 6x 1GbE ports 4x 10GbE ports	10	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	4	Not used (Disabled in factory)
Power Receptacle	2	Power Input
Reset Button	1	Control Input
LEDs	28	Status Output
VGA Port	1	Data Output, Status Output
Alarm Port	1	Not Used
Console Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input

4. Roles, Services and Authentication

The module supports a Crypto Officer role, a User Role, and AP (Access Point) Role. The Crypto Officer installs and administers the module. The Users and APs use the cryptographic services provided by the module. The module provides the following services.

Table 8: Approved Mode 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	Crypto Officer User	All (not including instances in NVM): Z
Zeroization	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R
Show status	Crypto Officer User AP	N/A
Login	Crypto Officer User	Password: R, W SSH Keys: R,W TLS Keys: R,W DRBG seed: R, W
SSH Tunnel	Crypto Officer User AP	Password: R, W SSH Keys: R,W DRBG seed: R, W
Configuration	Crypto Officer	Password: R, W SSH Keys: R,W TLS Keys: R,W DRBG seed: R, W
RadSec	AP	TLS Keys: R,W DRBG seed: R, W Radius Secret: R,W
NTP	Crypto Officer	NTP Keys: R,W
HTTPS/TLS	Crypto Officer User AP	TLS Keys: R,W DRBG seed: R, W
IPsec tunnel	Crypto Officer AP	IKEv2 Keys: R,W
EAP authenticator (EAP-TLS, EAP-TTLS, EAP-PEAP)	AP	SSH Keys: R,W DRBG seed: R, W TLS Keys: R,W
SNMPv3	Crypto Officer User	Password: R, W SNMP Keys: R,W
FIPS mode enable/disable	Crypto Officer	N/A

Table 9: Roles and Services – Non-Approved Mode

Service	Corresponding Roles
Self-test	Crypto Officer User
Reboot	Crypto Officer User
Zeroization	Crypto Officer
Firmware update	Crypto Officer
Show status	Crypto Officer User AP
Login	Crypto Officer User
SSH Tunnel	Crypto Officer User AP
Configuration	Crypto Officer
HTTPS/TLS	Crypto Officer User AP
IPsec tunnel	AP
AAA Test	Crypto Officer
EAP authenticator _(EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA)	AP
SNMPv2	Crypto Officer User
SNMPv3	Crypto Officer User
FIPS mode enable/disable	Crypto Officer
Diagnostics	N/A: intended for manufacturing only; the module requires authorization by the admin before accessing

The module supports the following authentication mechanisms:

Table 10: Authentication Mechanisms

Role	Authentication Type	Authentication Mechanisms	Authentication Attempt
User Role (Monitoring user)	Role-based (default UID is used)	User ID and Password (Minimum 8 characters)	26 lowercase, 26 uppercase, 10 numeric, and 10 special characters are supported. With a min. length of 8 characters, the authentication strength is 1/8^72 An operator must configure a try limit within the range of 1-100. Attempts to authenticate in a one-minute period are limited to 100 in the Approved mode of operation. The probability of randomly successfully authenticating is 100 * (1/8^72) which is much less than one in 100,000.
CO Role (Configuration user)	Role-based (admin ID is non-modifiable)	Admin ID and Password (Minimum 8 characters)	26 lowercase, 26 uppercase, 10 numeric, and 10 special characters are supported. With a min. length of 8 characters, the authentication strength is 1/8^72 An operator must configure a try limit within the range of 1-100. Attempts to authenticate in a one-minute period are limited to 100 in the Approved mode of operation. The probability of randomly successfully authenticating is 100 * (1/8^72) which is much less than one in 100,000.
AP Role (Access Point user)	Identity-based	SSH RSA key (3072 bits)	The authentication strength of RSA-3072 with SHA-384 verification is 1/2^128 The module is incapable of processing more than roughly 607,000 RSA signature verifications per minute. The probability of randomly successfully authenticating is 607,000 * (1/2^218) which is much less than one in 100,000.

5. Cryptographic Keys and CSPs

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

Table 11: Cryptographic Keys and CSPs

Key	Description/Usage
TLS Master Secret	Used to derive TLS Encryption Key and TLS Authentication Key

TLS Pre-Master Secret	Used to derive TLS Master Secret
TLS Encryption Key	AES key used during encryption and decryption of data within the TLS protocol
TLS Authentication Key	HMAC key used to protect integrity of data within the TLS protocol
TLS Server RSA Private Key	Used during the TLS handshake to sign the server certificate
TLS Server RSA Public Key	Used during the TLS handshake to authenticate to the TLS client
TLS Client RSA Public Key	Used during the TLS handshake to authenticate the TLS client
TLS DH/ ECDH Host Private Key	DH or ECDH private key used to establish the TLS Pre-Master Secret
TLS DH/ ECDH Host Public Key	DH or ECDH public key sent to the TLS client to establish the TLS Pre-Master Secret
TLS DH/ ECDH Client Public Key	DH or ECDH public key used to establish the TLS Pre-Master Secret
DRBG Entropy Input	Entropy Input for the SP800-90A CTR DRBG
DRBG Internal State	Internal state of the SP 800-90A CTR DRBG (Key and V)
User Password	Password used to authenticate the User (at least eight (8) characters)
Enable Password	Password used by the Crypto Officer to enable the CLI (at least eight (8) characters)
Crypto Officer Password	Password used to authenticate the Crypto Officer (at least eight (8) characters)
SSHv2 RSA/ ECDSA Private Key	RSA or ECDSA private key used during the SSH handshake to sign the host or client certificate, depending on whether the module is acting as the SSH client or host
SSHv2 Host RSA/ ECDSA Public Key	RSA or ECDSA public key used during the SSH handshake to authenticate the SSH host
SSHv2 Client RSA/ ECDSA Public Key	RSA or ECDSA public key used during the SSH handshake to authenticate the SSH client
SSHv2 ECDH Private Key	ECDH private key used to derive SSH Session and Authentication Keys

SSHv2 Host ECDH Public Key	ECDH public key sent to the TLS client to derive SSH Session and Authentication Keys
SSHv2 Client ECDH Public Key	ECDH public key used to derive SSH Session and Authentication Keys
SSHv2 Session Key	AES encryption key used to secure an SSH session
SSHv2 Authentication Key	HMAC key used to authenticate and integrity-check an SSH session
IKEv2/ IPsec Encryption Key	AES Key used to encrypt session data
IKEv2/ IPsec Authentication Key	HMAC Key used to authenticate and integrity-check a session
IKEv2/ IPsec ECDH Private Key	ECDH private key used to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec Host ECDH Public Key	ECDH public key sent to the IKE/ IPsec client to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec Client ECDH Public Key	ECDH public key used to derive IKE/ IPsec Session and Authentication Keys
IKEv2/ IPsec RSA/ ECDSA Private Key	RSA or ECDSA private key used during the IKE/ IPsec handshake to sign the host certificate
IKEv2/ IPsec Host RSA/ ECDSA Public Key	RSA or ECDSA public key used during the IKE/ IPsec handshake to authenticate to the SSH client
IKEv2/ IPsec Client RSA/ ECDSA Public Key	RSA or ECDSA public key used during the IKE/ IPsec handshake to authenticate the SSH client
IKEv2/ IPsec Pre-Shared Key	Used to authenticate IKE/ IPsec peers to each other
Firmware Upgrade Key	Used to verify the signature of firmware being loaded into the module
SNMP Passphrases	Separate passphrases used to derive the SNMPv3 auth key and SNMPv3 privacy key respectively (8-63 characters)
SNMP Authentication Key	Used to authenticate SNMPv3 packet using HMAC-SHA-1
SNMP Privacy Key	Used to encrypt SNMPv3 packet using AES-CFB-128
RADIUS Secret	Used to authenticate with the RadSec server (at least eight (8) characters)
NTP Key	Used to authenticate with the NTP server (40 characters in Approved mode, no restriction in non-Approved mode)

6. Self-Tests

The module performs the following power-up and conditional self-tests. Upon failure of a power-up or conditional self-test the module halts its operation.

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

Table 12: Power-Up Self-Tests

Algorithm	Test
Linux Kernel	
AES	AES-128/ 192/ 256 CBC KAT (encryption/ decryption)
HMAC	HMAC SHA-256 KAT
SHA	SHA-1/256/ 384/ 512 KAT
OpenSSL/ OpenSSH	
AES	AES-128 CBC KAT (encryption/decryption)
SHS	SHA-1/ 256/ 512 KAT
HMAC	HMAC SHA-1/ 224/ 256/ 384/ 512 KAT
SP800-90A DRBG	AES-256 CTR DRBG KAT (DRBG health tests per SP 800-90A Section 11.3)
DSA	(L=2048, N=256) with SHA-384 KAT (signature generation/ verification)
RSA	RSA-2048 w/SHA-384 KAT (signature generation/ verification)
ECDH	P-256 KAT (includes Primitive "Z" computation)
ECDSA	P-256 KAT (signature generation/ verification)
Firmware integrity	RSA-4096 with SHA384 signature verification during bootup

Table 13: 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
FW Load	RSA-4096 with SHA-384 with signature verification.

7. Physical Security

The module meets requirements of FIPS 140-2 level 1 for physical security. The cryptographic module is a multi-chip standalone module consisting of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum.

8. Procedural Rules

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

- An operator shall zeroize all keys/ CSPs when switching between the Approved and non-Approved mode (or vice versa).
- Approved key sizes are used by default, however the operator is capable of loading their own TLS certificates containing non-Approved RSA key lengths. Only Approved RSA key lengths specified in Table 3 shall be used.
- An operator shall not attempt to access the module's BIOS. In particular, an operator shall not change the port configurations specified in Section 3 of this Security Policy.
- The module does not enforce a limit on the number of authentication attempts without first being configured to do so. The User and Cryptographic Officer shall have an authentication try limit configured between the range of 1-100.
- An operator shall not authorize access to the Diagnostics service while in the Approved mode.
- An operator shall not evoke the OpenJDK AAA Test Service as use of these algorithms constitutes exiting the Approved mode of operation.
- The module's validation to FIPS 140-2 is no longer valid once a non-validated firmware version is loaded. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

8.1 Module Initialization

The following initialization procedure is taken from the Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and AP's. The procedure is applicable to the SmartZone 100 models, SZ-104/124, and the SmartZone 300 models, SZ-300/310. Please refer to pages 15 – 41 of the Configuration Guide for further instructions and diagrams which describe the CLI output.

- Installation: The installation procedure for all hardware pertaining to the module is carried out at the Ruckus manufacturing facility. This includes port configurations, and BIOS settings which govern the ports. Shipping box should be checked for tampering during shipping process upon receipt of module.
- Controller Configuration with FIPS Image:
    - Power on the module and open a console window to log in to the CLI via ssh.
    - At the login prompt, login with the administrator username and password, then type the enable (en) command and the admin password to change to Privileged EXEC mode.
    - At the command prompt enter 'fips ?' to display the list of available FIPS commands.
    - Enter 'fips status' to verify whether FIPS mode is enabled or disabled.
    - Enter 'fips enable' to enable FIPS mode, then enter 'yes' to confirm.
    - Enter 'fips showlog' to display the results of self-tests and verify all are passing.
    - Follow steps in Section 8, above, while operating the module.

9. References

Table 14: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions