Ruckus Wireless, Inc. SmartZone 104 (SZ-104), SmartZone 124 (SZ-124) and SmartZone 300 (SZ-300) WLAN Controllers

FIPS 140-2 Level 2 Non-Proprietary Security Policy

Version Number: 1.10

Table of Contents

1. Module Overview

SmartZone 104 (SZ-104) and SmartZone 124 (SZ-124) are scalable, resilient, and high performing wireless LAN controllers within Ruckus Wireless, Inc. 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 (SZ300) 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 SZ300 supports up to 10,000 AP and 100,000 Clients per unit.

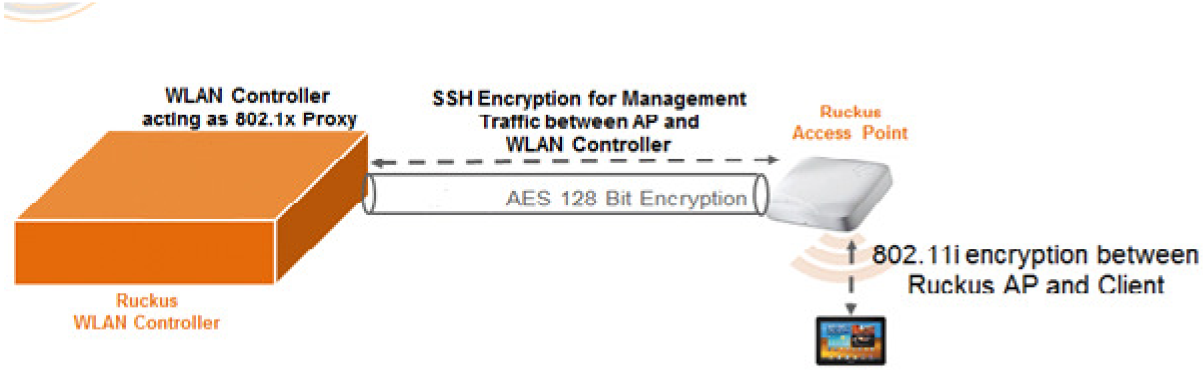


Figure 1: Encryption between AP and Controller

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

Table 1: Configurations tested by the lab.

Module Name and Version	Firmware version
SmartZone 104 SmartZone 124 SmartZone 300	3.6.0.3 3.6.0.3 3.6.0.3

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	2
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 labels to provide the evidence of tampering.

Figure 2: SmartZone 104

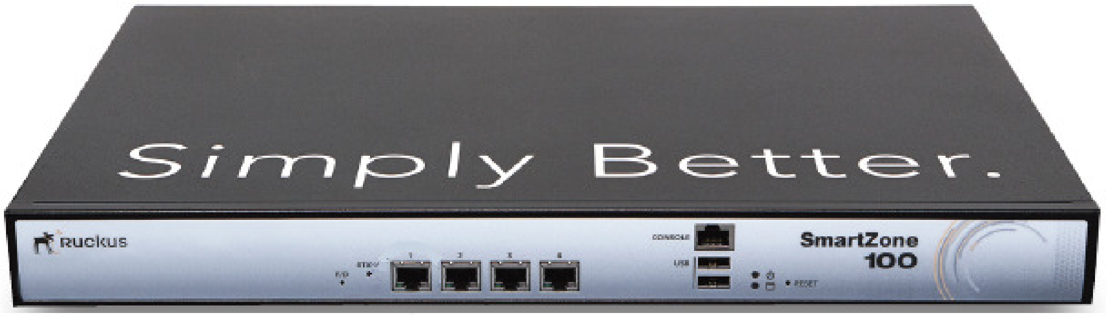


Figure 3: SmartZone 124

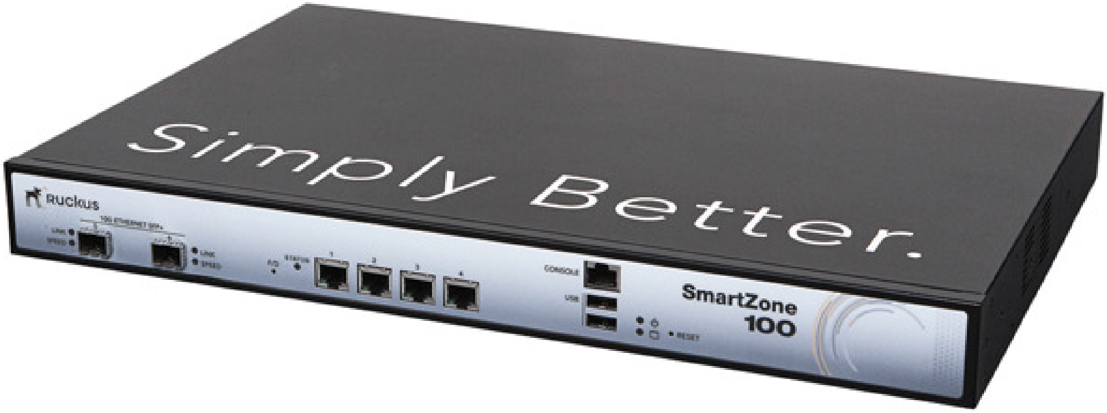


Figure 4: SmartZone 300

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. Refer to the Ruckus Wireless, Inc. FIPS Configuration Guide for more information.

The Crypto Officer must invoke the user interface using default password. The following command must be executed prior to operating the module in the FIPS mode:

```
fips enable
```

Crypto Officer must change the default password during the installation.

2.1 Approved Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 3: Approved Cryptographic Functions

CAVP Cert	Library	Algorithm	Standard	Model/Method	Key Lengths, Curves or Moduli	Use
5471	Ruckus Smartzone Controller Java Crypto Library	AES	FIPS 197 SP 800-38F, SP 800-38C, SP 800-38D	CBC Decrypt/Encrypt	128, 256	Data Encryption/ Decryption KTS (AES Cert. #5097 and HMAC Cert. #3399; key establishment methodology provides between 128 and 256 bits of encryption strength)
5097	Ruckus Smartzone SSL Crypto Library			ECB, CBC, CTR, GCM[1] Decrypt/Encrypt	128, 192, 256	
2624	Ruckus Smartzone SSL Crypto Library	Triple-DES	SP 800-67	TECB, TCBC	192	Data Encryption/ Decryption[2] KTS (Triple-DES Cert. #2624 and HMAC Cert. #3399; key establishment methodology provides 112 bits of encryption strength)
4390	Ruckus Smartzone Controller Java Crypto Library	SHA	FIPS 180-4	SHA1 SHA224 SHA256 SHA384 SHA512		Message Digest
4351	Ruckus SmartZone Controller DRBG SHA Java Crypto Library					
4145	Ruckus Smartzone SSL Crypto Library					
3627	Ruckus Smartzone Controller Java Crypto Library	HMAC	FIPS 198-1	HMAC-SHA256 HMAC-SHA384		Message Authentication KTS

CAVP Cert	Library	Algorithm	Standard	Model/Method	Key Lengths, Curves or Moduli	Use
3399	Ruckus Smartzone SSL Crypto Library			HMAC-SHA1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512		
2150	Ruckus Smartzone Controller Java Crypto Library	DRBG	SP 800-90A	Hash based		Deterministic Random Bit Generation[3]
1903	Ruckus Smartzone SSL Crypto Library			Counter Hash based HMAC based		
1322	Ruckus Smartzone SSL Crypto Library	ECDSA	FIPS 186-4		SigGen: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Digital Signature Generation and Verification
					SigVer: B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521	

CAVP Cert	Library	Algorithm	Standard	Model/Method	Key Lengths, Curves or Moduli	Use
2938	Ruckus Smartzone Controller Java Crypto Library	RSA	FIPS 186-2 FIPS 186-4	SHA224, SHA256, SHA384 SHA512 PKCS1 v1.5	RSA SigGen (186-4) 2048, 3072 RSA SigVer (186-2) 1024, 1536, 2048, 3072, 4096 RSA SigVer (186-4)) 1024, 2048, 3072 RSA SigGen (186-4) 4096	Key Generation Digital Signature Generation and Verification
2759	Ruckus Smartzone SSL Crypto Library			SHA-224 SHA-256, SHA-384, SHA-512 PKCS1 v1.5 ANSI X9.31 PKCSPSS	RSA KeyGen (186-4) 2048, 3072 RSA SigGen (186-2) 4096 RSA SigGen (186-4) 2048, 3072 RSA SigVer (186-2) 1024, 1536, 2048, 3072, 4096	
1923	Ruckus Smartzone Controller Java Crypto Library	CVL RSASP1	FIPS 186-4	PKCS 1.5	2048	RSA Signature Primitive
1922	Ruckus Smartzone Controller Java Crypto Library	TLS 1.2	SP 800-135			Key Derivation[4]
1778	Ruckus Smartzone SNMP Crypto Library	SNMP				

CAVP Cert	Library	Algorithm	Standard	Model/Method	Key Lengths, Curves or Moduli	Use
1647	Ruckus Smartzone SSL Crypto Library	TLS 1.2 SSH				
CKG (vendor affirmed)		Cryptographic Key Generation	SP 800-133			Key Generation[5]

Note 1: not all CAVS tested modes of the algorithms are used in this module.

Note 2: 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.

[1] The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288. AES-GCM is only used in TLS version 1.2.

[2] Operators are responsible for ensuring that the same Triple-DES key is not used to encrypt more than 2^16 64-bit data blocks.

[3] The minimum number of bits of entropy generated by the module is 367 bits.

[4] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

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

2.2 Non-FIPS Approved But Allowed Cryptographic Functions.

Table 4: Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
RSA Key Wrapping using 2048 bits key	Provides 112 bits of encryption strength.	Used during TLS handshake
EC DH using 224 / 256 / 384 / 521 bits key	Provides between 112 and 256 bits of encryption strength	Used during SSH handshake and TLS handshake
DH using 2048 bits key	Provides 112 bits of encryption strength.	Used during TLS handshake and SSH session establishment.
MD5		RADIUS

Algorithm	Caveat	Use
		Note: RADIUS is available in the FIPS approved mode. It is secured using TLS.
NDRNG		Used to seed SP 800-90A DRBG.

2.3 All other algorithms

Table 5: All other algorithms

Algorithm	Use
MD5	RADIUS in non-approved mode
Elliptic Curves secp256k1, sect239k1, secp224k1, sect193r1, sect193r2, secp192k1, secp192r1, sect163k1, sect163r1, sect163r2, secp160k1, secp160r1, and secp160r2	Elliptic Curve Cryptography in non-approved mode.

3. Ports and interfaces

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

Table 6.1: Ports and Interfaces of 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
USB Port	2	Not used
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
Console Port	1	Data Input, Data Output, Control Input, Status Output

Table 6.2: Ports and Interfaces of SmartZone 300

Port Name	Count	Interface(s)
Ethernet Ports: 6x 1GbE ports 4x 10GbE ports	10	Data Input, Data Output, Control Input, Status Output
USB Port	4	Not used
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

4. Roles, Services and Authentication

The module supports role-based authentication. The module supports a Crypto Officer role, a User Role, and AP Role. The Crypto Officer installs and administers the module. The Users and APs use the cryptographic services provided by the module. The module supports concurrent operators. The module provides the following services.

Table 7.1: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Self-test	Crypto Officer User	N/A
Reboot	Crypto Officer User	N/A
Zeroization	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R, E
Show status	Crypto Officer User AP	N/A

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Login	Crypto Officer User	Password: R, W SSH Keys: R, W, E TLS Keys: R,W, E DRBG seed: R, W
SSH Tunnel	Crypto Officer User AP	Password: R, W SSH Keys: R,W, E DRBG seed: R, W
Configuration	Crypto Officer	Password: R, W SSH Keys: R,W, E TLS Keys: R,W, E DRBG seed: R, W
RadSec	AP	TLS Keys: R,W, E DRBG seed: R, W
GRE Tunnel	AP	RGRE packets AES key: R,W, E
HTTPS/TLS	Crypto Officer User AP	TLS Keys: R,W,E DRBG seed: R, W
EAP authenticator	AP	SSH Keys: R,W,E DRBG seed: R, W
SNMPv3	Crypto Officer User	Password: R, W SNMP Keys: R,W,E
FIPS mode enable/disable	Crypto Officer	All: Z

The module supports the following authentication mechanisms.

Table 7.2: Authentication Mechanisms

Role	Authentication Mechanisms
User Role (Monitoring user)	Passwords (Minimum 8 characters) The module uses passwords of at least 8 printable characters. Total number of password permutations with eight characters is 95^8 = 6,634,204,312,890,625. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur due to the authentication process performance limitation. The number of attempts that are required to reach 1/100,000 far exceeds the capabilities of the equipment since billions of attempts per second would be required.
CO Role (Configuration user)	Passwords (Minimum 8 characters) The module uses passwords of at least 8 printable characters. Total number of password permutations with eight characters is 95^8 = 6,634,204,312,890,625. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur due to the authentication process performance limitation. The number of attempts that are required to reach 1/100,000 far exceeds the capabilities of the equipment since billions of attempts per second would be required.

AP Role	RSA key (2048 bits) The module uses 2048 bits RSA key, which corresponds to 112 bits of security. 2^-112 is significantly less than 1/1,000,000. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur due to the authentication process performance limitation. The number of attempts that are required to reach 1/100,000 far exceeds the capabilities of the equipment since more than billions of attempts per second would be required.

5. Cryptographic Keys and CSPs

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

Table 8: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
TLS master secret	Used to derive TLS encryption key and TLS HMAC Key	RAM in plaintext
TLS pre-master secret	Used to derive TLS master secret	RAM in plaintext
TLS AES or Triple-DES key	Used during encryption and decryption of data within the TLS protocol	RAM in plaintext
TLS HMAC key	Used to protect integrity of data within the TLS protocol	RAM in plaintext
TLS RSA keys public and private keys	Used during the TLS handshake	RAM in plaintext Hard drive in plaintext
TLS ECDSA keys public keys	Used during the TLS handshake	RAM in plaintext
TLS Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext

Key	Description/Usage	Storage
TLS EC Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: entropy input, V and Key Hash_DRBG CSPs: entropy input, V and C HMAC_DRBG CSPs: entropy input, V and Key	Used during generation of random numbers	RAM in plaintext
Passwords	Used for operator authentication	RAM in plaintext Hard drive in plaintext
Firmware update RSA key	Used to protect integrity during firmware update	RAM in plaintext Hard drive in plaintext
RGRE packets AES key	Used for establishing RGRE tunnel	RAM in plaintext
SNMP Secret	Used to establish SNMP sessions	RAM in plaintext Hard drive in plaintext
SSH AES key	Used during encryption and decryption of data within the SSH protocol	RAM in plaintext
SSH HMAC key	Used to protect integrity of data within the SSH protocol	RAM in plaintext
SSH RSA public and private keys	Used to authenticate the SSH handshake and AP	RAM in plaintext Hard drive in plaintext
SSH ECDSA public keys	Used to authenticate the SSH handshake	RAM in plaintext Hard drive in plaintext
SSH Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext
SSH EC Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext

Note: Zeroization is achieved by changing the FIPS mode from Enable to Disable OR from Disable to Enable using the fips enable or the fips disable command.

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.

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

Table 9: Self-Tests

Algorithm	Test
AES	KAT using ECB and CBC modes (encryption/decryption)
Triple-DES	KAT using ECB mode (encryption/decryption)
SHS	KAT using SHA1, SHA224, SHA256, SHA384, and SHA512
HMAC	KAT using SHA1, SHA224, SHA256, SHA384 and SHA512
SP800-90A DRBG	KAT: CTR_DRBG HASH_DRBG HMAC_DRBG
	Continuous Random Number Generator test
NDRNG	Continuous Random Number Generator test
RSA	KAT using 2048 bit key, SHA-256
	Pairwise Consistency Test
Firmware integrity	MD5 checksum during bootup
Firmware load	RSA using 4096 bit key
ECDSA	Pairwise Consistency Test (sign/verify) using P-224, K-233 and SHA512
ECC CDH	Shared secret computation

7. Physical Security

The cryptographic module consists 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 must be checked periodically by the Crypto Officer. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module.

The tamper evident seals shall be installed by either the manufacturer or the Crypto Officer for the module to operate in the approved mode of operation.

FIPS security seal application instructions

For all seal applications, Crypto Officer ensures that the following instructions are observed:

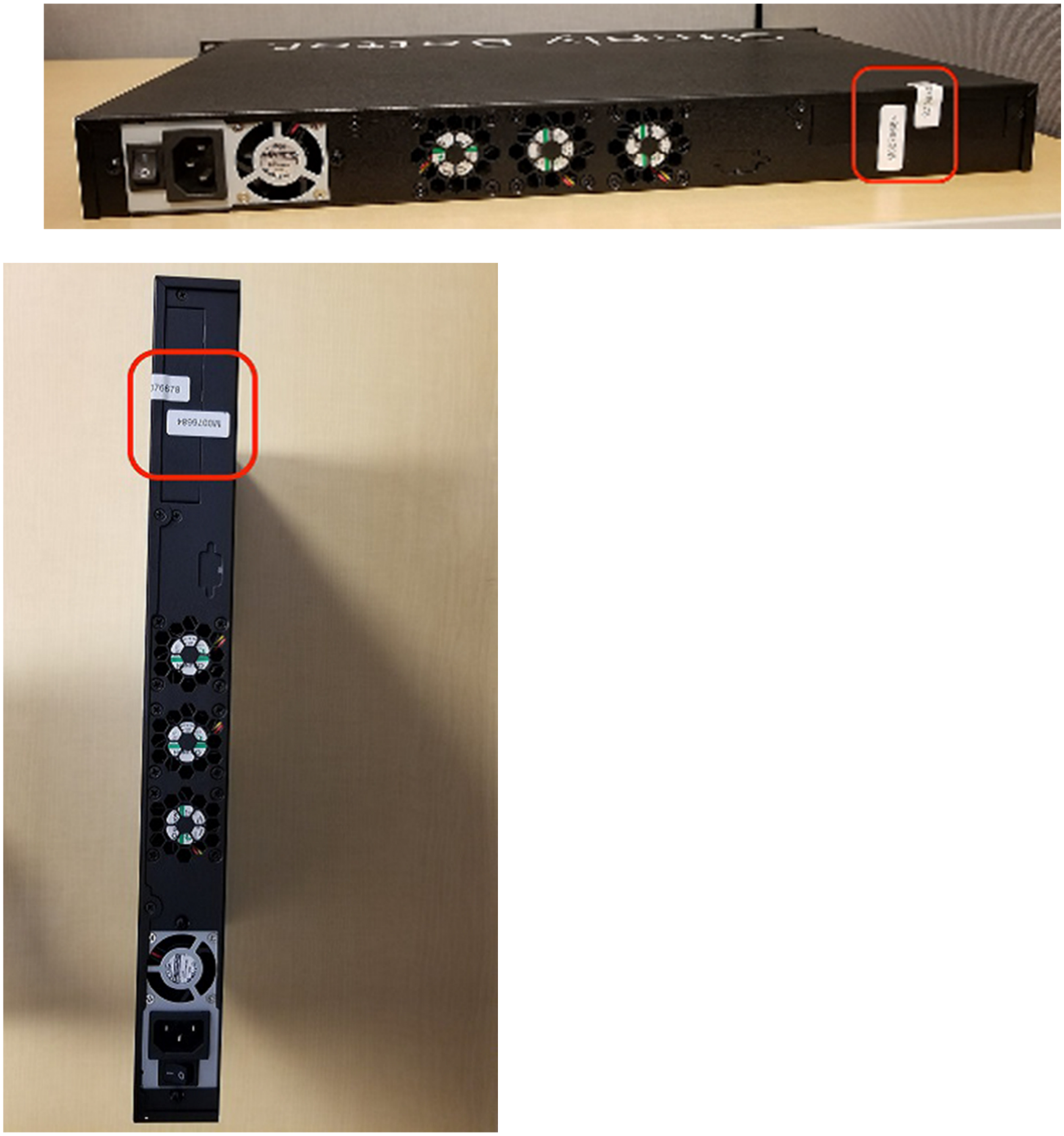
- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Do not use bare fingers to handle the labels. Slowly peel the backing from each seal, taking care not to touch 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.

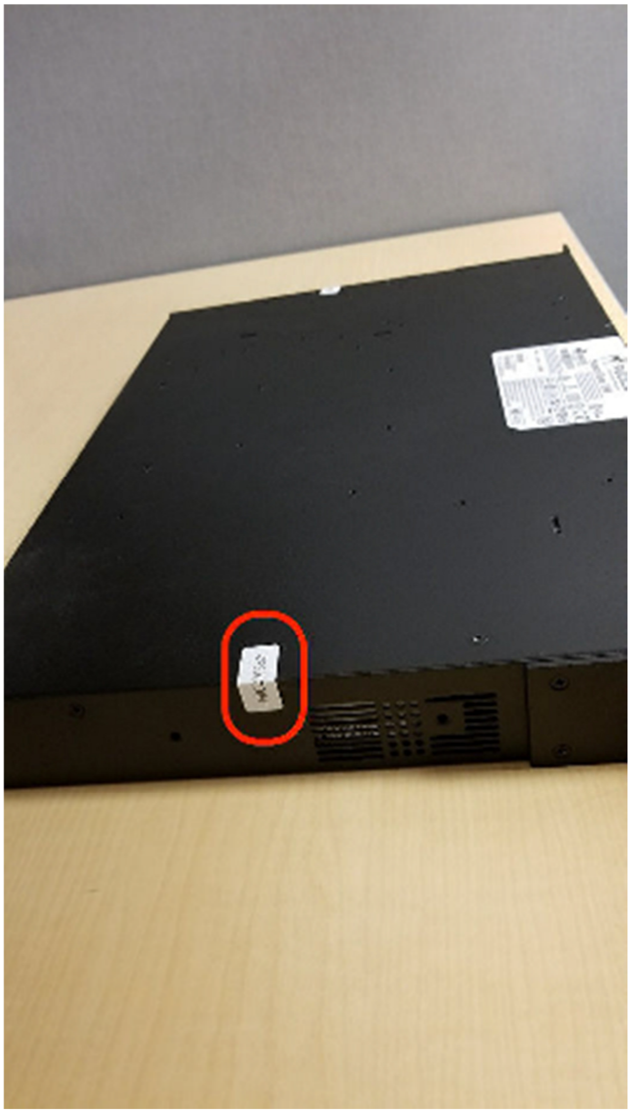
Order for seals is placed to Ruckus Wireless, Inc. through a partner/distributor and Ruckus Wireless, Inc. processes the order. The part number for the seals is XBR-000195.

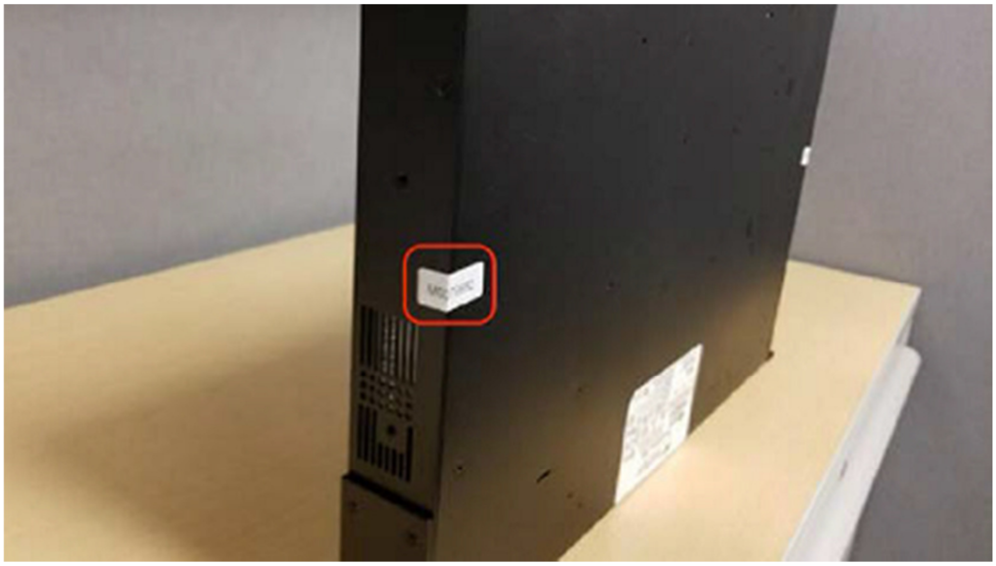
Number of seals per model: SZ-104/SZ-124 has four tamper evident seals and SZ-300 has eight tamper evident seals.

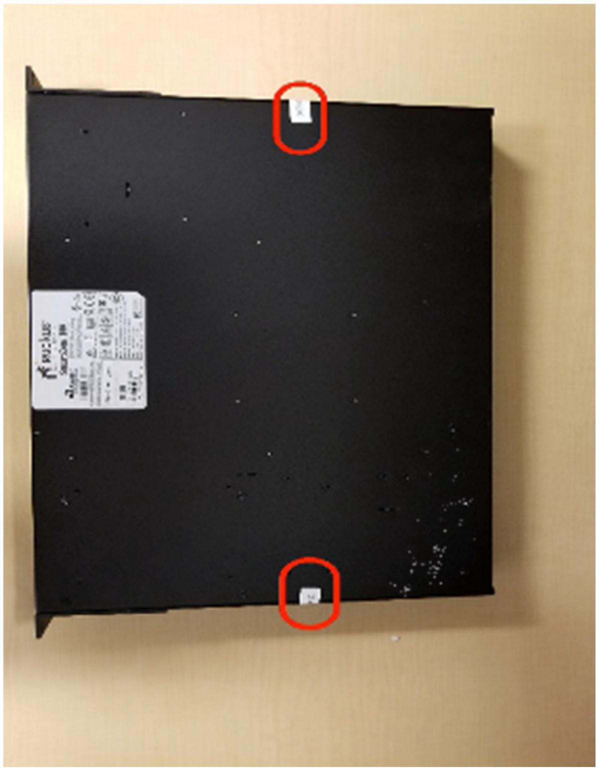
During the installation the Crypto Officer must check that the product was not damaged.

Figure 5: Tamper-evident seals on SmartZone 104 /124









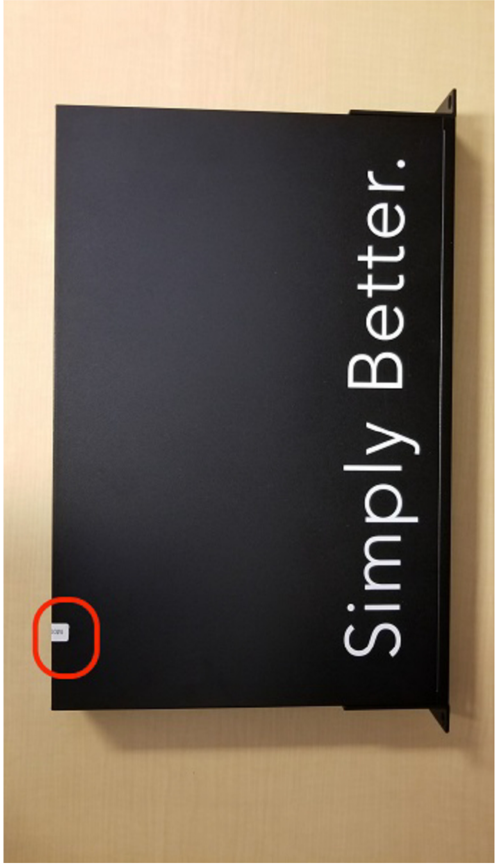
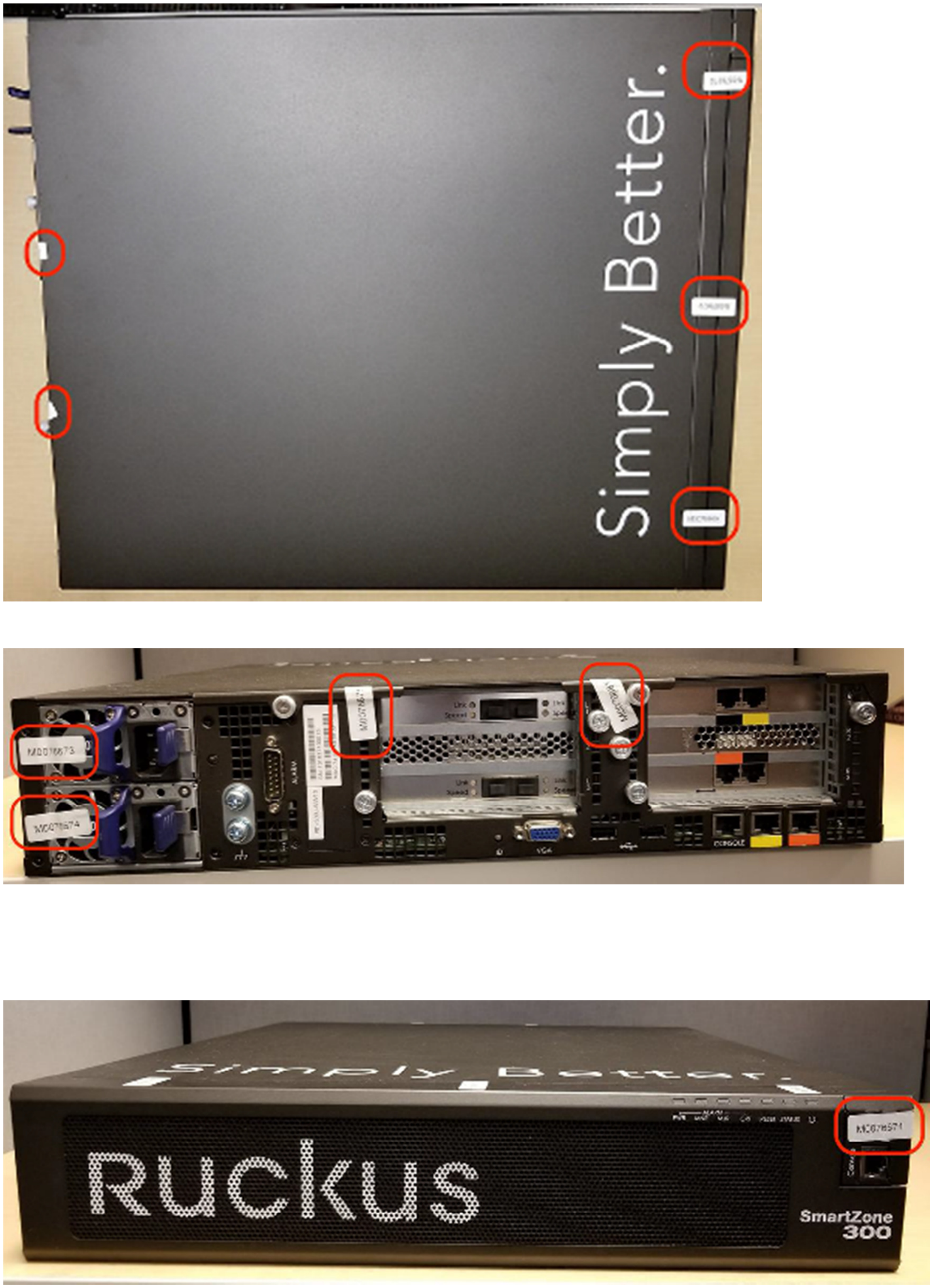

Simply Better.

Figure 6: Tamper-evident seals on SmartZone 300



8. References

Table 8: 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

Reference	Specification
[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