Ruckus Wireless, Inc.

R710 Access Point

R610 Access Point

R720 Access Point

T610 Access Point

T710 Access Point

FIPS 140-2 Level 2 Non-Proprietary Security Policy

Version Number: 1.10

Table of Contents

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 Wireless, Inc. AP and Ruckus Wireless, Inc. 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 the AP. The APs vary by the antenna support they offer, however the differences do not affect the security functionality claimed by the module.

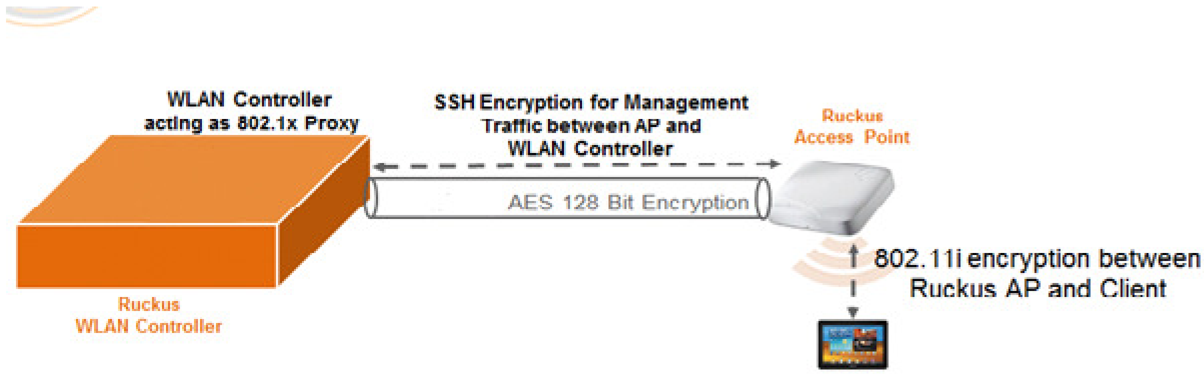


Figure 1: Encryption between AP and Controller

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

Table 1: Configurations tested by the lab.

Module Name and Version	Firmware version
R710 Access Point R610 Access Point R720 Access Point T610 Access Point T710 Access Point	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: R710 Access Point

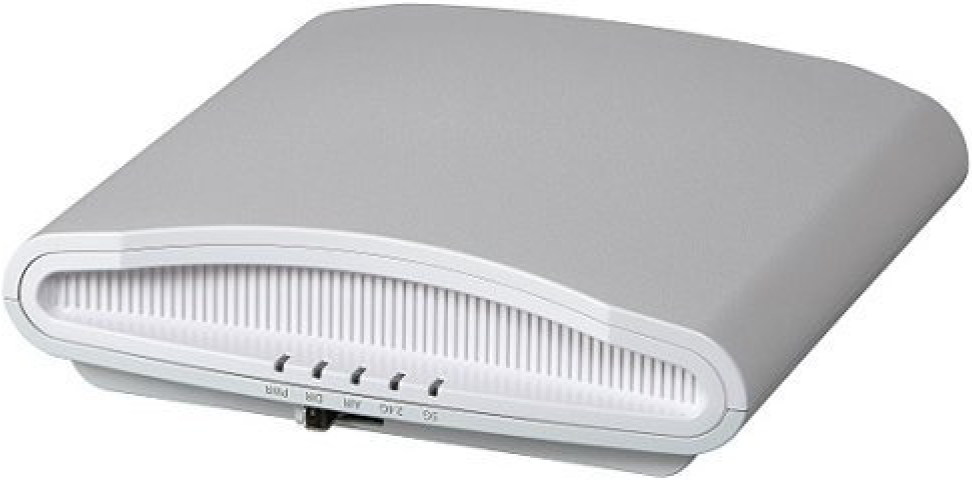


Figure 3: R610 Access Point

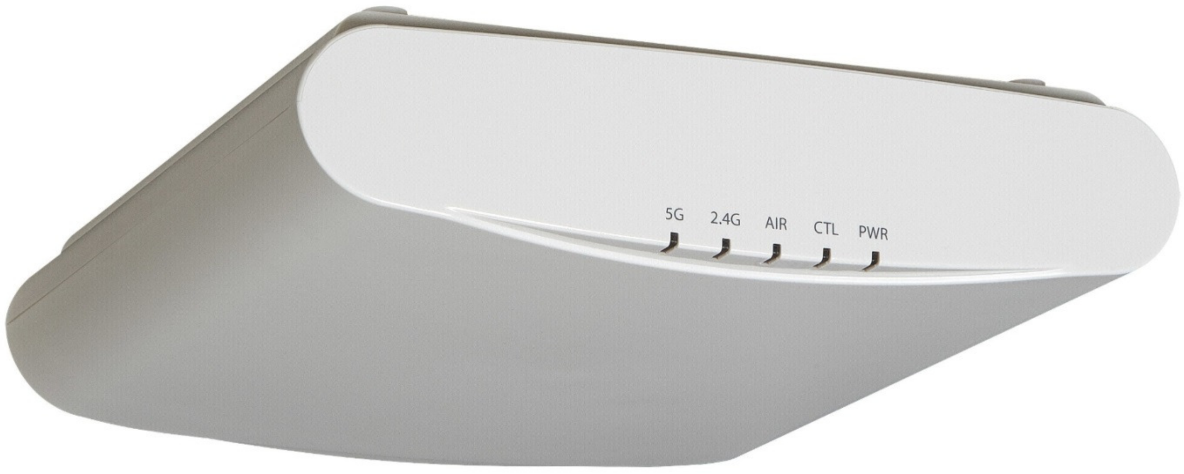


Figure 4: R720 Access Point

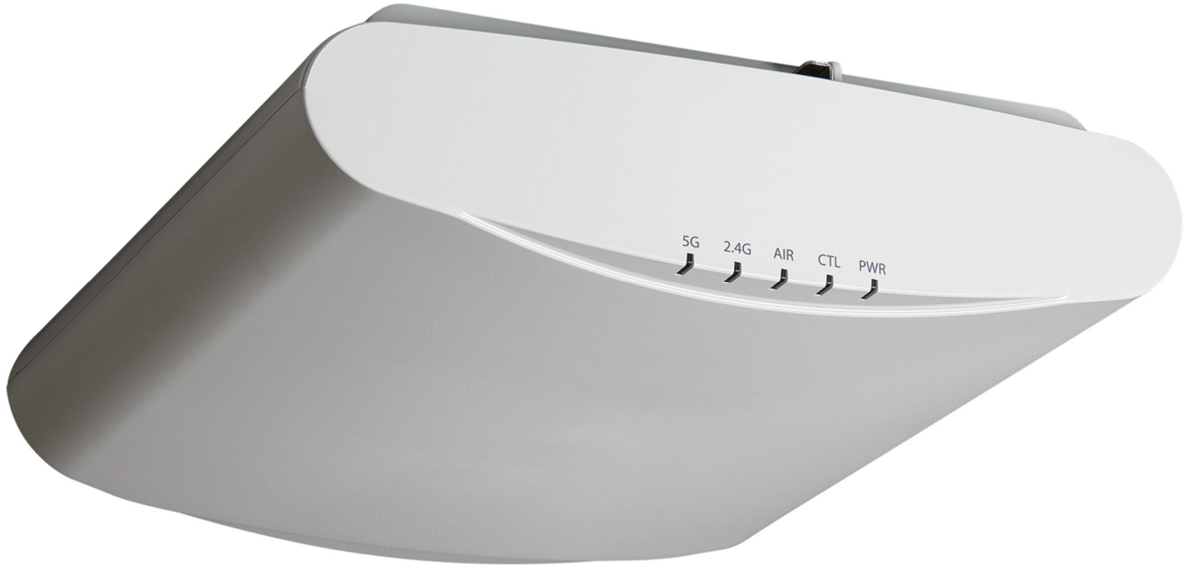


Figure 5: T610 Access Point

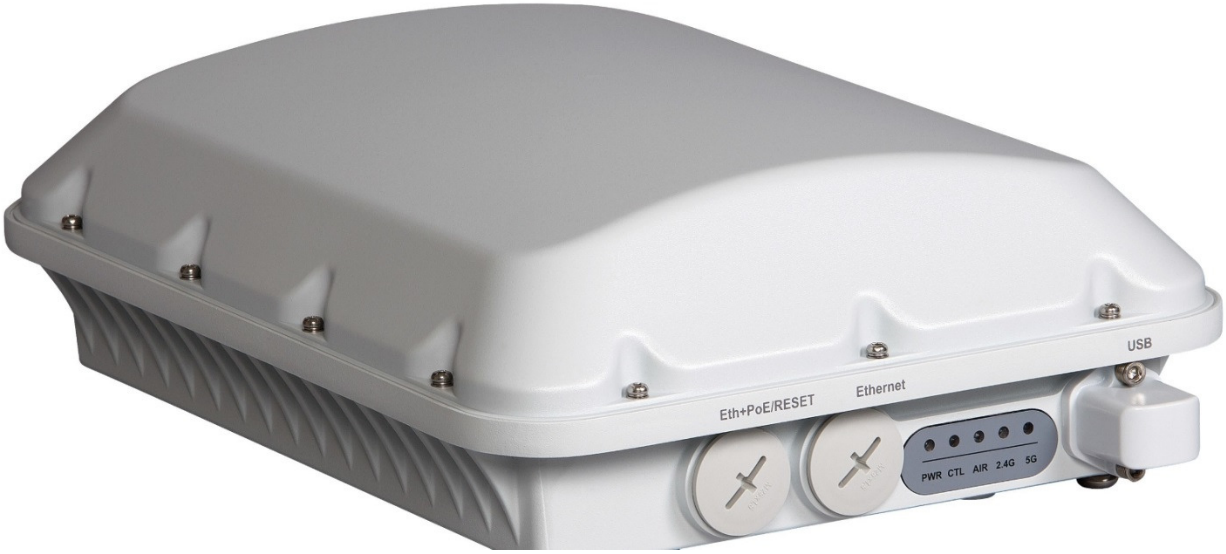
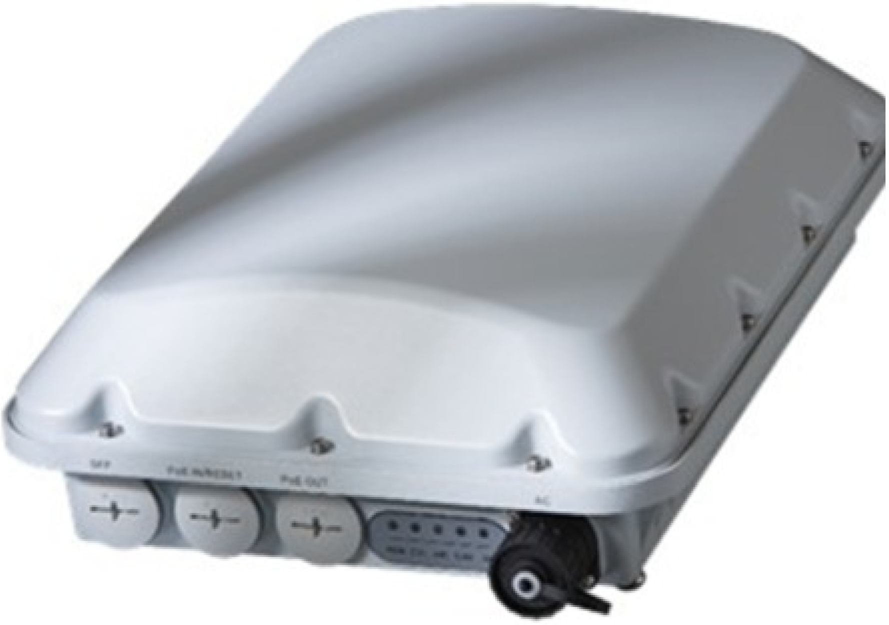


Figure 6: T710 Access Point



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

The following command must be executed prior to operating the module in the FIPS mode:
set fips-mode enable

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	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
5096 5309 5312 5381	AES	FIPS 197, SP 800-38F, SP 800-38C, SP 800-38D	ECB, CBC, CTR, GCM[5], CCM	128, 192, 256	Data Encryption/ Decryption KTS (key establishment methodology provides between 128 and 256 bits of encryption strength)
1902	DRBG	SP 800-90A	CTR_DRBG		Deterministic Random Bit Generation[1]
1321	ECDSA	FIPS 186-4		P-256, P-384, P-521	Digital Signature Generation and Verification
3398 3564	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512	160, 256, 512	Message Authentication KTS
2627	Triple-DES	SP 800-67	TECB, TCBC	192	Data Encryption/ Decryption[2] KTS (key establishment methodology provides 112

CAVP Cert	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
					bits of encryption strength)
4144 4317	SHA	FIPS 180-4	SHA-1 SHA-256 SHA-512		Message Digest
2758 2878	RSA	FIPS 186-4, FIPS186-2	SHA-1, SHA256, SHA512 PKCS1 v1.5	2048 4096 (verification only)	Digital Signature Generation and Verification
1646 1777	CVL TLS 1.2, SSH, SNMP	SP 800-135			Key Derivation[3]
199	KBKDF	SP 800-108			Key Derivation
CKG (vendor affirmed)	Cryptographic Key Generation	SP 800-133			Key Generation[4]

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

[1] The minimum number of bits of entropy generated by the module is 368 bits.

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

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

[5] 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.

2.2 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
RSA Key Wrapping using 2048 bits key	Provides 112 bits of encryption strength.	Used during TLS handshake
EC Diffie-Hellman (CVL Cert. #1646, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)	Provides between 112 and 256 bits of encryption strength	Used during TLS handshake
Diffie-Hellman (CVL Cert. #1646, key agreement; key establishment methodology provides 112 bits of encryption strength) using 2048 bits key	Provides 112 bits of encryption strength.	Used during SSH session establishment.

The module also implements other cryptographic algorithms:

Algorithm	Use
ECDSA using brainpoolP512r1, brainpoolP384r1, brainpoolP256r1, and secp256k1	Digital Signature Generation and Verification in non-approved mode

3. Ports and interfaces

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

The Access Points have similar ports, except that T610 doesn’t have a Power Receptacle and T710 has an SFP port as well as the ability to output power via Ethernet. It doesn’t have a USB port.

Table 6: Ports and Interfaces.

R720 Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input
USB Port	1	Disabled
Power Receptacle	1	Power Input

Port Name	Count	Interface(s)
Reset Button	1	Control Input
LEDs	5	Status Output

R710 Access Point

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

R610 Access Point

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

T610 Access Point

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

T710 Access Point

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output, Power Input, Power Output
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

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 7: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Self-test	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Zeroization	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R TLS Keys: R,W DRBG seed: R,W
Show status	Crypto Officer	N/A
Installation	Crypto Officer	TLS Keys: R,W DRBG seed: R, W
GRE Tunnel	Crypto Officer	RGRE tunnel RSA key: R RGRE packets AES key: R,W
SSH Tunnel	Crypto Officer	Password: R, W SSH Keys: R,W DRBG seed: R, W

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Login	Crypto Officer	Password: R, W 龜SH Keys: R,W TLS Keys: R,W DRBG seed: R, W
Secure Wireless connection for Clients	User	802.11i keys: R,W WPA2 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

The module supports the following authentication mechanisms.

Role	Authentication Mechanisms
User	802.11i Pre-shared secret The module uses 802.11i Pre-shared secret, which corresponds, at a minimum, to 112 bits of security, 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.
Crypto Officer	Passwords The module uses passwords of at least 8 characters 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.

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 pre-master secret	Used to derive TLS master secret	RAM in plaintext
TLS master secret	Used to derive TLS encryption key and TLS HMAC Key	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 public and private keys	Used during the TLS handshake	RAM in plaintext Flash in plaintext
TLS ECDSA public keys	Used during the TLS handshake	RAM in plaintext
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	Used during generation of random numbers	RAM in plaintext
Passwords	Used for user authentication	RAM in plaintext Flash in plaintext
4096 bits RSA Firmware update public key	Used to protect integrity during firmware update	RAM in plaintext Flash 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	RAM in plaintext Flash in plaintext

SSH Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext
RGRE tunnel RSA private key	Used for establishing RGRE tunnel	RAM in plaintext Flash in plaintext
RGRE packets AES key	Used for establishing RGRE tunnel	RAM in plaintext
802.11i Pairwise Master Key(PMK)	Used to derive 802.11i Pairwise Transient Key(PTK)	RAM in plaintext
802.11i Pairwise Transient Key(PTK)	All session encryption/decryption keys are derived from the PTK	RAM in plaintext
802.11i EAPOL MIC Key	Used for integrity validation in 4-way handshake	RAM in plaintext
802.11i EAPOL Encryption Key	Used for 802.11i message encryption	RAM in plaintext
802.11i Group Master Key(GMK)	Used to derive Group Transient Key(GTK)	RAM in plaintext
802.11i Group Transient Key(GTK)	Used to derive multicast cryptographic keys	RAM in plaintext
802.11i Group AES-CCM Data Encryption/MIC Key	Used to protect multicast message confidentiality and integrity (AES-CCM)	RAM in plaintext
802.11i AES-CCM session key	Used for 802.11i packet encryption	RAM in plaintext
WPA2 PSK	Used for client authentication	RAM in plaintext Flash in plaintext

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	Separate KATs (encryption/decryption)
Triple-DES	Separate KATs (encryption/decryption)

Algorithm	Test
SHS	KAT
HMAC	KAT
SP800-90A DRBG	KAT
	Continuous Random Number Generator test
NDRNG	Continuous Random Number Generator test
RSA	KAT
	Pairwise Consistency Test
Firmware integrity	MD5 checksum during bootup
Firmware update	RSA
ECDSA	Pairwise Consistency Test

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 customers 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: T610 has three tamper evident seals, T710 has 3 tamper evident seals, R610 has 2 tamper evident seals, R710 has 2 tamper evident seals and R720 has 2 tamper evident seals.

Figure 7: Tamper-evident seals on T610 Access Point

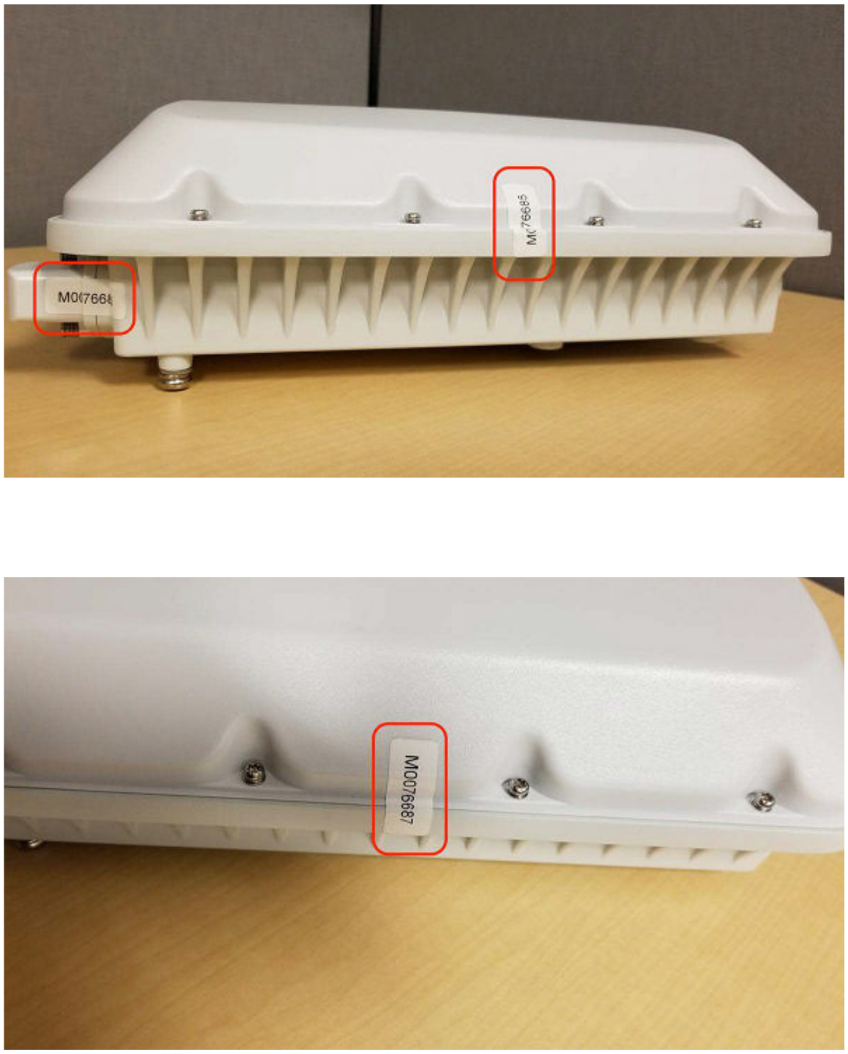


Figure 8: Tamper-evident seals on T710 Access Point

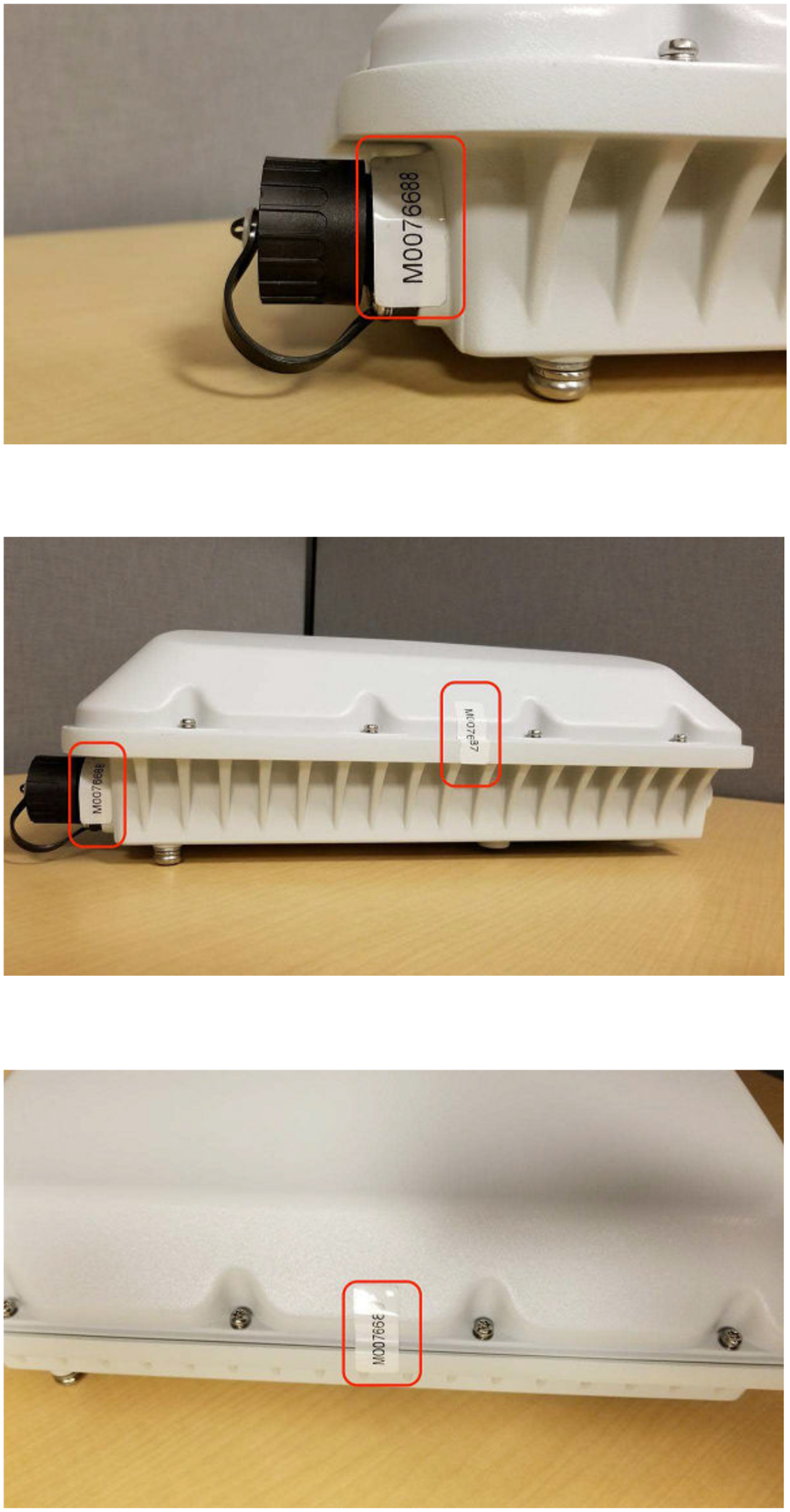


Figure 9: Tamper-evident seals on R610 Access Point

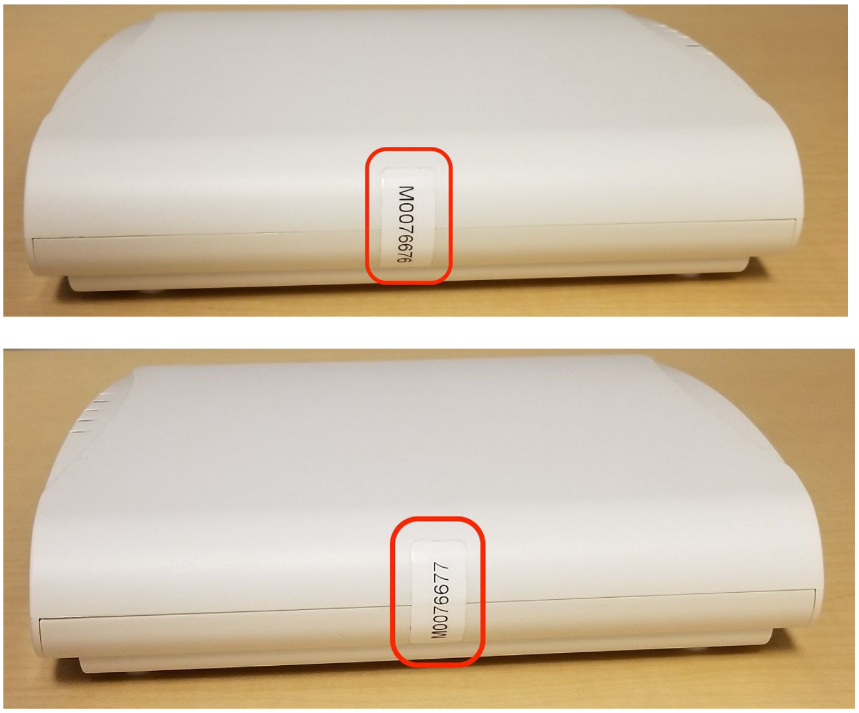
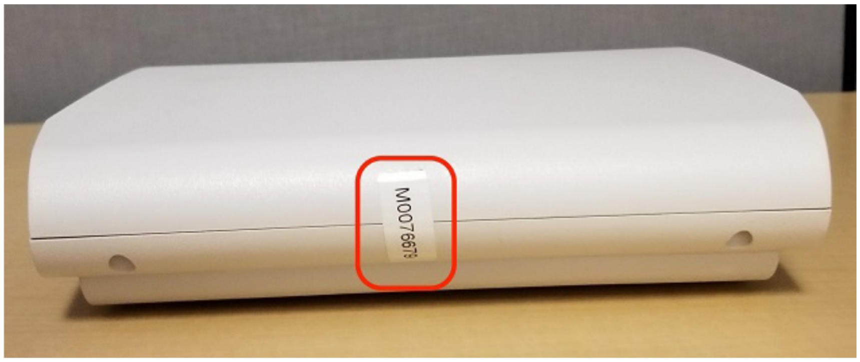


Figure 10: Tamper-evident seals on R710 Access Point



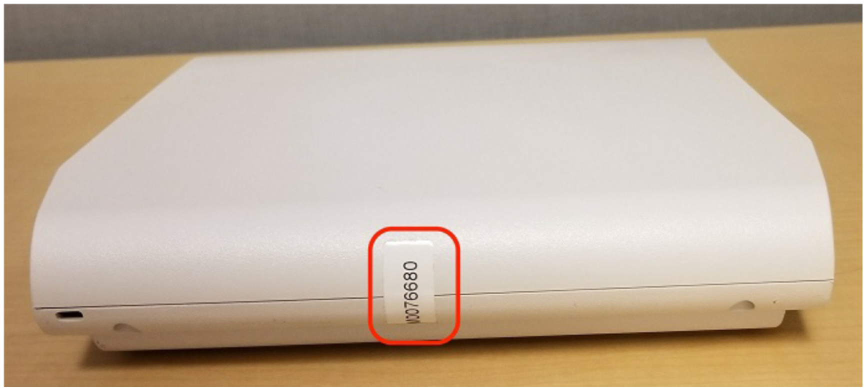
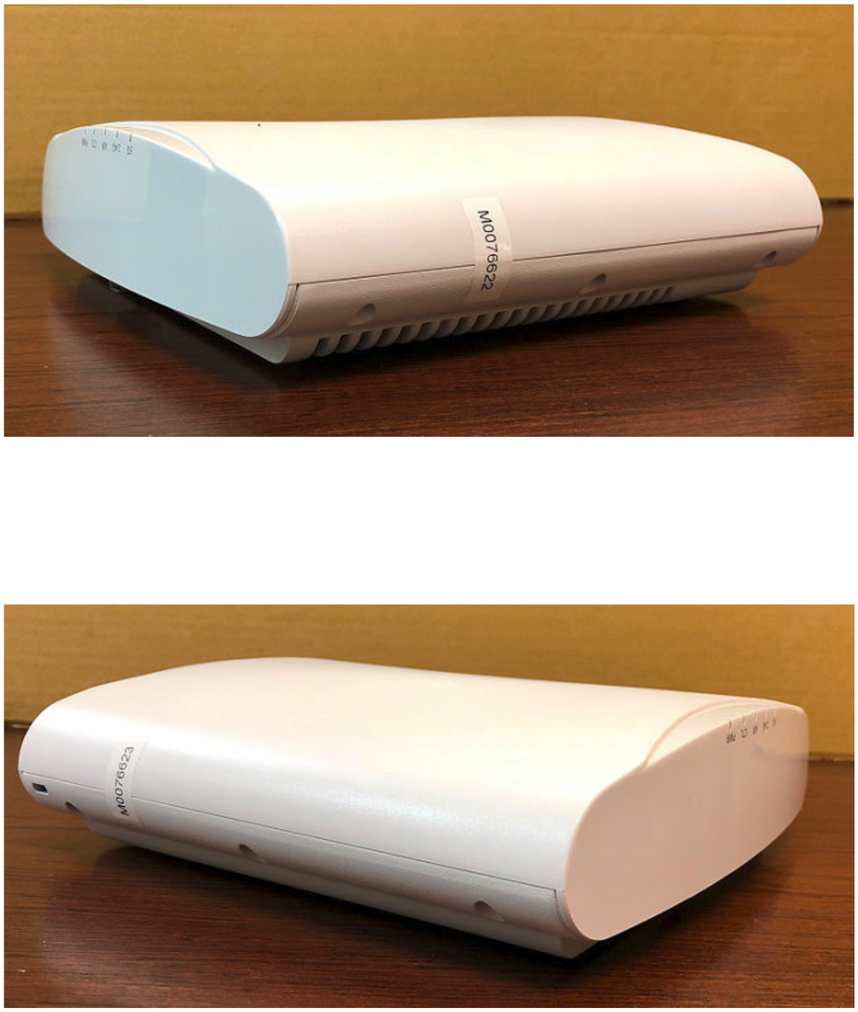


Figure 11: Tamper-evident seals on R720 Access Point



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
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

Reference	Specification
[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