Ruckus Wireless Cloudpath Enrollment System by Ruckus Wireless, Inc.

Version 5.3

FIPS 140-2 Level 1 Non-Proprietary Security Policy

Document Version Number: 4.5
Date: July 21, 2020

Table of Contents

1. Module Overview 3
2. Modes of Operation 4
   2.1 Approved and Allowed Cryptographic Functions 5
   2.2 All other algorithms 8
3. Ports and interfaces 9
4. Roles and Services 9
5. Cryptographic Keys and CSPs 11
6. Self-tests 12
7. References 13

1. Module Overview

Ruckus Wireless Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices.

Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure.

Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

This software is a cryptographic module claiming compliance to FIPS 140-2 requirements for validation.

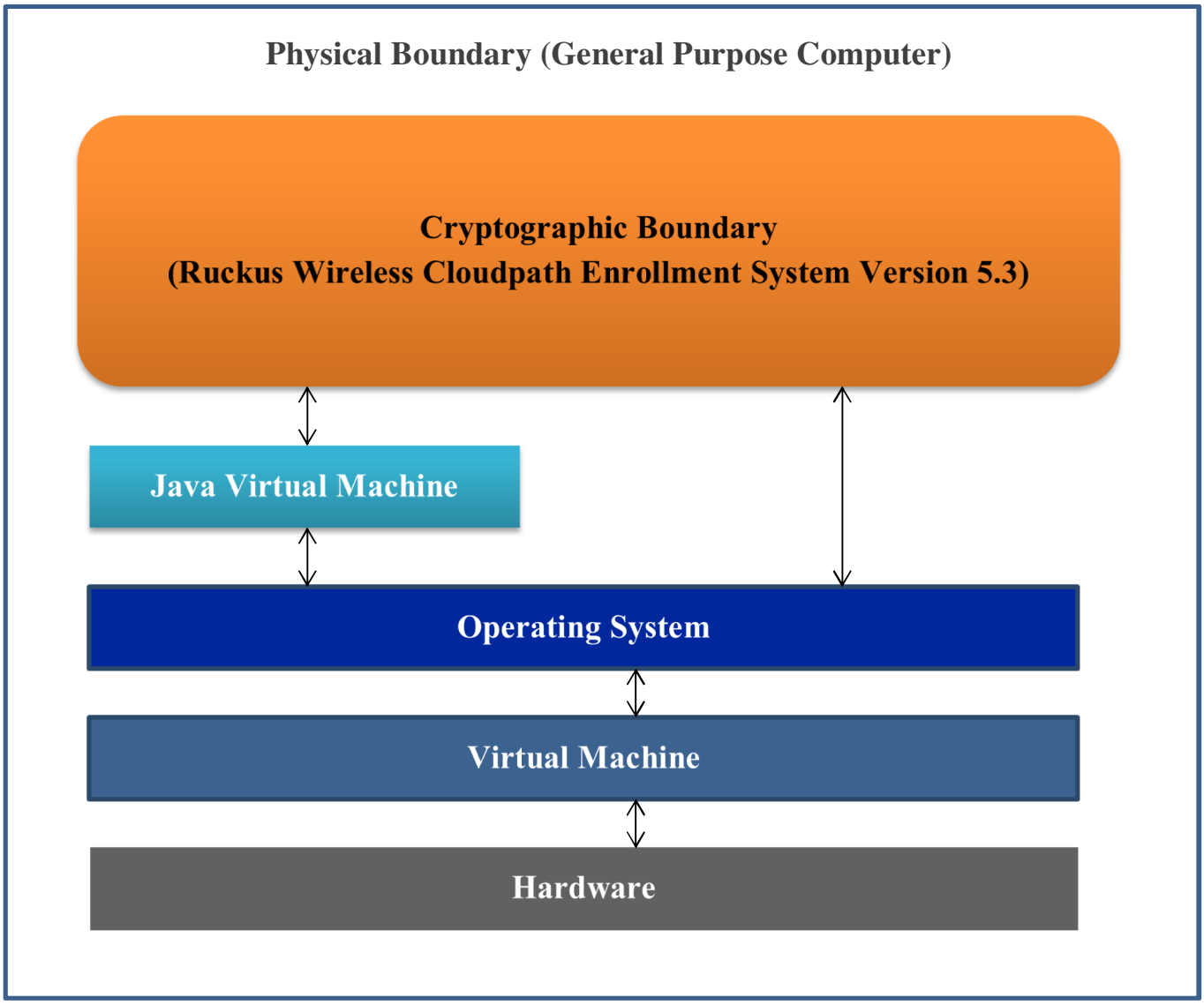
Table 1.1: Configuration tested by the lab

Module	Platform	Processors	Operating Systems
Ruckus Wireless Cloudpath Enrollment System	Dell Optiplex 7050	Intel(R) Core(TM) i7-7700 with AES-NI	Open JDK 1.7.0 on CentOS 7 on VMware ESXi 6.5
	Dell Optiplex 7050	Intel(R) Core(TM) i7-7700 with AES-NI	Open JDK 1.7.0 on CentOS 7 on Hyper-V Manager 2016

Table 1.2: Module Security Level Statement

FIPS Security Area	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 1: Block Diagram for Ruckus Wireless Cloudpath Enrollment System



2. Modes of Operation

To obtain the FIPS-compliant version, you must specify FIPS when you place your Cloudpath order. When the FIPS-compliant version is delivered, it is delivered with an activation code. A FIPS-specific activation code is required to activate the FIPS-compliant version. The FIPS-compliant version always supports FIPS mode.

The "show config" command is used to check whether the delivered version is FIPS-compliant. The output must state: "*FIPS: Enabled*"

The installation is performed by authorized personnel with crypto officer role in a secure location which is only accessible by the authorized personnel. The personnel must follow the instructions found in the security policy.

2.1 Approved and Allowed Cryptographic Functions

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

Table 2.1: Approved Cryptographic Functions.

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
5095 C1817	Cloudpath Cryptographic Library	AES	FIPS 197, SP 800-38D, SP 800-38F	ECB, CBC, CFB, CTR, GCM[4]	128, 192, 256	Data Encryption/ Decryption KTS[6]
5382	Cloudpath Cryptographic Library for Java			CBC	128, 256	
1901	Cloudpath Cryptographic Library	DRBG	SP 800-90A	Counter Hash based HMAC based		Deterministic Random Bit Generation[3]
2083	Cloudpath Cryptographic Library for Java					
1642	Cloudpath Cryptographic Library	CVL Partial DH	SP 800-56A	ECC	P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Shared Secret Computation
1846	Cloudpath Cryptographic Library for Java					
3397	Cloudpath Cryptographic Library	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 256, 384, 512	Message Authentication

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
3565	Cloudpath Cryptographic Library for Java			HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512		
1320	Cloudpath Cryptographic 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 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 ECDSA KeyGen: 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 Key Pair Generation
1421	Cloudpath Cryptographic Library for Java					
1430	Cloudpath Cryptographic Library for Java	DSA	FIPS 186-4		DSA KeyGen (186-4) DSA PQGGen (186-4) DSA PQGVer (186-4) DSA SigGen (186-4) DSA SigVer (186-4) 2048, 3072	Digital Signature Generation and Verification Key Pair Generation
1431	Cloudpath Cryptographic Library					
4143	Cloudpath Cryptographic Library	SHS	FIPS 180-4	SHA-1 SHA-224, SHA-256 SHA-384 SHA-512		Message Digest
4318	Cloudpath Cryptographic Library for Java					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
2757	Cloudpath Cryptographic Library	RSA	FIPS 186-4 FIPS 186-2	PKCS1 v1.5 ANSI X9.31 PKCSPSS SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	RSA KeyGen (186-4) 2048, 3072 RSA SigGen (186-4) 2048, 3072 RSA SigGen (186-2) 4096 RSA SigVer (186-2) 1024, 1536, 2048, 3072, 4096	Digital Signature Generation and Verification Key Generation
2879	Cloudpath Cryptographic Library for Java					
1643,	Cloudpath Cryptographic Library	CVL TLS 1.2, SSH	SP 800-135			Key Derivation[5]
1847	Cloudpath Cryptographic Library for Java					
2802	Cloudpath Cryptographic Library for Java	Triple-DES	SP 800-67	TECB, TCBC	168	Data Encryption/ Decryption[2] KTS[6]
2803	Cloudpath Cryptographic Library					
CKG (vendor affirmed)		Cryptographic Key Generation	SP 800-133			Key Generation[1]

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

[1] The module directly uses the output of the DRBG. The generated seed used in the asymmetric key generation is an unmodified output from DRBG.

[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. While the module is always intended to operate in approved mode, failure to comply with the limits would place the module in non-approved mode.

[3]The minimum number of bits of entropy generated by the module is 378 bits.

[4]The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1.
AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key.

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

[6]KTS (AES Certs. #5095 and #C1817; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (AES Certs. #5095 and #C1817 and HMAC Cert. #3397; key establishment methodology provides between 128 and 256 bits of encryption strength); KTS (AES Cert. #5382 and HMAC Cert. #3565; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (Triple-DES Cert. #2802 and HMAC Cert. #3565; key establishment methodology provides 112 bits of encryption strength); KTS (Triple-DES Cert. #2803 and HMAC Cert. #3397; key establishment methodology provides 112 bits of encryption strength).

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

Table 2.2: Non-FIPS Approved but Allowed Cryptographic Functions.

Algorithm	Caveat	Use
RSA Key Wrapping using 2048 bits key	Provides 112 bits of encryption strength	Used in TLS / SSH handshake
DH using between 2048 and 8192 bits key	Provides between 112 and 201 bits of encryption strength	Used in TLS / SSH handshake
EC DH using any NIST defined B, K and P curves except sizes 163 and 192	Provides between 112 and 256 bits of encryption strength	Used in TLS handshake
NDRNG		Used to seed SP 800-90A DRBG.

2.2 All other algorithms

Non-approved usage is within an internal protocol that is wrapped by TLS with approved algorithms when transported.

- MD5 is wrapped by TLS with RadSec,
- PKCS12 is wrapped by TLS with HTTPS

Table 2.3: Non-Approved Cryptographic Functions

Algorithm	Use	Description
MD5	RADIUS	Inherent part of RADIUS protocol
PKCS12-3DES-3DES	Certificate Authority	Archive file format for cryptographic keys

3. Ports and interfaces

The physical ports of the module are the same as those of the computer system on which it is executing. The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role and a User role.

The Crypto Officer role installs and manages the module via the Admin UI ("Administrator" and "CA Administrator" admin UI roles) and the 'cpn-service' CLI user.

The User role are end-user devices and other network infrastructure such as network switches and wireless access controllers. These Users can use the cryptographic services provided by the module for certificate assignment and certificate trust verification.

The module provides the following services.

Table 4: 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
Show status	Crypto Officer	N/A
Zeroization	Crypto Officer	All:Z
Reboot or shutdown	Crypto Officer	N/A
Configuration Using Command Line Interface	Crypto Officer	Web Server Certificate and Private Key: R, W SSH Keys: R,W DRBG seed: R,W
Admin UI: General Management	Crypto Officer	Web Server Certificate and Private Key: R, W RADIUS Server Certificate and Private Key: R, W TLS Keys: R,W DRBG seed: R.W
Admin UI: Certificate Authority Management	Crypto Officer	CA Certificate and Private Key: R,W End User Device Certificate and Private Key: R,W TLS Keys: R,W DRBG seed: R,W
Admin UI: Outgoing TLS Truststore	Crypto Officer	Trusted 3rd Party TLS Certificates & CA Certificates: R,W TLS Keys: R,W
End User Enrollment (obtaining certificate)	User	Web Server Certificate: R CA Certificate and Private Key: R End User Device Certificate and Private Key: R,W TLS Keys: R, W DRBG seed: R,W
RadSec (RADIUS over TLS)	User	CA Certificate: R RADIUS Server Certificate: R End User Device Certificate and Private Keys: R TLS Keys: R,W DRBG seed: R,W

Note:

TLS Keys means: TLS master secret, TLS pre-master secret, TLS AES or Triple-DES key, TLS HMAC key, TLS RSA public and private keys, TLS ECDSA public keys, TLS EC Diffie-Hellman public and private keys, TLS Diffie-Hellman public and private keys.

SSH Keys means: SSH AES or Triple-DES key, SSH HMAC key, SSH RSA public and private keys, SSH ECDSA public keys, SSH Diffie-Hellman public and private keys.

5. Cryptographic Keys and CSPs

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

Table 5: 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 public and private keys	Used during the TLS handshake	RAM 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
TLS Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: seed, entropy input, V and Key Hash_DRBG CSPs: seed, entropy input, V and C HMAC_DRBG CSPs: seed, entropy input, V and Key	Used during generation of random numbers	RAM in plaintext
SSH AES or Triple-DES 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

Key	Description/Usage	Storage
SSH ECDSA public and private keys	Used to authenticate the SSH handshake	RAM in plaintext
SSH Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext
CA Certificate and Private Key	Used during end user enrollment and RadSec session	RAM in plaintext
End User Device Certificate and Private Key	Used during end user enrollment	RAM in plaintext

Note: public keys are not considered CSPs

The Keys and CSPs are stored in plaintext in RAM within the module.

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.

Table 6: Self-Tests

Algorithm	Test
Software integrity	HMAC SHA256
HMAC	KAT
SHS	KAT
AES	KAT(encryption/decryption)
RSA	KAT
	Pairwise consistency test on generation of a key pair
DRBG	KAT
	Continuous Random Number Generator test
ECDSA	Pairwise consistency test during power-up
	Pairwise consistency test on generation of a key pair
NDRNG	Continuous Random Number Generator test
ECC CDH	Shared secret computation

Algorithm	Test
Triple-DES	KAT(encryption/decryption)
DSA	Pairwise consistency test during power-up
	Pairwise consistency test on generation of a key pair

7. References

Table 7: 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

Reference	Specification
[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