Ruckus Wireless Cloudpath Enrollment System

Cryptographic Library

By

CommScope Technologies LLC

Software Version 5.10

FIPS 140-2 Level 1 Non-Proprietary Security Policy

Document Version Number: 1.3
Date: December 16, 2022

Table of Contents

1. Module Overview

This document is the non-proprietary security policy for the Ruckus Wireless Cloudpath Enrollment System Cryptographic Library (ES) (hereafter referred to as the module), hereafter referred to as the cryptographic module, or Module.

The module 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. The module is classified by FIPS 140-2 level 1 multi-chip standalone embodiment. Figure 1 below demonstrates the logical cryptographic boundary of the module. All cryptographic functions are carried out within this cryptographic boundary. The physical cryptographic boundary is the General-Purpose Computer (GPC) on which the module is installed. The module performs no communication other than with the calling application (the process that invokes the module services). The module consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

The module's software version for this validation is 5.10.

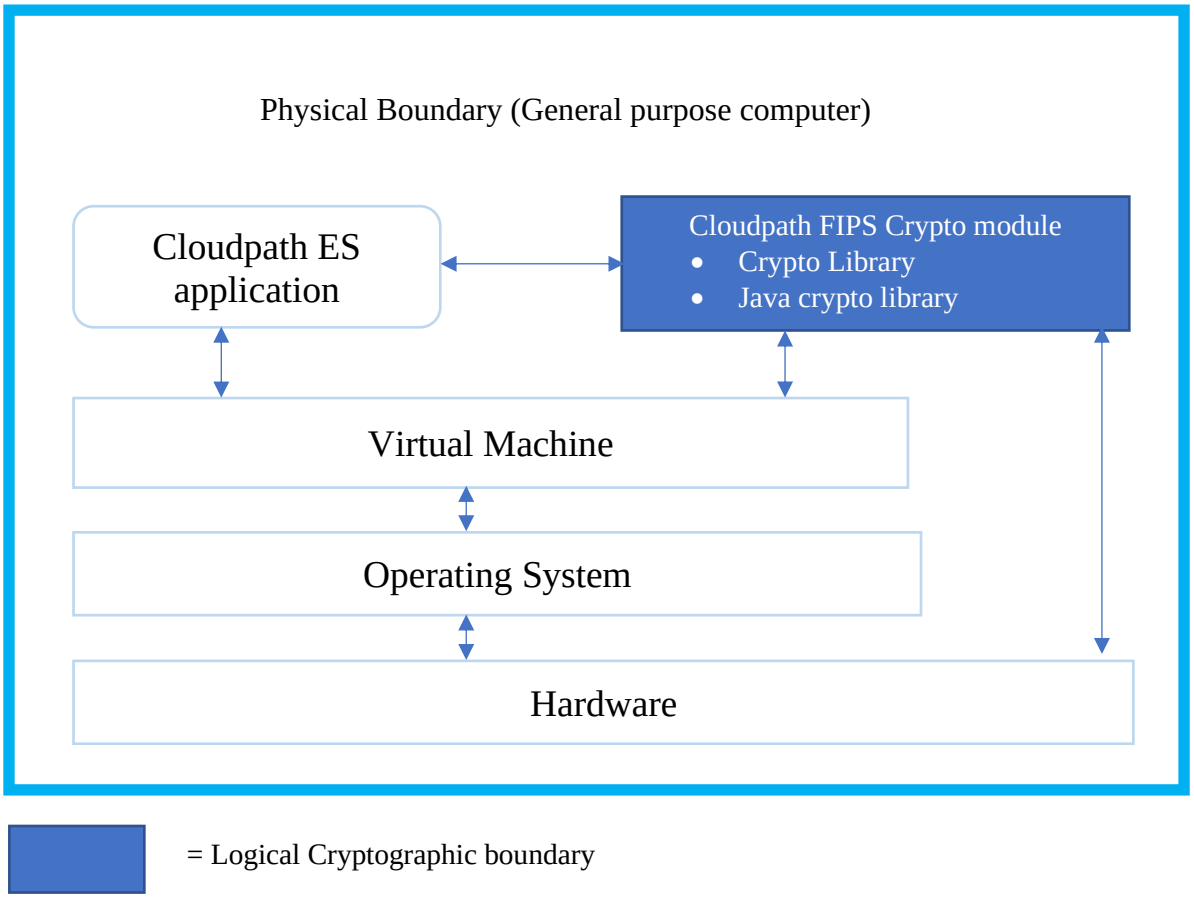

Figure 1 - Block Diagram for Cloudpath Enrollment system

The module meets the overall requirements applicable to Level 1 security for FIPS 140-2 as shown in Table 1.

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
Overall Security Level	**1**

Table 1: Module Security Level Statement

2. Modes of Operation

The module supports the following two modes of operation:

- FIPS mode (the Approved mode of operation): only approved or allowed security functions with sufficient security strength can be used.
- Non-Approved mode (the non-Approved mode of operation): when using any security functions not listed in are used.

The Module will be in FIPS-approved mode when all power up self-tests have completed successfully and only Approved or Allowed algorithms are invoked. See Tables 2 and 3 below for a list of the supported Approved algorithms and Table 4 for allowed algorithms. Otherwise, the module will be considered not in FIPS mode.

2.1. Approved Cryptographic Algorithms

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

CAVP Cert	Crypto Library	Algorithm/Standard	Model/Method	Key Lengths, Curves or Moduli	Use
A2447	Cloudpath Crypto Library	AES [FIPS 197, SP 800-38D]	ECB, CBC, CFB1, CFB8, CFB128, CTR, OFB, GCM	128, 192, 256	Data Encryption/Decryption
A2447	Cloudpath Crypto Library	DRBG [SP 800-90Arev1]	CTR_DRBG HASH_DRBG HMAC_DRBG	CTR_DRBG (AES-128,192,256); HASH_DRBG (SHA-1/224/256/384/512); HMAC_DRBG (HMAC-SHA-1/224/256/384/512)	Deterministic Random Bit Generator

CAVP Cert	Crypto Library	Algorithm/Standard	Model/Method	Key Lengths, Curves or Moduli	Use
A2447	Cloudpath Crypto Library	KAS-ECC-SSC [SP 800-56Arev3]	KAS-ECC-SSC Scheme: ephemeralUnified: KAS Role: initiator, responder	B-233, B-283, B-409, B-571, K-233, K-283, K-571, K-409, P-224, P-256, P-384, P-521	Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3 KAS-ECC-SSC: Key establishment methodology provides between 112 and 256 bits of encryption strength
A2447	Cloudpath Crypto 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
A2447	Cloudpath Crypto Library	ECDSA [FIPS 186-4]		Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	ECDSA KeyGen, KeyVer, SigGen and SigVer
A2447	Cloudpath Crypto Library	DSA [FIPS 186-4]		Capabilities: L: 2048 N: 224; Capabilities: L: 2048 N: 256; Capabilities: L: 3072 N: 256	DSA KeyGen, PGQGen, PQGVer, SigGen and SigVer
A2447	Cloudpath Crypto Library	SHS [FIPS 180-4]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest
A2447	Cloudpath Crypto Library	RSA [FIPS 186-4, FIPS 186-2]	PKCS1 v1.5 ANSI X9.31	RSA SigGen (FIPS186-4): 2048, 3072 bits; RSA SigVer (FIPS186-2): 1024, 1536, 2048, 3072, 4096 bits	RSA SigGen (FIPS186-4), SigVer (FIPS186-2)
N/A	Cloudpath Crypto Library	CKG (vendor affirmed) [SP 800-133rev2]			Vendor affirmed SP 800-133rev2 Complaint Key Generation

Table 2: Approved Cryptographic Functions for Cloudpath Crypto Library

CAVP Cert	Library	Algorithm/Standard	Model/Method	Key Lengths, Curves or Moduli	Use
A2448	Cloudpath Java Crypto Library	AES [FIPS 197, SP 800-38D]	ECB, CBC, CFB8, CFB128, CTR, GCM	128, 192, 256	Data Encryption/Decryption
A2448	Cloudpath Java Crypto Library	DRBG [SP 800-90Arev1]	CTR_DRBG HASH_DRBG HMAC_DRBG	CTR_DRBG (AES-128,192,256); HASH_DRBG (SHA-1/224/256/384/512); HMAC_DRBG (HMAC-SHA-1/224/256/384/512)	Deterministic Random Bit Generator
A2448	Cloudpath Java Crypto Library	KAS-ECC-SSC [SP 800-56Arev3]	KAS-ECC-SSC Scheme: fullMqv: KAS Role: initiator, responder staticUnified: KAS Role: initiator	B-233, B-283, B-409, B-571, K-233, K-283, K-571, K-409, P-224, P-256, P-384, P-521	Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3 KAS-ECC-SSC: Key establishment methodology provides between 112 and 256 bits of encryption strength
A2448	Cloudpath Java Crypto 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
A2448	Cloudpath Java Crypto Library	ECDSA [FIPS 186-4]		Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	ECDSA KeyGen, KeyVer, SigGen and SigVer
A2448	Cloudpath Java Crypto Library	DSA [FIPS 186-4]		Capabilities: L: 2048 N: 224; Capabilities: L: 2048 N: 256; Capabilities: L: 3072 N: 256	DSA KeyGen, PGQGen, PQGVer, SigGen and SigVer
A2448	Cloudpath Java Crypto Library	SHS [FIPS 180-4]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest

CAVP Cert	Library	Algorithm/Standard	Model/Method	Key Lengths, Curves or Moduli	Use
A2448	Cloudpath Java Crypto Library	RSA [FIPS 186-4, FIPS 186-2]	PKCS1 v1.5 ANSI X9.31 PKCSPSS with SHA-1 SHA-224 SHA-256 SHA-384, SHA-512	RSA KeyGen (186-4) 2048, 3072 bits; RSA SigGen (186-4) 2048, 3072 bits; RSA SigVer (FIPS186-4) 1024, 2048, 3072 bits; RSA SigVer (186-2) 1024, 1536, 2048, 3072, 4096 bits	RSA KeyGen, SigGen, SigVer (FIPS186-4), SigVer (FIPS186-2)
N/A	Cloudpath Java Crypto Library	CKG (vendor affirmed) SP 800-133rev2			Vendor affirmed SP 800-133rev2 Complaint Key Generation

Table 3: Approved Cryptographic Functions for Cloudpath Java Crypto Library

Notes:

1. Not all CAVP tested modes of the algorithms are used in this module.

2. 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 Rev2, Section 3.3.1. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possiblevalues 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.

   In addition, for deterministic construction of AES GCM IV the IV must be constructed with the first 32 bits as a unique identifier (e.g., name of module) and use at least 32 bits as a deterministic non-repetitive counter for a combined IV length between 64 bits and 128 bits. The encryption of blocks must be aborted if the counter part of the IV exhausts the maximum number of possible values for a given encryption key. Per IG A.5, in the event module power is lost and restored the consuming application must ensure that any of its AES-GCM keys used for encryption or decryption are re-distributed.

3. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP 800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.

2.2. Non-Approved but Allowed Cryptographic functions

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

Algorithm	Caveat	Use
RSA Key Wrapping using 2048bits key	Provides 112 bits of encryptionstrength	Used in TLS / SSH handshake

Table 4: Non-FIPS Approved but Allowed Cryptographic Functions.

2.3. Non-Approved Not Allowed Cryptographic functions

The following non-approved not allowed cryptographic algorithms shall not be used in FIPS approved mode of operation.

Algorithm	Use/Description
MD5	Used by RADIUS protocol handshakes
PKCS12-3DES-3DES	Archive file format for cryptographic keys
SP 800-135 KDF (KDF-SSHv2 and KDF-TLSv1.2 due to the lack of KDF self-test)	Used for key derivation

Table 5: Non-Approved not Allowed Cryptographic Functions.

Note: Prior to using any of the non-approved services in Table 5, the Crypto Officer must zeroize all CSPs which were used in the approved 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 11 of this document to put the module into the FIPS mode.

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.

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

Table 6: FIPS 140-2 Logical Interfaces.

4. Roles, Services and Authentication

The Module implements both authorized roles: The Crypto-Officer (CO) and User. The Module does not support user authentication. The CO and user roles are implicitly assumed by the entity accessing services implemented by the Module. No further authentication is required. The Module does not allow concurrent operators.

The Module does not provide a maintenance role or bypass capability.

All services implemented by the Module are listed below, along with a description of service CSP access. The access types are determined as follows:

- R – Read or Execute
- W – Write or Create
- Z - Zeroize

Service	Roles	Description	Access Type
Installation	CO	Module installation.	**N/A**

Service	Roles	Description	Access Type
		CSP: None	
Initialize	CO, User	Module initialization. CSP: None	**N/A**
Self-test	CO, User	Perform self-tests, including software integrity verification. CSP: None	N/A
Show status	CO, User	Functions providing module status information. CSP: None	N/A
Zeroization	CO, User	Function to destroy all CSP's	R, W, Z
Random Number Generation	CO, User	Used for random number generation. CSPs: Entropy input string, DRBG seed, DRBG V and DRBG Key	R, W
Asymmetric Key Generation	CO, User	Used to generate asymmetric keys. CSPs: RSA SGK, RSA SVK, ECDSA SGK, ECDSA SVK, DSA SGK and DSA SVK	R, W
Symmetric encrypt/decrypt	CO, User	Used to encrypt or decrypt data. CSPs: AES EDK, AES-GCM key, AES-KW key	R, W
Message Digest	CO, User	Used to generate a SHA-1 or SHA-2 message digest. CSP: None	R, W
Keyed Hash	CO, User	Used to generate or verify data integrity with HMAC. CSP: HMAC key	R, W
Signature Generation and Verification	CO, User	Used to generate or verify RSA or ECDSA digital signatures. CSPs: RSA SGK, RSA SVK, ECDSA SGK, ECDSA SVK, DSA SGK and DSA SVK	R, W
Reboot or shutdown	CO, User	Reboot/Shutdown CSP: None	N/A
EC Diffie-Hellman Keypairs Generation	CO, User	EC Diffie-Hellman Keypairs Generation CSP: EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key	R, W
EC Diffie-Hellman Shared Secret Computation	CO, User	EC Diffie-Hellman Shared Secret Computation CSP: EC Diffie-Hellman Shared Secret	R, W
TLS Handshakes Initialization	CO, User	TLS Handshakes Initialization CSP: TLS Pre-Master Secret, TLS Master Secret	R, W

Table 7: Roles and Services

5. Cryptographic Keys and CSPs

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

#	CSP/Key Name	Description
1	RSA SGK	RSA (2048/3072 bits) signature generation key
2	RSA KDK	RSA (2048 bits) key decryption (private key transport) key
3	ECDSA SGK	FIPS 186-4 ECDSA (P-224/P-256/P-384/P-521 Curves) signature generation key
4	DSA SGK	FIPS 186-4 DSA (2048/3072 bits) signature generation key
5	AES Key	AES (128/192/256 bits) encrypt/decrypt key
6	AES GCM Key	AES (128/192/256 bits) encrypt/decrypt/generate/verify key
7	HMAC Key	Keyed hash key (160/224/256/384/512 bits)
8	SP800-90Arev1 DRBG CSPs	V (128 bits), Seed (256/320/384 bits) and Key (AES 128/192/256 bits), Entropy input (384 bits from entropy source)
9	EC Diffie-Hellman Public Key	EC Diffie-Hellman public key (B-233, B-283, B-409, B-571, K-233, K-283, K-571, K-409, P-224, P-256, P-384, P-521)
10	EC Diffie-Hellman Private Key	EC Diffie-Hellman KAS-ECC-SSC private key (B-233, B-283, B-409, B-571, K-233, K-283, K-571, K-409, P-224, P-256, P-384, P-521)
9	EC Diffie-Hellman Shared Secret	EC Diffie-Hellman Shared Secret (B-233, B-283, B-409, B-571, K-233, K-283, K-571, K-409, P-224, P-256, P-384, P-521)
10	RSA SVK	RSA (1024/2048/3072 bits) signature verification public key
11	RSA KEK	RSA (2048 bits) key encryption (public key Transport) key
12	ECDSA SVK	ECDSA (P-224/P-256/P-384/P-521 Curves) signature verification public key
13	DSA SVK	FIPS 186-4 DSA (2048/3072 bits) signature verification public key
14	TLS Pre-Master Secret	Shared secret, used in TLS exchange for TLS sessions.
15	TLS Master Secret	Shared secret, used in TLS exchange for TLS sessions.
16	Software Integrity Key	Software integrity test key using HMAC-SHA-256 key

Table 8: Cryptographic Keys and CSPs

Notes:

- Public keys are not considered CSPs
- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP 800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.

For all CSPs and Public Keys

Storage: RAM, associated to entities by memory location. The Module stores DRBG state values for the lifetime of the DRBG instance. The Module uses CSPs passed in by the calling application on the stack or registers. The Module does not store any CSP persistently (beyond the lifetime of an API call), with the exception of DRBG state values used for the Modules' default key generation service.

Generation: The Module implements SP 800-90Arev1 compliant DRBG services for creation of symmetric keys, and for generation of elliptic curve and RSA keys. The calling application is responsible for storage of generated keys returned by the Module.

FIPS 140-2 IG 7.14 1 (b) is applicable to this Module. The Module, a software library based in user space will request entropy from the Operational Environment within the physical cryptographic boundary as appropriate to the security strength and seeding configuration for the DRBG that is using it. The minimum number of bits of entropy requested per each GET function call is at least 256 bits.

For operation in the Approved mode, the module users (the calling applications) shall use entropy sources that contain at least 256 bits of entropy. To ensure full DRBG strength, the entropy sources must meet or exceed the security strengths.

Entry: All CSPs, including AES key and HMAC Key, enter the Module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

Output: The Module does not output CSPs, other than as explicit results of key generation services. However, none cross the physical boundary.

Destruction: Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. In addition, the Module provides functions to explicitly destroy CSPs related to random number generation services. The calling application is responsible for parameters passed in and out of the module.

Private and secret keys as well as seeds are provided to the Module by the calling application and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the Module defined API. The operating system protects memory and process space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An authorized application as user (Crypto Officer and User) has access to all key.

6. Physical Security

The module is a software entity only and thus does not claim any physical security.

7. Operational Environment

The Module will operate in a modifiable operational environment per the FIPS 140-2 definition. The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The external application that makes calls to the Module is the single user of

the Module, even when the application is serving multiple clients.

The Module was tested in the following configurations.

Operating Environment	Processor	Platform
CentOS 7 on VMware ESXi 6.7	Intel Xeon Gold 6230 CPU with PAA	Dell PowerEdge R540
CentOS 7 on VMware ESXi 6.7	Intel Xeon Gold 6230 CPU without PAA	Dell PowerEdge R540

Table 9: Configuration tested by the lab

8. EMI/EMC

The module is a software module. Therefore, the only electromagnetic interference produced is that of the host platform on which the module resides and executes. FIPS 140-2 requires that the host systems on which FIPS 140-2 testing is performed meet the Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15.

9. Self-tests

At start-up, Known Answer Tests (KATs) and software integrity check are performed. These tests are automatic and do not need operator intervention. If the value calculated and the known answer do not match, the Module immediately enters into the error state. Once the Module is in the error state, the Module becomes unusable via any interface.

The Module implements each of the following Power On Self-Tests (POST):

Software Integrity Test:

- HMAC-SHA-256

Cloudpath Crypto Library Power On Self-Test:

- AES-CBC encryption and decryption KATs
- AES-GCM encryption and decryption KATs
- DSA power on self-tests (sign/verify)
- ECDSA power on self-tests (sign/verify)
- SP 800-90Arev1DRBG Health Tests: Generate, Reseed, Instantiate functions (per Section 11.3 of SP 800-90Arev1)
- HMAC KATs (HMAC-SHA-1/256/512)
- KAS-ECC-SSC Primitive Z KAT
- RSA KATs (separate KAT for signing; separate KAT for verification)
- SHA KATs (SHA-1/256/512)

Cloudpath Java Crypto Library Power On Self-Test:

- AES-CBC encryption and decryption KATs
- AES-GCM encryption and decryption KATs

- DSA power on self-tests (sign/verify)
- ECDSA power on self-tests (sign/verify)
- SP 800-90A90Arev1 DRBG KAT (Note: DRBG health tests as specified in SP800-90A Section 11.3 are performed)DRBG Health Tests: Generate, Reseed, Instantiate functions (per Section 11.3 of SP 800-90Arev1HMAC KATs (HMAC-SHA-1/256/512)
- KAS-ECC-SSC Primitive Z KAT
- RSA KATs (separate KAT for signing; separate KAT for verification)
- SHA KATs (SHA-1/256/512)

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by power-cycling the host platform.

Conditional self-tests are run during operation of the module. If any of these tests fail, the module will enter the error state, where no services can be accessed by the operators. The module can be reinitialized to clear the error and resume FIPS mode of operation. Each module performs the following conditional self-tests.:

Cloudpath Crypto Library conditional self-tests:

- DSA PWCT
- ECDSA PWCT

Cloudpath Java Crypto Library Power On Self-Test:

- DSA PWCT
- ECDSA PWCT
- RSA PWCT

Entropy Health Tests

The module's entropy source conducted the following Self-Tests:

1. ENT (NP) SP800-90B Start-Up Health Tests:
   - Repetition Count Test (RCT)
   - Adaptive Proportion Test (APT)

Note: Please refer to SP800-90B, sections 4.4.1 and 4.4.2 for more information about the RCT and APT.

2. ENT (NP) SP800-90B Continuous Health Tests:
   - Repetition Count Test (RCT)
   - Adaptive Proportion Test (APT)

10.Physical Security

There are no physical security requirements as this is a software module.

11.Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The Crypto Officer shall make sure the module with software version 5.10 installed. In addition, only FIPS approved services and their associated FIPS approved and FIPS allowed cryptographic algorithms as identified in this Security Policy shall be used while in a FIPS approved mode.

12.Mitigation of Other Attacks

The Module is not designed to mitigate any specific attacks outside the scope of FIPS 140-2. These requirements are not applicable.

13.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 800-56Arev3]	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 800-90Arev1]	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 800-135rev1]	Recommendation for Existing Application –Specific Key Derivation Functions

Table 9: References