Mist Systems

FIPS AP43

FIPS 140-2 Non-Proprietary Security Policy

Document Revision: V1.1

F.W. Version: fips_apfw-0.9.23115-illyrio-9e5f

H.W. Version: AP43-FIPS-US (REV. AA and AB) and AP43E-FIPS-US (REV. AA and AB)

Table of Contents

REVISION HISTORY

Author(s)	Version	Date	Description
Gurpreet Singh	1.0	August 15th, 2022	Initial Release
Santosh Rokade	1.1	December 12th, 2022	Updated firmware version, hardware version, and figures 1-12. Updated Tables 6 and 11 for additional services in non-FIPS Approved Mode of Operation.

1. INTRODUCTION

This is a FIPS 140-2 Non-Proprietary Security Policy for Mist Systems FIPS AP43 Cryptographic Module. The module is a multi-chip standalone cryptographic module designed for the wireless space supporting a secure Firmware Upgrade and other features.

The AP43 and AP43E modules, hereby referred to as the "cryptographic module" or simply "module" in the context of this document, are similar in form fit and function. The difference between the modules is internal [AP43] vs. external antennas [AP43E]. Both modules execute the identical version of the FIPS Validated firmware and employ the same Physical Security Mechanisms.

Table 1 - Module version information

Module Name	Hardware Version	Firmware Version
FIPS AP43	AP43-FIPS-US [REV. AA and AB]	fips_apfw-0.9.23115-illyrio-9e5f
	AP43E-FIPS-US [REV. AA and AB]	

NOTE: Any firmware loaded into the module with a version not showing in the module certificate is out of scope of this validation and requires a separate FIPS 140-2 validation.

2. SECURITY LEVEL SPECIFICATION

The module achieves an overall of Security Level 2 for FIPS 140-2.

Table 2 - Security Level

Security Requirements Area	Level
Cryptographic Module Specification	2
Cryptographic 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

3. CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary of the module is the contiguous physical perimeter of the plastic enclosure (outlined in red below).

Figure 1- AP43 Front Side (REV. AA on top, AB on bottom)

Figure 2 - AP43 Back Side (REV. AA on top, AB on bottom)

Figure 3 - AP43 Top Side (REV. AA on top, AB on bottom)

Figure 4 - AP43 Bottom Side (REV. AA on top, AB on bottom)

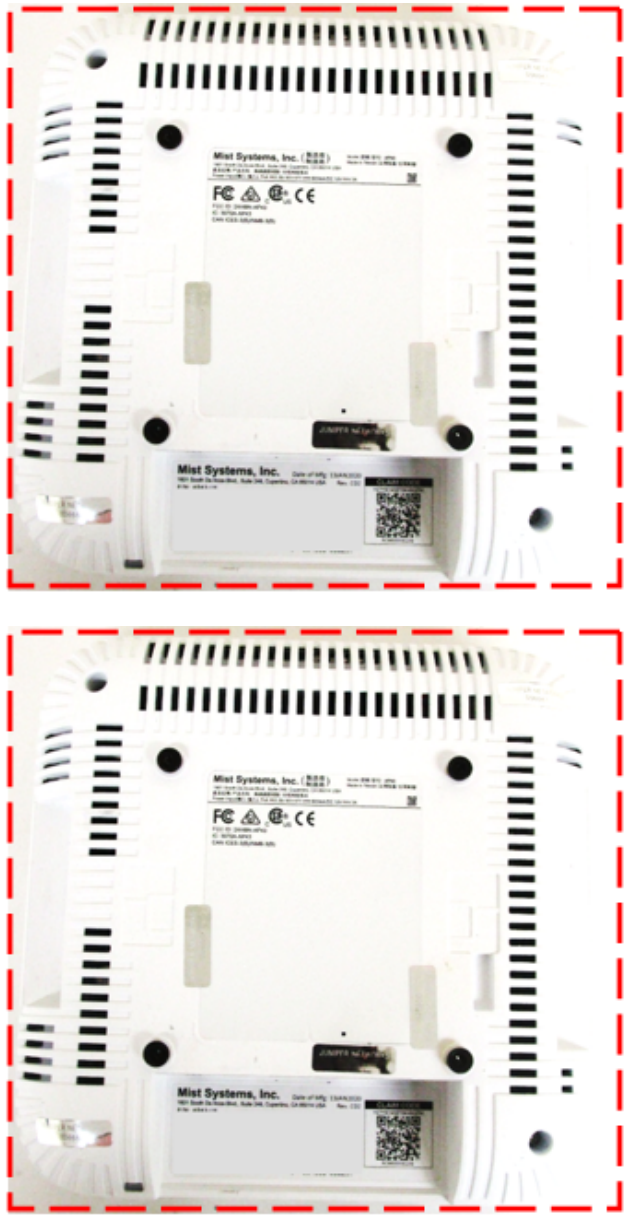


Figure 5 - AP43 Left Side (REV. AA on top, AB on bottom)

Figure 6 - AP43 Right Side (REV. AA on top, AB on bottom)

Figure 7- AP43E Front Side (REV. AA on top, AB on bottom)

Figure 8 - AP43E Back Side (REV. AA on top, AB on bottom)

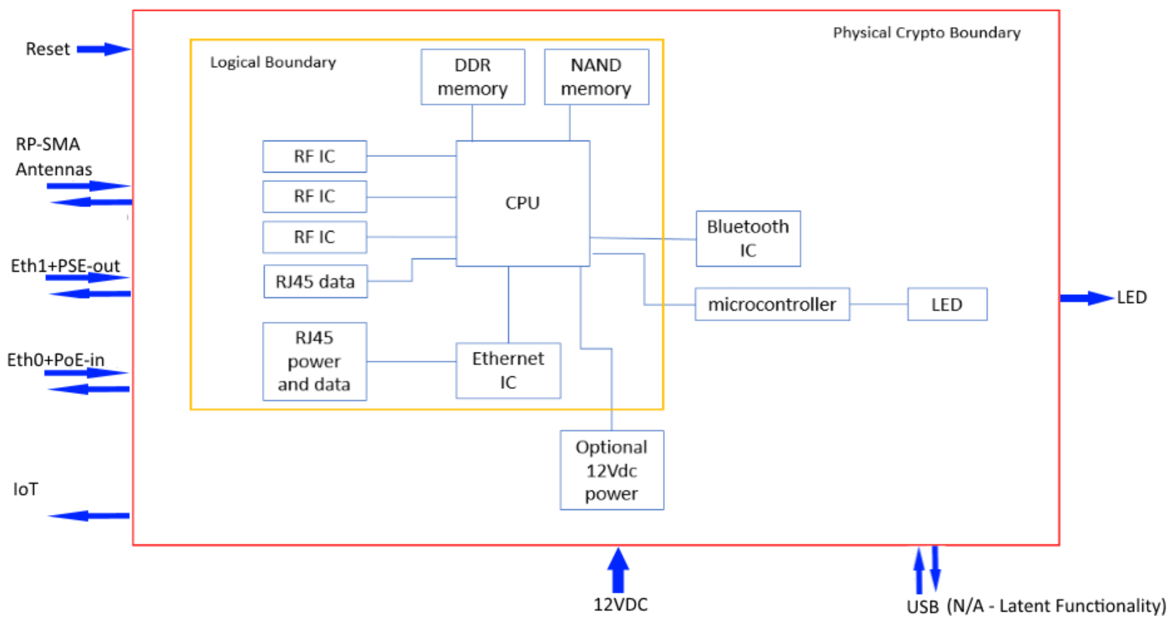
Figure 9 - AP43E Top Side (REV. AA on top, AB on bottom)

Figure 10 - AP43E Bottom Side (REV. AA on top, AB on bottom)

Figure 11 - AP43E Left Side (REV. AA on top, AB on bottom)

Figure 12 - AP43E Right Side (REV. AA on top, AB on bottom)

Figure 13 - Block Diagram of the module



All security related components are enclosed within the opaque enclosure; the enclosure is protected by Tamper Evident Labels (TELs). There are non-security components inside of the enclosure which are excluded from the FIPS 140-2 requirements. The components do not process any cryptographic operations, and even if malfunctioning or misused, they cannot cause a compromise under any reasonable condition to the security of the module. Excluded components listed below:

- Capacitors
- FETs
- Resistors
- RF Filters
- Connectors
- Ground Test Point
- Ground
- 32KHz Crystal
- Inductors
- Power converters
- Power Diodes
- Unpopulated jumper connector
- Isolation ICs for Power
- DC-to-DC Converters
- Power Transformer

4. PHYSICAL PORTS AND LOGICAL INTERFACES

Below is a description of physical ports and corresponding logical interfaces supported by the cryptographic module.

Table 3 - Specification of Cryptographic Module Physical Ports and Logical Interfaces

Physical Port	FIPS 140-2 Logical Interface	Description
Reset	Control Input	Physical button; reset to factory settings.
RP-SMA Antennas	Data Input and Data output	**AP43 (Internal Antennas)** Four 2.4GHz omni-directional antennas with 4 dBi peak gain and Four 5GHz omni-directional antennas with 6 dBi peak gain **AP43E (External Antennas)** Six RP-SMA Male connectors (four dual-band for client radios; two dual-band for 3rd radio)
Eth1+PSE-out	Data Input, Data Output, Control Input, Status Output, Power	10/100/1000Base-T; RJ45; optional PoE PSE mode (requires 802.3bt on Eth0)
Eth0+PoE-in	Data Input, Data Output, Control Input, Status Output, Power	100/1000Base-T, 2.5GBase-T (802.3bz); RJ45; PoE PD
IoT	Data output[1]	8-pin interface for digital I/O and analog input (0 to +5V)
12VDC	Power	Input for optional DC power supply
LED	Status Output	One multi-color status LED
USB	Data Input and Data output	N/A - Latent Functionality; reserved for future use.

[1] The IoT interface does not support data input (latent-functionality); only data output is supported by the module.

5. MODES OF OPERATION

The module supports a FIPS Approved Mode of Operation and a non-FIPS Approved Mode of Operation. The module is considered to be operating in the FIPS Approved Mode of Operation when abiding by the security rules and requirements in the Security Policy. The module is shipped to the end customer in the FIPS Approved Mode of Operation.

The operator transitions into the non-FIPS Approved Mode of Operation upon any violation of the security rules set forth in this Security Policy, including execution of non-compliant services. (Please see section

5.2 Non-FIPS Approved Mode of Operation).

Any violation of the Security Policy will immediately place the module in a non-FIPS Approved Mode of Operation, and the module is not considered fit to protect sensitive but unclassified information.

5.1 FIPS Approved Mode of Operation

To invoke the FIPS Approved mode of operation the Cryptographic Officer must perform the following steps:

1. Inspect the module and confirm you have a FIPS Validated module, verify the hardware version as per Table 1 above.
2. Inspect the module and confirm the Physical Security Mechanisms are in place and untampered as described in section

3. PHYSICAL SECURITY POLICY. *(Note: The module is shipped with tamper evident labels applied.)*
4. Connect to the module via the Eth0+PoE-in interface, this interface will provide power to the module as described in Table 3.
5. After completing its power-up self-tests successfully, the module will be in the FIPS Approved Mode of Operation. The module's LED will have a Solid Green pattern to indicate to the operator that FIPS power-up self-tests passed successfully.
6. Invoke the Extended Status Report service and confirm the Firmware version of the module is as per Table 1 above.
7. **DO NOT** change the AP Configuration service to disable LED; settings shall remain ON for "Enable LEDs".

If the module encounters an Error during the self-tests, it will transition to the FIPS ERROR State. The FIPS ERROR State forces the module to reboot, the LED will turn OFF followed by the Blinking RED pattern to indicate the module is going through its boot sequence and re-executing the FIPS power-up self-tests. The module will transition to an operational state only if the power-up self-tests are successful.

It is recommended to power-cycle the module to exit the FIPS ERROR State, however if you are experiencing a rolling reboot the module has encountered an unrecoverable error and must be returned to manufacturing. A rolling reboot can be recognized by a recursive LED pattern of Blinking Red, Yellow, and Green. The pattern will flash until such a time that the operator disconnects power to the module.

Table 4 – LED Pattern Description

LED	Description
OFF	Module is powered OFF
Blinking Red	Module is executing the FIPS power-up self-tests part 1 (Uboot)
Alternating Green and Yellow	Module is executing the FIPS power-up self-tests part 2 (Linux)
Solid Green	Power-up self-tests passed and module connections ready
Blinking Yellow	Power-up self-tests passed but no ethernet link (connections not ready)
Blinking Red, Yellow, Green (Recursive)	Module has encountered an unrecoverable error; rolling reboot.

5.1.1 Self-tests

The module supports the self-tests specified in this section. Please note that self-tests run regardless if the module is in the FIPS Approved Mode of Operation or the non-FIPS Approved Mode of Operation. To run self-tests on demand, operator shall power-cycle the module.

Power-up self-tests:

1. Mist Boot SPL Firmware Integrity Test: CRC-32
2. Uboot Firmware Integrity Test: CRC-32
3. Atmega Firmware Integrity Test: EDC-32 Checksum
4. RootFS Manifest Firmware Integrity Test: openssl_mist ECDSA P-384 with SHA-384 Digital Signature Verification
5. openssl_mist ECDSA P-384 SHA-384 Sign/Verify KAT
6. openssl_mist AES-KW-128 Wrap KAT
7. openssl_mist AES-KW-128 Unwrap KAT
8. openssl_mist AES-256-CTR with DF SP800-90A DRBG KAT
9. openssl_mist AES-256-CTR with DF SP800-90A DRBG Section 11.3 Health Tests[2]
10. openssl_mist HMAC-SHA-1 KAT
11. openssl_mist HMAC-SHA-256 KAT
12. openssl_mist 802.11i KDF (SP800-108) HMAC-SHA-256 KAT
13. gocrypto_mist SHA-256 KAT
14. gocrypto_mist SHA-384 KAT
15. gocrypto_mist HMAC-SHA-256 KAT
16. gocrypto_mist HMAC-SHA-384 KAT
17. gocrypto_mist RSA 4096 SHA-256 PSS Signature Verification KAT
18. gocrypto_mist AES-GCM-128 Encrypt KAT
19. gocrypto_mist AES-GCM-128 Decrypt KAT
20. gocrypto_mist TLS V1.2 KDF (SP800-135) SHA-256 KAT
21. gocrypto_mist TLS V1.2 KDF (SP800-135) SHA-384 KAT
22. gocrypto_mist ECDSA P-384 with SHA-384 Signature Verification KAT
23. gocrypto_mist ECCCDH P-256 Primitive "Z" Computation KAT
24. R0 wireless driver BCM43694 AES-128-CCM Encrypt KAT
25. R0 wireless driver BCM43694 AES-128-CCM Decrypt KAT
26. R1 wireless driver BCM43694 AES-128-CCM Encrypt KAT
27. R1 wireless driver BCM43694 AES-128-CCM Decrypt KAT
28. SP800-90B Power-up Health Tests (RCT and APT) for ENT (P)

[2] The module supports health testing for Instantiate, Generate and Reseed functions for the AES-256-CTR with DF implementation.

Conditional self-tests:

1. Firmware Download Test: openssl_mist ECDSA P-384 with SHA-384 Digital Signature Verification
2. Continuous Random Number Generation Test for ENT (P) (32-byte comparison)
3. Continuous Random Number Generation Test for openssl_mist SP800-90A DRBG (16-byte comparison)
4. SP800-90B Continuous Health Tests for ENT (P) (RCT and APT)
5. SP800-56Ar3 Section 5.6.2.3.3 ECCCDH Full Public Key Validation for gocrypto_mist ECCCDH P-256

5.1.2 FIPS Approved Services

The module supports the following Approved Services in the FIPS Approved Mode Service.

Table 5 - FIPS Approved Services

Service	Role	Description
Power-up self-tests	None[3]	Automatically invoked by the module at boot.
Show status	None	Status of the module provided by LED.
Extended status report	None	Status report.
Upgrade	FW Download User	Firmware Upgrade service.
Reset Push button	None	Reset to Factory settings (removes all configuration). Must be pressed for 5 seconds when applying power to the module.
Reboot	CO	Control command to power-cycle the module.
Disconnect clients	CO	Control command to disconnect, deauthorize or terminate clients from the network.
Bounce Ethernet Ports	CO	Control command to toggle power of Ethernet ports.
Radio Reinit	CO	Control command to re-initialize the radios.
Network Status Test	CO	Control command to perform network statistic tests including ping, pcap, traceroute, and arp.
Configure IoT Block	CO	Configure (set and get) for IoT pins. Only data output is supported
Zeroize	CO	Control command to zeroize all CSPs.
AP Configuration	CO	Modify the device configuration of the AP such as LED brightness.

[3] Unauthenticated services will be assigned "None" as the role. By virtue of being unauthenticated, a CO or User can also execute the service.

Service	Role	Description
TLSV1.2 EP Terminator	CO	Support for TLS V1.2 secure communication between the AP and the Cloud.
RADIUS	User	Support for RADIUS authentication within 802.1X.
802.1X WPA2	User	Support for 802.1X Port-Based Network Access Control.
WPA2	User	Support for 802.11i Wi-Fi Protected Access (WPA) II.
Bonjour	CO	Support for bonjour network service discovery protocol.
L2TP	CO	Support for Layer 2 Tunneling Protocol (Tunneling of TLS V1.2 traffic).
BLE	CO	Support for Bluetooth Low Energy (BLE) beacons.
MESH	CO	Support for mesh network configuration.
ALS	CO	Support for AeroScout Real-Time Location Services (ALS).
Network configure	CO	Control commands to configure network settings, limits, routing, DNS, etc.

5.2 Non-FIPS Approved Mode of Operation

The module is operating in a non-FIPS Approved Mode of Operation when the operator executes non-compliant services. Please note any violation of the Security Policy will immediately place the module in a non-FIPS Approved Mode of Operation, and the module is not considered fit to protect sensitive but unclassified information.

5.2.1 Non-compliant Services

Executing any of the following services, will place the module in the non-FIPS Approved mode of Operation:

Table 6 - Non-compliant Services

Service	Role	Description
QoS Learn	CO	Non-compliant service unavailable for testing (reserved for future use).
SSHv2 IP Tunnel	CO	Non-compliant SSHv2 communication from Cloud to AP.
IPSec	CO	Non-compliant IPSec service unavailable for testing (reserved for future use).
RADSec	CO	Non-compliant RADSec service unavailable for testing (reserved for future use).

6. ALGORITHMS

The module supports the following approved algorithms in the FIPS Approved Mode of Operation. Only algorithms, modes and key sizes specified within this section are supported by the module. (i.e. other algorithms, modes and key sizes specified by CAVP certificates not listed within this section are NOT supported by the module).

Table 7 captures the algorithms implemented by the openssl_mist implementation. The BCM49408(Arm Cortex A-53) CPU is the operational environment for these algorithms.

Table 7 - Approved Algorithms implemented by openssl_mist implementation

CAVP Cert	Algorithm	Standard	Mode	Length	Use
A1759	AES	FIPS 197 SP 800-38A	CTR	256	DRBG Prerequisite
A1759	AES	FIPS 197 SP 800-38A	ECB	128	AES-KW Prerequisite
A1759	AES	SP 800-38F	KW	128	Key wrapping and unwrapping
Vendor affirmed	CKG	SP 800-133r2	N/A	N/A	Cryptographic Key Generation
A1759	DRBG	SP 800-90Ar1	AES Counter DRBG (with DF)	256	Random Number Generation
A1759	ECDSA	FIPS 186-4	SigVer	P-384	Signature Verification
N/A	ENT	SP 800-90B	N/A	N/A	Entropy Source
A1759	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA2-256	160, 256	Message Authentication
A1759	KBKDF	SP 800-108	Counter (HMAC-SHA2-256)	N/A	Key Based Key Derivation
A1759	KTS	SP 800-38F	KW	128	Key wrapping and unwrapping; key establishment methodology provides 128 bits of encryption strength
A1759	SHS	FIPS 180-4	SHA-1 SHA2-256 SHA2-384	N/A	Message Digest

Table 8 captures the algorithms implemented by the gocrypto_mist implementation. The BCM49408(Arm Cortex A-53) CPU is the operational environment for these algorithms. These algorithms are used to support the "TLS V1.2 EP Terminator" service, this service facilitates the TLS V1.2 communications to/from the module.

Table 8 – Approved Algorithms implemented by gocrypto_mist implementation

CAVP Cert	Algorithm	Standard	Mode	Length	Use
A1758	AES	FIPS 197 SP 800-38A	ECB	128, 256	AES-GCM Prerequisite
A1758	AES	SP 800-38D	GCM	128, 256	Data Encryption/ Decryption
A1758	CVL	SP 800-135r1	TLS V1.2 KDF[4] (SHA2-256, SHA2-384)	N/A	Key Derivation
A1758	ECDSA	FIPS 186-4	SigVer	P-384	Signature Verification
A1758	ECDSA	FIPS 186-4	KeyGen	P-256	Key Generation
A1758	HMAC	FIPS 198-1	HMAC-SHA2-256 HMAC-SHA2-384	256, 384	Message Authentication
(KAS-SSC Cert. #A1758, CVL Cert. #A1758)	KAS[5]	SP 800-56Ar3	N/A	P-256	Key Agreement; key establishment methodology provides 128 bits of encryption strength
A1758	KAS-SSC	SP 800-56Ar3	KAS-ECC-SSC Ephemeral Unified	P-256	Shared Secret Computation
KTS (AES Cert. #A1758)	KTS	SP 800-38D	GCM	128, 256	Key wrapping and unwrapping; key establishment methodology provides 128 or 256 bits of encryption strength
A1758	RSA	FIPS 186-4	SigVer PKCSPSS	4096	Signature Verification

[4] No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.
[5] SP 800-56A Rev3 compliant key agreement scheme, where testing is performed separately for the shared secret computation and for a KDF compliant with SP 800-135 Rev1. No key confirmation. Per FIPS 140-2 IG D.8 Scenario X1 path (2).

CAVP Cert	Algorithm	Standard	Mode	Length	Use
A1758	SHS	FIPS 180-4	SHA2-256 SHA2-384	N/A	Message Digest

Table 9 captures the algorithms implemented by the R0/R1 wireless driver BCM43694 implementation. The BCM43694 RF IC is the operational environment for these algorithms. These algorithms are used to support the "802.1x WPA2" and "WPA2" services of the module which support AES-128-CCM Data Encryption & Decryption.

Table 9 – Approved Algorithms implemented by R0/R1 wireless driver BCM43694 implementation

CAVP Cert	Algorithm	Standard	Mode	Length	Use
C1273 and C1274	AES	FIPS 197 SP 800-38A	ECB	128	AES-CCM Prerequisite
C1273 and C1274	AES	SP 800-38C	CCM	128	Data Encryption/ Decryption

Table 10 - Allowed Algorithms

Algorithm	Caveat	Use
MD5 (no security claimed)	Non-approved cryptographic algorithm used to facilitate an insecure communications channel (L2TP) which tunnels an already secure channel (TLS V1.2 traffic). No security claimed as per FIPS 140-2 IG 1.23 – option 2c.	L2TP Service (Tunneling of TLS V1.2 traffic)
SHA-1 (no security claimed)	Non-approved cryptographic algorithm used to facilitate an insecure communications channel (L2TP) which tunnels an already secure channel (TLS V1.2 traffic). No security claimed as per FIPS 140-2 IG 1.23 – option 2c.	L2TP Service (Tunneling of TLS V1.2 traffic)
HMAC-SHA-1 (no security claimed)	Non-approved cryptographic algorithm used to facilitate an insecure communications channel (L2TP) which tunnels an already secure channel (TLS V1.2 traffic). No security claimed as per FIPS 140-2 IG 1.23 – option 2c.	L2TP Service (Tunneling of TLS V1.2 traffic)

Algorithm	Caveat	Use
HMAC-MD5 (no security claimed)	Non-approved cryptographic algorithm used to facilitate an insecure communications channel (L2TP) which tunnels an already secure channel (TLS V1.2 traffic). No security claimed as per FIPS 140-2 IG 1.23 – option 2c.	L2TP Service (Tunneling of TLS V1.2 traffic)
L2TP Key Transforms (no security claimed)	Non-approved algorithm used to facilitate random number generation for an insecure communications channel (L2TP) which tunnels an already secure channel (TLS V1.2 traffic). No security claimed as per FIPS 140-2 IG 1.23 – option 2c.	L2TP Service (Tunneling of TLS V1.2 traffic)

The module supports the following Non-Approved Algorithms in the non-FIPS Approved Mode of Operation.

Table 11 - Non-Approved Algorithms

Algorithm(s)	Non-compliant Service Mapping
AES-128-CTR (non-compliant), AES-256-CTR (non-compliant), DH 2048 (non-compliant), DRBG (SP800-90A AES-256-CTR) (non-compliant), ECDH P-256, P-384, P-521 (non-compliant), ECDSA P-256, P-384, P-521 (non-compliant), HMAC-SHA-256 (non-compliant), HMAC-SHA-512 (non-compliant), RSA 2048 (non-compliant), SSHv2 KDF (non-compliant)	SSHv2 IP Tunnel
AES-256-CTR (non-compliant), AES-256-GCM (non-compliant), DH 4096-bit MODP group (non-compliant), DRBG (SP800-90A AES-256-CTR) (non-compliant), EdDsa Ed25519 (non-compliant), IKEv2 KDF SHA-512 (non-compliant), SHA-512 (non-compliant)	IPSec
AES-128-GCM (non-compliant), AES-128-CBC (non-compliant), DRBG (SP800-90A AES-256-CTR) (non-compliant), ECDH P-256 (non-compliant), ECDSA P-384 (non-compliant), RSA 4096 (non-compliant), SHA-256 (non-compliant), TLS V1.2 KDF (non-compliant)	RADSec

7. IDENTIFICATION AND AUTHENTICATION POLICY

The module supports a Cryptographic Officer (CO), a User and a FW Download User. The module does support concurrent operators. The module supports role-based authentication.

The CO is responsible for installation and initialization of the module as per Section 5.1 of the Security Policy. After installation, the CO can access the module over TLS V1.2 and perform the authenticated services defined for the role in Section 5.1.2 FIPS Approved Services. Module can support only one CO at a time.

The User operates the module in the field and accesses the module over 802.11i Wi-Fi Protected Access (WPA) II. Please see Section 5.1.2 FIPS Approved Services for more information on the services available to the User. Module can support up to 256 Users simultaneously.

The FW Download User can only perform the Upgrade service, and is authenticated using ECDSA P-384 SHA-384 Digital Signature Verification. Module can support only one FW Download User at a time.

Table 12 - Roles and Required Identification and Authentication

Role	Authentication type	Authentication data
Cryptographic Officer (CO)	Role-Based	Cloud TLS Public Key (RSA 4096 or ECDSA P-384)
User	Role-Based	WPA2 Pre-Shared Key (256-bits) or WPA2 Master Session Key (MSK) (256-bits)
FW Download User	Role-Based	Mist Firmware Upgrade Public Key (ECDSA P-384)

Table 13 - Strengths of Authentication Mechanisms

Authentication mechanism	Strength of mechanism
Cloud TLS Public Key signature verification (RSA 4096 or ECDSA P-384)	When the CO authenticates to the module, the Cloud TLS Public Key will enter the boundary in plaintext during the TLS V1.2 handshake. The module performs validations on the incoming public key to ensure it is either an RSA 4096-bit or an ECDSA P-384 public key. RSA 4096 has an equivalent computational resistance to attack of 2^{128}, while ECDSA P-384 has an equivalent computational resistance to attack of 2^{192}. As such, taking a pessimistic approach we will use RSA 4096 for the following calculations. **The probability of a successful random attempt is 1/(2^{128}). This probability is less than the 1/1,000,000 required by FIPS 140-2.** The module supports an exponential back off, starting with a 1 second delay where 33% delay is incrementally added after each unsuccessful authentication attempt (e.g. module will impose a 1 second delay for the first attempt, a 1.33 second delay on second attempt, a 1.7689 on third attempt, etc.) Taking a pessimistic approach, within a one-minute period the module can process 10 authentication attempts. **The probability of a successful random attempt in a minute period is 10/2^{128}. This probability is less than the 1/100,000 required by FIPS 140-2.**

Authentication mechanism	Strength of mechanism
WPA2 Pre-Shared Key (256-bits)	The user can authenticate to the module using 802.11i WPA2 Pre-Shared Key (256-bits). **The probability of a successful random attempt is 1/(2^{256}). This probability is less than the 1/1,000,000 required by FIPS 140-2.** The module can process WPA2 authentication attempts in less than 1.6ms, being pessimistic and reducing the authentication duration by 50% to 0.8ms, the module could process 75,000 attempts in a minute period (75,000 = 60,000ms/0.8ms). **The probability of a successful random attempt in a minute period is 75,000/(2^{256}). This probability is less than the 1/100,000 required by FIPS 140-2.**
WPA2 Master Session Key (MSK) (256-bits)	The user can also authenticate to the module via RADIUS using 802.1x WPA2 Master Session Key (MSK) (256-bits). **The probability of a successful random attempt is 1/(2^{256}). This probability is less than the 1/1,000,000 required by FIPS 140-2.** The module imposes a 6 second delay interval for each RADIUS authentication attempt. In a one minute period, there can be a maximum of 10 authentication attempts. **The probability of a successful random attempt is 10/(2^{256}). This probability is less than the 1/100,000 required by FIPS 140-2.**

Authentication mechanism	Strength of mechanism
Mist Firmware Upgrade Public Key (ECDSA P-384)	The module enforces ECDSA P-384 keys for FW Download, which have a minimum equivalent computational resistance to attack of 2^{192}. **Thus the probability of a successful random attempt is $1/(2^{192})$. This probability is less than the 1/1,000,000 required by FIPS 140-2.** If the verification fails, the module enforces a reboot to abort the operation and forces the module to run the power-up self-tests before allowing the "Upgrade" service again. Each power-up event takes approximately 37 seconds, therefore being pessimistic the number of attempts possible in a one minute period is limited to 2. **The probability of a successful random attempt in a minute period is $2/2^{192}$. This probability is less than the 1/100,000 required by FIPS 140-2.**

8. ACCESS CONTROL POLICY

This section describes the access per service of the module to Keys and CSPs. The types of access can be any of the following: Read (R), Write(R), Execute(E), and Zeroize (Z),

Table 14 - Access Control Policy

Service	Role	CSPs and public keys	Type of Access
Power-up self-tests	None	N/A	N/A
Show status	None	N/A	N/A
Extended status report	None	N/A	N/A
Upgrade	FW Download User	Mist Firmware Upgrade Public Key	R, E
Reset Push button	None	N/A	N/A
Reboot	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Disconnect clients	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E

Service	Role	CSPs and public keys	Type of Access
Bounce Ethernet Ports	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Radio Reinit	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Network Status Test	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Configure IoT Block	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Zeroize	CO	All CSPs	Z
AP Configuration	CO	This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E

Service	Role	CSPs and public keys	Type of Access
TLSV1.2 EP Terminator	CO	Openssl SP800-90A DRBG Internal DRBG state {V, Key}	R, W, E
		Openssl SP800-90A DRBG DRBG Entropy input	R, W, E
		Openssl SP800-90A DRBG DRBG Seed	R, W, E
		Module TLS ECCCDH Private Key	R, W, E, Z
		TLS Pre-Master Secret	R, W, E, Z
		TLS Master Secret	R, W, E, Z
		TLS Session Encryption and Integrity Key	R, W, E
		TLS KDF Internal State	R, W, E
		Mist CA certificate	R, E
		Cloud TLS Public Key	R, W, E
		Module TLS ECCCDH Public Key	R, W, E
		Cloud (Extern) TLS ECCCDH Public Key	R, W, E
RADIUS	User	Radius secret	R, E
		Radius AES KW KEK	R, E
		Radius MACK	R, E

Service	Role	CSPs and public keys	Type of Access
802.1X WPA2	User	WPA2 Master Session Key (MSK) This service utilizes the same CSPs as the "WPA2" service with exception of the WPA2 Pre-Shared Key. Please see WPA2".	R, W, E E
WPA2	User	WPA2 Pre-shared key 802.11i PTK 802.11i MIC keys (KCK) 802.11i Key Encryption Key (KEK) 802.11i Temporal keys (AES-CCM 128-bits) 802.11i Group Master Key (GMK) 802.11i Gnonce Group Temporal Key (GTK) 802.11i KDF internal state	R, E R, W, E R, W, E R, W, E R, W, E R, W, E R, W, E R, W, E R, W, E
Bonjour	CO	This service is configured over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
L2TP	CO	This service is configured over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
BLE	CO	This service is configured over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
MESH	CO	This service is configured over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E

Service	Role	CSPs and public keys	Type of Access
ALS	CO	This service is configured over TLS V1.2. Please see "TLS V1.2 EP Terminator".	E
Network configure	CO	Radius secret Radius AES KW KEK Radius MACK WPA2 Pre-shared key This service is issued over TLS V1.2. Please see "TLS V1.2 EP Terminator".	R, W R, W R, W R, W E

9. SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

1. The module is considered to be operating in the FIPS Approved Mode of Operation when abiding by the security rules and requirements in the Security Policy. The module is shipped to the end customer in the FIPS Approved Mode of Operation. Any violation of the Security Policy will immediately place the module in a non-FIPS Approved Mode of Operation, and the module is not considered fit to protect sensitive but unclassified information.
2. By procedural guidance, to zeroize the entire module the operator is required to issue the "Zeroize" service and power cycle the module.
3. The module inhibits data output when performing power-up self-tests; interfaces are not enabled until such a time that all power-up self-test pass.
4. The module logically inhibits data output from processes performing key generation and zeroization.
5. The module supports a FIPS Error State. Any failure of power-up self-tests, or conditional self-tests, will transition the module to this state.
6. The module inhibits data output when in the FIPS Error State.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The module does not support concurrent operators.
9. The module will clear results of previous authentications when it is power-cycled; operator shall be required to re-authenticate into the module before executing any authenticated services.
10. The module does not support feedback (e.g. echo) of authentication data during the authentication procedure.
11. The module supports a limited operational environment; it only loads and executes trusted code; signed by Mist using ECDSA P-384 SHA-384. In such case all of the FIPS 140-2 Area 6 requirements are not applicable.
12. The IoT interface does not support data input (latent-functionality); only data output is supported by the module. To enable the pins and data output capability, use the "Configure IoT Block" service to modify the "iot_config" and specify the following for each of the 8-pins:

    "enabled": true
    "output": true

13. The module complies with FIPS 140-2 IG A.5 Technique #1: TLS 1.2 protocol IV generation
    -Module is a TLS client and performs all necessary operations entirely within the cryptographic boundary.
    -The keys for the client and server negotiated in the handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical.
    -The IV is 96 bits in length. The counter portion of the IV (64-bits) is set by the module within its cryptographic boundary; when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key the module will trigger a handshake to establish a new encryption key.
    -In case the module's power is lost and then restored, a new key for use with the AES GCM will be established.

10. CRITICAL SECURITY PARAMETERS and PUBLIC KEYS

The module supports the following CSPs and public keys. By procedural guidance, to zeroize the entire module the operator is required to issue the "Zeroize" service and power cycle the module.

Table 15 – Secret Keys and CSPs

Name	Type	Generation	Input/output	Storage	Zeroization
Openssl SP800-90A DRBG Internal DRBG state {V, Key}	AES-256-CTR DRBG with DF	SP800-90A DRBG	Input: N/A Output: N/A	Plaintext in RAM	Power cycle
Openssl SP800-90A DRBG DRBG Entropy input	384 bits from ENT (P)	SP800-90B ENT (P)	Input: N/A Output: N/A	Plaintext in RAM	Function completion or Power cycle
Openssl SP800-90A DRBG DRBG Seed	384 bit seed	SP800-90A DRBG	Input: N/A Output: N/A	Plaintext in RAM	Power cycle
Module TLS ECCCDH Private Key	SP800-56Ar3 ECCCDH (P-256)	SP800-90A DRBG	Input: N/A Output: N/A	Plaintext in RAM	Actively overwritten after Pre-Master Secret calculation or Power cycle
TLS Pre-Master Secret	256-bits	N/A – established by KAS-SSC.	Input: N/A Output: N/A	Plaintext in RAM	Actively overwritten after Master Secret calculation or Power cycle
TLS Master Secret	384-bits	N/A – established by TLS V1.2 KDF.	Input: N/A Output: N/A	Plaintext in RAM	Actively overwritten after Session Key calculation or Power cycle
TLS Session Encryption and Integrity Key	AES-GCM (128 and 256 bits)	N/A – established by TLS V1.2 KDF.	Input: N/A Output: N/A	Plaintext in RAM	Zeroize service or Power cycle

Name	Type	Generation	Input/output	Storage	Zeroization
TLS KDF Internal State	SP800-135 KDF with SHA-256 or SHA-384	SP800-135 TLS V1.2 KDF	Input: N/A Output: N/A	Plaintext in RAM	Power cycle
Radius secret	Fixed config string as per RFC-2865 (8-64 characters)	N/A	Input: Encrypted using TLS V1.2 Output: N/A	Plaintext in NAND and RAM	Zeroize service and Power cycle
Radius AES KW KEK	SP800-38F AES KW (128-bits)	N/A	Input: Encrypted using TLS V1.2 Output: N/A	Plaintext in NAND and RAM	Zeroize service and Power cycle
Radius MACK	HMAC-SHA-1 (128-bits)	N/A	Input: Encrypted using TLS V1.2 Output: N/A	Plaintext in NAND and RAM	Zeroize service and Power cycle
WPA2 Pre-shared key	256-bits	N/A	Input: Encrypted using TLS V1.2 Output: N/A	Plaintext in NAND and RAM	Zeroize service and Power cycle
WPA2 Master Session Key (MSK)	256-bits	N/A	Input: Encrypted using "Radius AES KW KEK" Output: N/A	Plaintext in RAM	Power cycle
802.11i PTK	512-bits	N/A – established by SP800-108 KDF (SHA-256) with either the WPA2 Pre-	Input: N/A Output: N/A	Plaintext in RAM	Power cycle

Name	Type	Generation	Input/output	Storage	Zeroization
		shared key or the WPA2 Master Session Key (MSK) as the Key Input (KI) depending on the Authentication Mechanism chosen.			
802.11i MIC keys (KCK)	HMAC-SHA-1 (128-bits)	N/A – portion of PTK established by SP800-108 KDF (SHA-256). See "802.11i PTK" row above for the Key Input (KI).	Input: N/A Output: N/A	Plaintext in RAM	Power cycle
802.11i Key Encryption Key (KEK)	SP800-38F AES KW (128-bits)	N/A – portion of PTK established by SP800-108 KDF (SHA-256). See "802.11i PTK" row above for the Key Input (KI).	Input: N/A Output: N/A	Plaintext in RAM	Power cycle
802.11i Temporal keys (AES-CCM 128-bits)	AES-CCM (128-bits)	N/A – portion of PTK established by SP800-108 KDF (SHA-256). See "802.11i PTK" row above for the Key Input (KI).	Input: N/A Output: N/A	Plaintext in RAM and BCM43694 register table	Zeroize service and Power cycle
802.11i Group Master Key (GMK)	256-bits	SP800-90A DRBG	Input: N/A Output: N/A	Plaintext in RAM	Actively overwritten after GTK calculation or Power cycle
802.11i Gnonce	256-bits	N/A – established by SP800-108 KDF (SHA-256) with the 802.11i Group Master	Input: N/A Output: N/A	Plaintext in RAM	Actively overwritten after GTK calculation or Power cycle

Name	Type	Generation	Input/output	Storage	Zeroization
		Key (GMK) as the Key Input (KI).			
Group Temporal Key (GTK)	AES-CCM (128-bits)	N/A – established by SP800-108 KDF (SHA-256) with the 802.11i Group Master Key (GMK) as the Key Input (KI).	Input: N/A Output: Encrypted using "802.11i Key Encryption Key (KEK)"	Plaintext in RAM and BCM43694 HW key table	Zeroize service and Power cycle
802.11i KDF internal state	SP800-108 KDF (SHA-256)	SP800-108 KDF	Input: N/A Output: N/A	Plaintext in RAM	Power cycle

Table 16 – Public Keys

Name	Type	Generation	Input/output	Storage
Mist Firmware Upgrade Public Key	ECDSA P-384 SHA-384	N/A – Generated outside of the module during manufacturing.	Input: N/A Output: N/A	Plaintext in NAND and RAM
Mist CA certificate	RSA PSS 4096 with SHA-256 or ECDSA P-384 SHA-384	N/A - Generated outside of the module during manufacturing.	Input: N/A Output: N/A	Plaintext in NAND and RAM
Cloud TLS Public Key	RSA PSS 4096 with SHA-256 or ECDSA P-384 SHA-384	N/A	Input: Plaintext over TLS V1.2 handshake Output: N/A	Plaintext in RAM
Module TLS ECCCDH Public Key	SP800-56Ar3 ECCCDH (P-256)	SP800-56ARev3 (Derived from private key)	Input: N/A Output: Plaintext over TLS V1.2 handshake	Plaintext in RAM
Cloud (Extern) TLS ECCCDH Public Key	SP800-56Ar3 ECCCDH (P-256)	N/A	Input: Plaintext over TLS V1.2 handshake Output: N/A	Plaintext in RAM

11. PHYSICAL SECURITY POLICY

The module is a Level 2 module with production grade materials, an opaque enclosure, and tamper evident materials. The module is shipped from manufacturing with Tamper Evident Labels (TELs) applied. A total of QTY.5 Labels will be present as per Figure 14. The TELs are not re-orderable parts. If during the inspection there is suspected compromise, this product is no longer considered fit to protect sensitive but unclassified information and must be returned to Manufacturer.

Figure 14 - QTY.5 TEL Placement

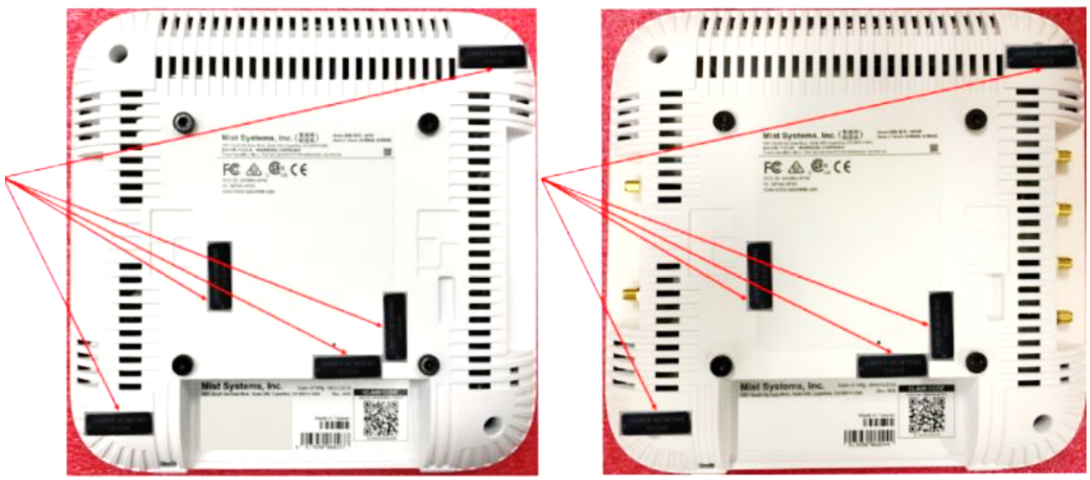


Table 17 - Inspection of Physical Security Mechanisms

Physical security mechanisms	Recommended frequency of inspection	Inspection guidance details
TELs	Once per year	Check for label damage or evidence of adhesive showing

12. MITIGATION OF OTHER ATTACKS POLICY

The module does not mitigate against other attacks outside the scope of FIPS 140-2.

Table 18 - Mitigation of Other Attacks

Other attacks	Mitigation mechanism	Specific limitations
N/A	N/A	N/A

13. ACRONYMS

Acronyms related to the cryptographic module that will be referenced in this document are found below.

Table 19 - Specification of Acronyms and their Descriptions

Term	Description
AP	Access Point
APT	Adaptive Proportion Test
CO	Cryptographic Officer
DRBG	Deterministic Random Bit Generator
ECCCDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ENT (P)	Physical Entropy Source
FIPS	Federal Information Processing Standards
KAS	Key Agreement Scheme
KAT	Known Answer Test
KTS	Key Transport Scheme
RCT	Repetition Count Test
RSA	Rivest Shamir Adleman
SHS	Secure Hashing Standard
SSC	Shared Secret Calculation
TEL	Tamper Evident Label