Mist Systems

FIPS AP43

FIPS 140-2 Non-Proprietary Security Policy

Document Revision: V1.0

F.W. Version: fips_apfw-0.8.20681-master-5ce6

H.W. Version: AP43-FIPS-US [REV. AA] and AP43E-FIPS-US [REV. AA]

Table of Contents

REVISION HISTORY

Author(s)	Version	Date	Description
Gurpreet Singh	1.0	February 10, 2021	Initial Release

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 feature.

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]	fips_apfw-0.8.20681-master-5ce6
	AP43E-FIPS-US [REV. AA]	

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

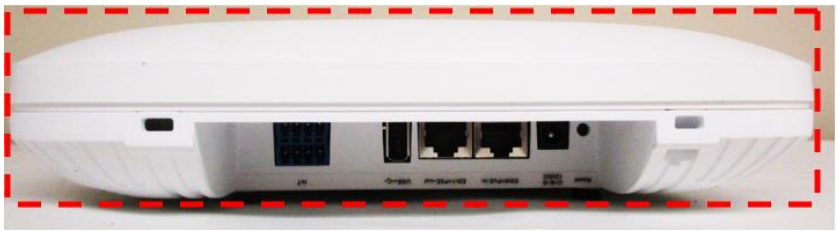


Figure 2 - AP43 Back Side

Figure 3 - AP43 Top Side

Figure 4 - AP43 Bottom Side

Figure 5 - AP43 Left Side

Figure 6 - AP43 Right Side

Figure 7- AP43E Front Side

Figure 8 - AP43E Back Side

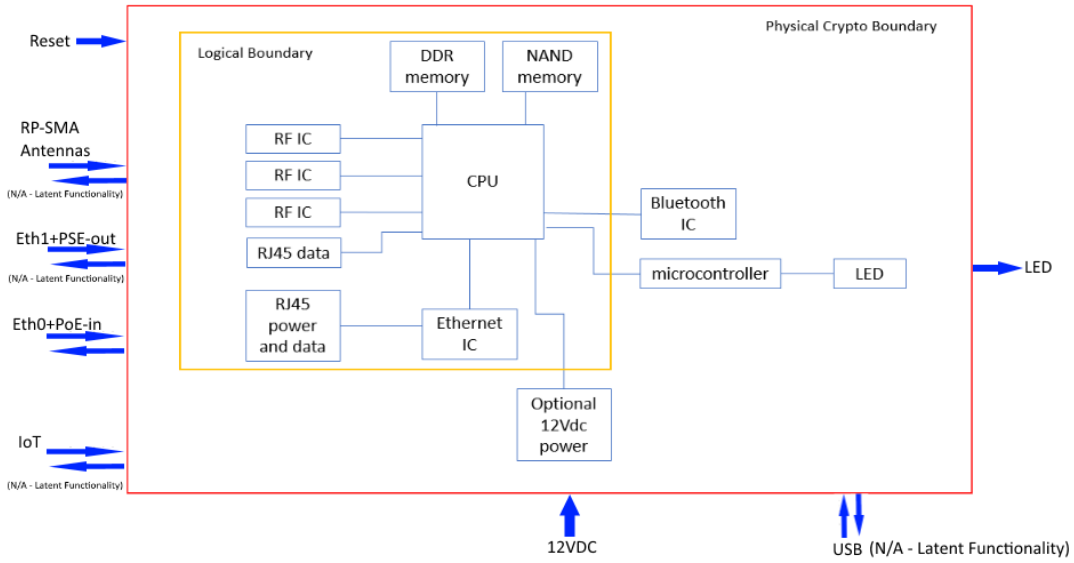
Figure 9 - AP43E Top Side

Figure 10 - AP43E Bottom Side

Figure 11 - AP43E Left Side

Figure 12 - AP43E Right Side

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
- TPM (Latent functionality; not used)

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	N/A - Latent Functionality; reserved for future use. **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	N/A - Latent Functionality; reserved for future use. 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 Input and Data output	N/A - Latent Functionality; reserved for future use. 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.

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 PHYSICAL SECURITY POLICY. *(Note: The module is shipped with tamper evident labels applied.)*
3. Connect to the module via the Eth0+PoE-in interface, this interface will provide power to the module as described in Table 3.
4. 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.
5. Invoke the Extended Status Report service and confirm the Firmware version of the module is as per Table 1 above.
6. **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: RSA 4096 SHA-512 Digital Signature Verification[1]
5. SHA-512 KAT

Conditional self-tests:

1. Firmware Download Test: RSA 4096 SHA-512 Digital Signature Verification

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[2]	Automatically invoked by the module at boot.
Show status	None	Status of the module provided by LED.
Extended status report	None	Status report.
Upgrade	CO, 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	None	Control command to power-cycle the module.
Network Status Test	None	Control command to perform network statistic tests including ping, pcap, traceroute, and arp.
AP Configuration	None	Modify the device configuration of the AP such as LED brightness.

[1] As per FIPS 140-2 IG 9.3, this approved integrity technique is considered a KAT since the cryptographic module uses itself as an input to the algorithm and a known answer as the expected output.
[2] Unauthenticated services will be assigned “None” as the role. By virtue of being unauthenticated, a CO or User can also execute the service.

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
Disconnect Clients	None[3]	Service issued over non-compliant TLSV1.2, to disconnect, deauthorize, and terminate APs in the network.
Bounce Ethernet Ports	None	Control command to toggle the power of Ethernet ports.
Configure IoT Block	None	Configure (set and get) for IoT pins.
SSHv2 IP Tunnel	None	Non-compliant SSHv2 communication from Cloud to AP.
TLSV1.2 EP Terminator	None	Non-compliant TLSV1.2 communication from Cloud to AP.
Update NVRAM Parameters	None	Non-compliant service unavailable for testing (reserved for future use).
Network configure	None	Non-compliant service unavailable for testing (reserved for future use).
Record Wifi Status	None	Non-compliant service unavailable for testing (reserved for future use).
DNS configure	None	Non-compliant service unavailable for testing (reserved for future use).
USB configure	None	Non-compliant service unavailable for testing (reserved for future use).
AP cache configure	None	Non-compliant service unavailable for testing (reserved for future use).

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

6. ALGORITHMS

The module supports the following approved algorithms in the FIPS Approved Mode of Operation.

Table 7 - Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode	Key Length	Use
C1751	RSA	FIPS 186-2	SigVer	4096	Digital Signature Verification
C1751	SHS	FIPS 180-4	SHA-512	N/A	Message Digest

Table 8 - Allowed Algorithms

Algorithm	Caveat	Use
N/A	N/A	N/A

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

Table 9 - Non-Approved Algorithms

Algorithm(s)	Non-compliant Service Mapping
AES-128-GCM (non-compliant), AES-256-GCM (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), RSA 2048 (non-compliant), TLSV1.2 KDF (non-compliant), TRNG	Disconnect Clients; Bounce Ethernet Ports Configure IoT Block; TLSV1.2 EP Terminator Update NVRAM Parameters; Network configure Record Wifi Status; DNS configure; USB configure AP cache configure
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), TRNG	SSHv2 IP Tunnel

7. IDENTIFICATION AND AUTHENTICATION POLICY

The module supports a Cryptographic Officer (CO) and a User; the module does not support concurrent operators. The CO is responsible for installation and initialization of the module as per Section 5.1 of the Security Policy. The User operates the module in the field.

The module supports role-based authentication. The authentication mechanism relies on RSA 4096 SHA-512 signature verification needed to execute the "Upgrade" service.

Table 10 - Roles and Required Identification and Authentication

Role	Authentication type	Authentication data
Cryptographic Officer (CO)	Role-Based	Mist Firmware Upgrade Public Key (RSA 4096)
User	Role-Based	Mist Firmware Upgrade Public Key (RSA 4096)

Table 11 - Strengths of Authentication Mechanisms

Authentication mechanism	Strength of mechanism
RSA 4096 SHA-512 signature verification	The module enforces RSA 4096-bit keys, which have a minimum equivalent computational resistance to attack of 2^{128}. Thus 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. 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 $2/2^{128}$. 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[4]. The types of access can be any of the following: Read (R), Write(R), Execute(E), and Zeroize (Z)[5],

Table 12 - Access Control Policy

Service	Role	Keys and CSPs	Type of Access
Power-up self-tests	None[6]	N/A	N/A
Show status	None	N/A	N/A
Extended status report	None	N/A	N/A
Upgrade	CO, User	Mist Firmware Upgrade Public Key	R, E
		Mist Firmware Upgrade Tool Public Key	R, E
Reset Push button	None	N/A	N/A
Reboot	None	N/A	N/A
Network Status Test	None	N/A	N/A
AP Configuration	None	N/A	N/A

[4] The module does not support CSPs, only Public Keys are supported in the FIPS Approved Mode.
[5] The module does not support zeroization as no CSPs are supported in the FIPS Approved Mode.
[6] Unauthenticated services will be assigned “None” as the role. By virtue of being unauthenticated, a CO or User can also execute the service.

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. 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.
3. 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.
4. The module inhibits data output when in the FIPS Error State.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module does not support concurrent operators.
7. The module does not support private keys, CSPs, key generation nor zeroization in the FIPS Approved Mode.
8. 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.
9. The module does not support feedback (e.g. echo) of authentication data during the authentication procedure. A successful authentication will result in a successful firmware upgrade. Failing to authenticate to the module, meaning the RSA 4096 SHA-512 Signature Verification fails, will result in the FIPS ERROR STATE.
10. The module supports a limited operational environment; it only loads and executes trusted code; signed by Mist using RSA 4096 SHA-512. In such case all of the FIPS 140-2 Area 6 requirements are not applicable.

10. CRITICAL SECURITY PARAMETERS and PUBLIC KEYS

The module does not support CSPs. The following Public Keys are supported by the module:

Table 13 - Public Keys

Name	Type	Generation	Storage	Zeroization
Mist Firmware Upgrade Public Key	RSA 4096 with SHA-512	N/A – Generated outside of the module during manufacturing,	Plaintext in NAND and RAM	N/A
Mist Firmware Upgrade Tool Public Key	RSA 4096 with SHA-512	N/A – Generated outside of the module during manufacturing,	Plaintext in NAND and RAM	N/A

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

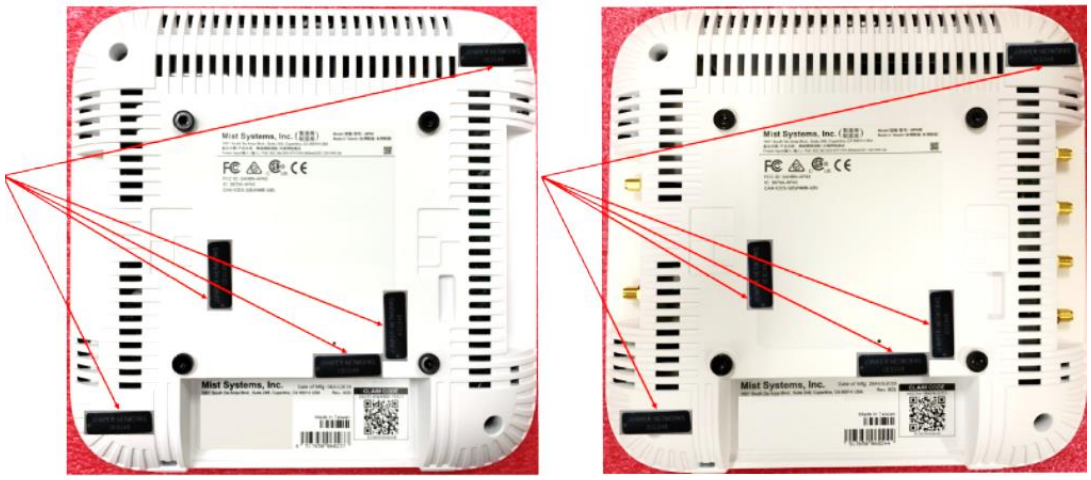


Table 14 - Inspection of Physical Security Mechanisms

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 15 - 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 16 - Specification of Acronyms and their Descriptions

Term	Description
AP	Access Point
CO	Cryptographic Officer
FIPS	Federal Information Processing Standards
RSA	Rivest Shamir Adleman
SHS	Secure Hashing Standard
TEL	Tamper Evident Label