

**FIPS 140-2 Non-Proprietary Security Policy
for Aruba AP-224 and AP-225
Wireless Access Points**


Version 4.1
September 2017



a Hewlett Packard
Enterprise company

Copyright

© 2017 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks

include  , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotectprotect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Hewlett Packard Enterprise Company products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Copyright

© 2017 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks include, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®.



www.arubanetworks.com

3333 Scott Blvd
Santa Clara, CA 95054
Phone: 408.227.4500
Fax 408.227.4550

1	INTRODUCTION	5
1.1	ACRONYMS AND ABBREVIATIONS.....	5
2	PRODUCT OVERVIEW	6
2.1	AP-224.....	6
2.1.1	<i>Physical Description</i>	6
2.1.1.1	Dimensions/Weight	6
2.1.1.2	Interfaces	6
2.1.1.3	Indicator LEDs	7
2.2	AP-225.....	7
2.2.1	<i>Physical Description</i>	8
2.2.1.1	Dimensions/Weight	8
2.2.1.2	Interfaces	8
2.2.1.3	Indicator LEDs	8
3	MODULE OBJECTIVES	10
3.1	SECURITY LEVELS	10
3.2	PHYSICAL SECURITY	10
3.2.1	<i>Applying TELs</i>	10
3.2.2	<i>AP-224/225 TEL Placement</i>	11
3.2.2.1	To detect opening of the chassis cover:	11
3.2.2.2	To detect access to restricted ports	11
3.2.3	<i>Inspection/Testing of Physical Security Mechanisms</i>	12
3.3	OPERATIONAL ENVIRONMENT.....	13
3.4	LOGICAL INTERFACES	13
4	ROLES, AUTHENTICATION AND SERVICES	15
4.1	ROLES	15
4.1.1	<i>Crypto Officer Authentication</i>	16
4.1.2	<i>User Authentication</i>	16
4.1.3	<i>Wireless Client Authentication</i>	16
4.1.4	<i>Strength of Authentication Mechanisms</i>	16
4.2	SERVICES	18
4.2.1	<i>Crypto Officer Services</i>	18
4.2.2	<i>User Services</i>	19
4.2.3	<i>Wireless Client Services</i>	19
4.2.4	<i>Unauthenticated Services</i>	20
4.2.5	<i>Service Available in Non-FIPS Mode</i>	20
5	CRYPTOGRAPHIC ALGORITHMS	21
6	CRITICAL SECURITY PARAMETERS	26

7	SELF TESTS.....	32
8	SECURE OPERATION	34

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba AP-224 and AP-225 Wireless Access Points with FIPS 140-2 Level 2 validation from Aruba Networks. This security policy describes how the AP meets the security requirements of FIPS 140-2 Level 2, and how to place and maintain the AP in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Web-site at:

<http://csrc.nist.gov/groups/STM/cmvp/index.html>

This document can be freely distributed.

In addition, in this document, the Aruba AP-224 and AP-225 Wireless Access Points are referred to as the Access Point, the AP, the module, the cryptographic module, Aruba Wireless AP, and AP-224/225.

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CLI	Command Line Interface
CO	Crypto Officer
CPSec	Control Plane Security protected
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
ECO	External Crypto Officer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FE	Fast Ethernet
GE	Gigabit Ethernet
GHz	Gigahertz
HMAC	Hashed Message Authentication Code
Hz	Hertz
IKE	Internet Key Exchange
IPsec	Internet Protocol security
KAT	Known Answer Test
KEK	Key Encryption Key
L2TP	Layer-2 Tunneling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPOE	Serial & Power Over Ethernet
TEL	Tamper-Evident Label
TFTP	Trivial File Transfer Protocol
WLAN	Wireless Local Area Network

2 Product Overview

This section introduces the various Aruba Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

- Firmware versions ArubaOS 6.5.1-FIPS

2.1 AP-224

This section introduces the Aruba AP-224 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba AP-224 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications

2.1.1 Physical Description

The Aruba AP-224 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports three external antennas through 3 X dual-band (RP-SMA) antenna interfaces for supporting external antennas.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- AP-224-F1 (HPE SKU JW173A)

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 20.3 cm (W) x 20.3 cm (D) x 5.4 cm (H).
- 750 g (27 oz)

2.1.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
 - 3x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x RJ-45 console interface (disabled in FIPS mode by TEL)
- 1 x USB 2.0

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.1.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 1- AP-224 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET0 ENET1	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbps Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.2 AP-225

This section introduces the Aruba AP-225 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba AP-225 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps via three internal antennas. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications

2.2.1 Physical Description

The Aruba AP-225 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports 3 integrated omni-directional multi-band dipole antenna elements (supporting up to 3x3 MIMO with spatial diversity).

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- AP-225-F1 (HPE SKU JW175A)
- FIPS Kit
 - 4011570-01 (Part number for Tamper Evident Labels)

2.2.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 20.3 cm (W) x 20.3 cm (D) x 5.4 cm (H).
- 750 g (27 oz)

2.2.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) ports
- 1 x RJ-45 console interface (Disabled in FIPS mode by TEL)
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.2.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2 - AP-225 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET0 ENET1	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard. .

3.1 Security Levels

Table 3 - Security Levels

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

3.2 Physical Security

The Aruba Wireless AP is a scalable, multi-processor standalone network device and is enclosed in a robust plastic housing. The AP enclosure is resistant to probing (please note that this feature has not been validated as part of the FIPS 140-2 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

3.2.1 Applying TELs

The Crypto Officer must apply Tamper-Evident Labels (TELs) to the AP to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). The TELs shall be installed for the module to operate in a FIPS Approved mode of operation. Vendor provides FIPS 140 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP). Aruba provides double the required amount of TELs with shipping and additional replacement TELs can be obtained by calling customer support and requesting part number 4011570-01 (HPE SKU JY894A).

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure the target surfaces are clean and dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.

- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.
- If evidence of tampering is found with the TELs, the module must immediately be powered down and the administrator must be made aware of a physical security breach
- To obtain additional or replacement TELS, please order Aruba Networks part number: 4011570—01 (HPE SKU JY894A).

Once applied, the TELs included with the AP cannot be surreptitiously broken, removed or reapplied without an obvious change in appearance:



Each TEL has a unique serial number to prevent replacement with similar label. To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:

3.2.2 AP-224/225 TEL Placement

This section displays all the TEL locations of the Aruba AP-224/225. The AP-224/225 requires a minimum of 4 TELs to be applied as follows:

3.2.2.1 To detect opening of the chassis cover:

- Spanning the bottom and top chassis covers and placed on the left, right, and bottom of the unit

3.2.2.2 To detect access to restricted ports

- Spanning the serial port

Following is the TEL placement for the AP-224/225:



Figure 1: AP-224/225 Front/Top view



Figure 2: AP-224/225 Back/Bottom View

3.2.3 Inspection/Testing of Physical Security Mechanisms

Table 4 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanism	Recommended Test Frequency	Guidance
Tamper-evident labels (TELs)	Once per month	Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELs. If there is any sign of removal, replacement, tearing, etc., of any

		TEL, then immediately stop using the module and notify the system administrator.
Opaque module enclosure	Once per month	Examine module enclosure for any evidence of new openings or other access to the module internals. If there is any sign of new openings or other access to the module internals, then immediately stop using the module and notify the system administrator.

3.3 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the module is designated as a non-modifiable operational environment. The module only allows the loading of trusted and verified firmware that is signed by Aruba.

3.4 Logical Interfaces

The physical interfaces are divided into logical interfaces defined by FIPS 140-2 as described in the following table.

Table 5 - Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	<ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 port
Data Output Interface	<ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • USB 2.0 port
Control Input Interface	<ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • Reset button
Status Output Interface	<ul style="list-style-type: none"> • 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • LEDs
Power Interface	<ul style="list-style-type: none"> • Power Supply • Power-over-Ethernet (POE)

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the networking functionality of the module.

- Control input consists of manual control inputs for power and reset through the power interfaces (DC power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
 - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- A power supply is used to connect the electric power cable. Operating power may also be provided via Power Over Ethernet (POE) device when connected. The power is provided through the connected Ethernet cable.
- Console port is disabled when operating in FIPS mode by TEL.

The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packet headers and contents.

4 Roles, Authentication and Services

4.1 Roles

The module supports the roles of Crypto Officer, User, and Wireless Client; no additional roles (e.g., Maintenance) are supported. Administrative operations carried out by the Aruba Mobility Controller map to the Crypto Officer role. The Crypto Officer has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.

Defining characteristics of the roles depend on whether the module is configured as in either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode or Mesh AP FIPS Mode. There are four FIPS approved modes of operations, which are Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode and the two Mesh Modes, Remote Mesh Portal FIPS Mode and Remote Mesh Point FIPS Mode. Please refer to section 8 in this documentation for more information.

- **Remote AP FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
 - Wireless Client role: in Remote AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i and access wireless network access/bridging services. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

- **CPSec Protected AP FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer
 - Wireless Client role: in CPSec Protected AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i Pre-shared secret and access wireless network access services.

- **Remote Mesh Portal FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: the adjacent Mesh Point APs in a given mesh cluster. Please notice that Remote Mesh Portal AP must be physically wired to Mobility Controller.
 - Wireless Client role: in Remote Mesh Portal FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

- **Remote Mesh Point FIPS mode:**
 - Crypto Officer role: the Crypto Officer role is the Aruba Mobility Controller that has the ability to configure, manage, and monitor the module, including the configuration,

loading, and zeroization of CSPs. The first mesh AP configured is the only AP with the direct wired connection.

- User role: the adjacent Mesh APs in a given mesh cluster. Please notice that User role can be a Mesh Point AP or a Mesh Portal AP in the given mesh network.
- Wireless Client role: in Mesh Remote Mesh Point FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

4.1.1 Crypto Officer Authentication

In each of FIPS approved modes, the Aruba Mobility Controller implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer's authentication is accomplished via either Pre-shared secret (IKEv1), RSA digital certificate (IKEv1/IKEv2) or ECDSA digital certificate (IKEv2).

4.1.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured in Remote Mesh Portal FIPS mode or Remote Mesh Point FIPS mode, the User role is authenticated via the WPA2 pre-shared key or EAP. When the module is configured as a Remote AP FIPS mode and CPSec protected AP FIPS mode, the User role is authenticated via the same IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer.

4.1.3 Wireless Client Authentication

The wireless client role defined in each of FIPS approved modes authenticates to the module via 802.11i. Please notice that WEP and TKIP configurations are not permitted in FIPS mode. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

4.1.4 Strength of Authentication Mechanisms

The following table describes the relative strength of each supported authentication mechanism.

Table 4.1 - Strength of Authentication Mechanisms

Authentication Mechanism	Mechanism Strength
IKEv1 Pre-shared secret based authentication (CO/User role)	Passwords are required to be a minimum of eight ASCII characters and a maximum of 64 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/3,608,347,333,959,680$, which is less than 1 in 100,000 required by FIPS 140-2.
802.11i Pre-shared secret based authentication (Wireless Client and Mesh AP user roles)	Passwords are required to be a minimum of eight ASCII characters and a maximum of 63 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/3,608,347,333,959,680$, which is less than 1 in 100,000 required by FIPS 140-2.
RSA Certificate based authentication (CO/User role)	The module supports 2048-bit RSA key authentication during IKEv1 and IKEv2. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112} , which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.
ECDSA Certificate based authentication (CO/User role)	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^{128} , which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{128}$, which is less than 1 in 100,000 required by FIPS 140-2.

4.2 Services

The module provides various services depending on role. These are described below.

4.2.1 Crypto Officer Services

The CO role in each of FIPS modes defined in section 4.1 has the same services.

Table 4.2 - Crypto Officer Services

Services	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO selects/de-selects FIPS mode as a configuration option.	None.
Key Management	The CO can configure/modify the IKEv1/IKEv2 shared secret (The RSA private key is protected by non-volatile memory and cannot be modified) and the 802.11i Pre-shared secret (used in advanced Remote AP configuration). Also, the CO/User implicitly uses the KEK to read/write configuration to non-volatile memory.	1 (read), 13 and 25 (write)
Remotely reboot module	The CO can remotely trigger a reboot	None
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization	None
Update module firmware	The CO can trigger a module firmware update	1,12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security	None.

Services	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Creation/use of secure management session between module and CO	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (read, write) 13 (read) 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 (read, write)
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.
Creation/use of secure mesh channel	The module requires secure connections between mesh points using 802.11i	1, 25 (read) 26, 27, 28, 29, 30 (read/write)
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared secret and 802.11i Pre-shared secret) stored in the flash can be zeroized by using command 'ap wipe out flash' or by overwriting with a new secret. The other keys/CSPs (KEK, RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command 'ap wipe out flash'.	All CSPs will be destroyed.

4.2.2 User Services

The User role for Remote AP FIPS mode and Control Plane Security (CPSec) Protected AP FIPS mode supports the same services listed in the Section 4.2.1 Crypto Officer Services.

The User role for Remote Mesh Portal FIPS mode and Remote Mesh Point FIPS mode supports the services listed in Section 4.2.3 Wireless Client Services.

4.2.3 Wireless Client Services

The following module services are provided for the Wireless Client role in Remote AP FIPS mode, CPSec protected AP FIPS mode, Remote Mesh Portal FIPS mode and Remote Mesh Point FIPS mode.

Table 4.3- Wireless Client Services

Service	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Generation and use of 802.11i	In all modes, the links between	1, 25 (read) 26,27,28,29,30

cryptographic keys	the module and wireless client are secured with 802.11i.	(read/write)
Use of 802.11i Pre-shared secret for establishment of IEEE 802.11i keys	When the module is in advanced Remote AP configuration, the links between the module and the wireless client are secured with 802.11i. This is authenticated with a shared secret only.	1, 25 (read)
Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None

4.2.4 Unauthenticated Services

The module provides the following unauthenticated services, which are available regardless of role.

- System status – module LEDs
- Reboot module by removing/replacing power
- Self-test and initialization at power-on.

4.2.5 Service Available in Non-FIPS Mode

All of the services that are available in FIPS mode are also available in non-FIPS mode.

- When operating in the non-FIPS mode, the TLS, SSH, and 802.11i services can utilize the non-Approved algorithms listed in the “Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode” section at the end of section 5.
- Upgrading the firmware via the console port.
- Debugging via the console port.

Please note that all CSPs will be zeroized automatically when switching from FIPS mode to non-FIPS mode, or from non-FIPS mode to FIPS mode.

5 Cryptographic Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode: NOTE: The modes listed for each algorithm are only those actually used by the module (additional modes may have been tested during CAVS testing and not currently used).

- ArubaOS OpenSSL Module algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS UBOOT Bootloader algorithm implementation
- Aruba AP Hardware algorithm implementation

Below are the detailed lists for the FIPS approved algorithms and the associated certificate implemented by each crypto library

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2680	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (ext only)	128, 192, 256	Data Encryption/Decryption
232	CVL RSASPI PKCS 1.5	FIPS 186-4		MOD 2048	RSA
433	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
469	ECDSA	186-2	PKG, SigGen, SigVer	P256, P384	Digital Signature Generation and Verification
469	ECDSA	186-4	PKG, SigGen, SigVer	P256, P384	Digital Key Generation, Signature Generation and Verification
1666	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
16	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384	Deriving Keys

1379	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
1379	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2249	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1607	Triple-DES	SP 800-67	TEBC, TCBC	192	Data Encryption/Decryption

Note:

- If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2²⁸ encryptions before the key is changed.
- RSA (Cert. #1379; non-compliant with the functions from the CAVP Historical RSA List)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1
- ECDSA (Cert. #469; non-compliant with the functions from the CAVP Historical ECDSA List)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2677	AES	FIPS 197, SP 800-38A	CBC, GCM	128, 192, 256	Data Encryption/Decryption
251	CVL RSASP1	186-4	2048 PKCS #1.5		Key Gen, SigVer, SigGen
150	CVL IKEv1 IKEv2	SP 800 - 135	IKEv1(DSA, PSK 2048, SHA-256, 384), IKEv2(2048 SHA-256,		Key Derivation

			384)		
466	ECDSA	186-2	PKG, SigGen, SigVer (P- 256, 384, SHA 1, 256, 384, 512	P256, P384	PKG,Digital Signature Generation and Verification
466	ECDSA	186-4	PKG, SigGen, SigVer (P- 256, 384, SHA 1, 256, 384, 512	P256, P384	PKG,Digital Signature Generation and Verification
1663	HMAC	FIPS 198-1	HMAC- SHA1, HMAC-SHA- 256, HMAC- SHA-384, HMAC-SHA- 512	112, 126, 160, 256	Message Authentication
1376	RSA	FIPS 186-2	SHA-1, SHA- 256, SHA- 384, SHA- 512 PKCS1 v1.5	2048, 1024 (legacy SigVer only)	Digital Signature Verification
1376	RSA	FIPS 186-4	SHA-1, SHA- 256, SHA- 384, SHA- 512 PKCS1 v1.5	2048, 1024 (legacy SigVer only)	Digital Key Generation, Signature Generation and Verification
2246	SHS	FIPS 180-4	SHA-1, SHA- 256, SHA- 384, SHA- 512 Byte Only		Message Digest
1605	Triple- DES	SP 800- 67	TCBC	192	Data Encryption/Decryption

Note:

- If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^{28} encryptions before the key is changed.
- RSA (Cert. #1376; non-compliant with the functions from the CAVP Historical RSA List)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1

- ECDSA (Cert. #466; non-compliant with the functions from the CAVP Historical ECDSA List)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2419	RSA	FIPS 186-4	SHA-1, SHA-256	2048	Digital Signature Verification
3657	SHS	FIPS 180-4	SHA-1, SHA-256, Byte Only		Message Digest

NOTE: Only Firmware signed with SHA-256 is permitted in the Approved mode. Digital signature verification with SHA-1, while available within the module, shall only be used while in the non-Approved mode.

Aruba AP Hardware (Freescale P1020)					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
1648	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB128, OFB, CTR (ext only) CCM, GCM(used for self-test only)	128, 192, 256	Data Encryption/Decryption
538	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
934	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest

758	Triple-DES	SP 800-67	TEBC, TCBC, TOFB	192	Data Encryption/Decryption
---------------------	------------	-----------	---------------------	-----	-------------------------------

Note: If Triple-DES is employed, the user is responsible for ensuring that the module limits the use of any single Triple-DES key to less than 2^{28} encryptions before the key is changed.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

- NDRNG (used solely to seed the Approved DRBG)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

NOTE: IKEv1 and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use, and are not used, in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits of encryption strength)

DES, MD5, HMAC-MD5 and RC4 are used for older versions of TLS, SSH and WEP non-approved mode.

6 Critical Security Parameters

The following Critical Security Parameters (CSPs) are used by the module:

Table 6.1 - Critical Security Parameters

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK)	Triple-DES (192 bits)	Hardcoded during manufacturing. Used only to protect keys stored in the flash, not for key transport. (3 Key, CBC)	Stored in Flash memory (plaintext)	Zeroized by using command 'ap wipe out flash'.
2	DRBG entropy input	SP 800-90A CTR_DRBG (512 bits)	Entropy inputs to DRBG function used to construct the DRBG seed. 64 bytes are gotten from the entropy source on each call by any service that requires a random number. Testing estimates 505.26 bits of entropy are returned in the 512 bit string.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	SP 800-90a CTR_DRBG (384-bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
4	DRBG Key	SP 800-90a CTR_DRBG (256 bits)	This is the DRBG key used for SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
5	DRBG V	SP 800-90a CTR_DRBG V (128 bits)	Internal V value used as part of SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

6	Diffie-Hellman private key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS approved DRBG (Cert. #433) to derive Diffie-Hellman shared secret used in both IKEv1 and IKEv2.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
7	Diffie-Hellman public key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (Cert #433) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
10	EC Diffie-Hellman public key	EC Diffie-Hellman (Curves: P-256 or P-384).	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
11	EC Diffie-Hellman shared secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in Flash encrypted with KEK	Zeroized by using command 'ap wipe out flash'

IPSec/IKE

13	IKEv1 Pre-shared secret	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret
14	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKEv1 protocol implementation.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.
15	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKEv1 session authentication key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
16	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
17	IKE session authentication key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKEv1/IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
18	IKE session encryption key	Triple-DES (192 bits, 3 Key CBC) /AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

			KDF (IKEv1/IKEv2). Used for IKE payload protection.		
19	IPSec session encryption keys	Triple-DES (192 bits, 3 KEY CBC) / AES (CBC) and AES-GCM (128/192/256 bits)	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
20	IPSec session authentication keys	HMAC-SHA-1 (160 bits)	The IPsec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
21	IKE RSA Private Key	RSA private key (2048 bits)	This is the RSA private key. This key is generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In both IKEv1 and IKEv2, DRBG (Cert. #433) is called for key generation. It is used for RSA signature signing in either IKEv1 or IKEv2.	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash'
22	IKE RSA public key	RSA public key (2048 bits)	This is the RSA public key. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. It is used for RSA signature verification in either IKEv1 or IKEv2. This key can also be entered by the CO on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash'

23	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Cert #433) is called for key generation. It is used for ECDSA signature signing in IKEv2.	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash'.
24	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO on the Mobility Controller via SSH (CLI) and/or TLS (for the GUI).	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash'
802.11i					
25	802.11i Pre-shared secret	Shared secret (8-63 ASCII characters, or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication.	Stored in Flash memory encrypted with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret.
26	802.11i Pair-Wise Master key (PMK)	Shared secret (256 bits)	The PMK is transported to the module, protected by IPSec secure tunnel. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	Stored in SDRAM (plaintext)	Zeroized by rebooting the module

27	802.11i Pairwise Transient Key (PTK)	384 bit HMAC	This key is used to derive 802.11i session key by using the KDF defined in SP800-108.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
28	802.11i session key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 then used as the session key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
29	802.11i Group Master Key (GMK)	Shared secret (256 bits)	Generated by calling DRBG (Cert. #433). Used to derive 802.11i Group Transient Key GTK.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
30	802.11i Group Transient Key (GTK)	AES-CCM (256 bits)	Derived from 802.11 GMK by using the KDF defined in SP800-108. The GTK is the 802.11i session key used for broadcast communications protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

Please note that:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 2. FIPS approved DRBG (Cert #433) is used for IV generation and 96 bits of IV is supported.
- CSPs labeled as “Entered by CO” (as well as the ECDSA/RSA public keys) are transferred into the module from the Mobility Controller via IPsec. From the perspective of the end user, these CSPs will be entered via an SSH or TLS connection to the Mobility Controller.
- For keys identified as being "Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.

7 Self Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode, Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode, Remote Mesh Portal FIPS mode or Remote Mesh Point FIPS mode). In addition, the module also performs Conditional tests after being configured into either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode, Remote Mesh Portal FIPS mode or Remote Mesh Point FIPS mode. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following power on self-tests:

ArubaOS OpenSSL Module:

- AES (encrypt/decrypt) KATs
- Triple-DES (encrypt/decrypt) KATs
- DRBG KAT
- RSA (sign/verify) KATs
- ECDSA (sign/verify) KATs
- SHS (SHA1, SHA256, SHA384 and SHA512) KATs
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

ArubaOS Crypto Module

- AES (encrypt/decrypt) KATs
- AES-GCM (encrypt/decrypt) KATs
- Triple-DES (encrypt/decrypt) KATs
- SHA (SHA1, SHA256, SHA384 and SHA512) KATs
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs
- RSA (sign/verify) KATs
- ECDSA (sign/verify) KATs

ArubaOS UBOOT Bootloader Module

- Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

ArubaOS AP Hardware (Freescale P1020) Known Answer Tests:

- AES (encrypt/decrypt) KATs
- AES-CCM (encrypt/decrypt) KAT
- AES-GCM (encrypt/decrypt) KAT
- Triple-DES (encrypt/decrypt) KATs
- SHA-1 KAT
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

The following Conditional Self-tests are performed in the AP

ArubaOS OpenSSL Module

- CRNG Test to Approved DRBG

- SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed).
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

ArubaOS Crypto Module

- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

ArubaOS UBOOT Bootloader Module

- Firmware Load Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

Conditional Tests on Hardware:

- CRNG Test to NDRNG

These self-tests are run for the hardware cryptographic implementation as well as for the Aruba OpenSSL and ArubaOS cryptographic module implementations.

Self-test results are written to the serial console.

In the event of a KATs failure, the AP logs different messages, depending on the error.

For an ArubaOS OpenSSL AP module and ArubaOS cryptographic module KAT failure:

```
AP rebooted [DATE][TIME] : Restarting System, SW FIPS KAT failed
```

For an AES Atheros hardware POST failure:

```
Starting HW SHA1 KAT ...Completed HW SHA1 AT
```

```
Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT
```

```
Starting HW AES KAT ...Restarting system.
```

8 Secure Operation

The module can be configured to be in the following FIPS approved modes of operations via corresponding Aruba Mobility Controllers that have been certified to FIPS level 2:

- Remote AP FIPS mode – When the module is configured as a Remote AP, it is intended to be deployed in a remote location (relative to the Mobility Controller). The module provides cryptographic processing in the form of IPsec for all traffic to and from the Mobility Controller.
- Control Plane Security (CPsec) Protected AP FIPS mode – When the module is configured as a Control Plane Security protected AP it is intended to be deployed in a local/private location (LAN, WAN, MPLS) relative to the Mobility Controller. The module provides cryptographic processing in the form of IPsec for all Control traffic to and from the Mobility Controller.
- Remote Mesh Portal FIPS mode – When the module is configured in Mesh Portal mode, it is intended to be connected over a physical wire to the mobility controller. These modules serve as the connection point between the Mesh Point and the Mobility Controller. Mesh Portals communicate with the Mobility Controller through IPsec and with Mesh Points via 802.11i session. The Crypto Officer role is the Mobility Controller that authenticates via IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i preshared key.
- Remote Mesh Point FIPS mode – an AP that establishes all wireless path to the Remote Mesh portal in FIPS mode over 802.11 and an IPsec tunnel via the Remote Mesh Portal to the controller.

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients. The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation.

Only firmware updates signed with SHA-256/RSA 2048 are permitted.

This section explains how to place the module in each FIPS mode and how to verify that it is in FIPS mode. An important point in the Aruba APs is that to change configurations from any one mode to any other mode requires the module to be re-provisioned and rebooted before any new configured mode can be enabled.

The access point is managed by an Aruba Mobility Controller in FIPS mode, and access to the Mobility Controller's administrative interface via a non-networked general purpose computer is required to assist in placing the module in FIPS mode. The controller used to provision the AP is referred to below as the "staging controller". The staging controller must be provisioned with the appropriate firmware image for the module, which has been validated to FIPS 140-2, prior to initiating AP provisioning. The Crypto Officer shall perform the following steps:

8.1.1 Configuring Remote AP FIPS Mode

1. Apply TELs according to the directions in section 3.2
2. Log into the administrative console of the staging controller
3. Deploying the AP in Remote FIPS mode configure the controller for supporting Remote APs, For detailed instructions and steps, see Section "Configuring the Secure Remote Access Point Service" in Chapter "Remote Access Points" of the Aruba OS User Manual.
4. Enable FIPS mode on the controller. This is accomplished by going to the **Configuration > Network > Controller > System Settings** page (this is the default page when you click the **Configuration** tab), and clicking the **FIPS Mode for Mobility Controller Enable** checkbox.
5. Enable FIPS mode on the AP. This accomplished by going to the **Configuration > Wireless > AP Configuration > AP Group** page. There, you click the **Edit** button for the appropriate AP group, and then select **AP > AP System Profile**. Then, check the "Fips Enable" box, check "Apply", and save the configuration.

6. If the staging controller does not provide PoE, either ensure the presence of a PoE injector for the LAN connection between the module and the controller, or ensure the presence of a DC power supply appropriate to the particular model of the module.
7. Connect the module via an Ethernet cable to the staging controller; note that this should be a direct connection, with no intervening network or devices; if PoE is being supplied by an injector, this represents the only exception. That is, nothing other than a PoE injector should be present between the module and the staging controller.
8. Once the module is connected to the controller by the Ethernet cable, navigate to the **Configuration > Wireless > AP Installation page**, where you should see an entry for the AP. Select that AP, click the “Provision” button, which will open the provisioning window. Now provision the AP as Remote AP by filling in the form appropriately. Detailed steps are listed in section entitled “Provisioning an Individual AP” in the ArubaOS User Guide. Click “Apply and Reboot” to complete the provisioning process.
 - a. During the provisioning process as Remote AP if Pre-shared secret is selected to be the Remote AP Authentication Method, the IKE Pre-shared secret (8 - 64 ASCII or 64 HEX characters) is input to the module during provisioning. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPsec session. If certificate based authentication is chosen, the AP’s RSA or ECDSA key pair is used to authenticate AP to controller during IPsec.
9. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration
10. Terminate the administrative session
11. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network.

8.1.2 Configuring Control Plane Security (CPsec) Protected AP FIPS mode

1. Apply TELs according to the directions in section 3.2
2. Log into the administrative console of the staging controller
3. Configure the staging controller with CPsec under **Configuration > Controller > Control Plane Security** tab. AP will authenticate to the controller using certificate based authentication (IKEv2) to establish IPsec. The AP is configured with an RSA key pair at manufacturing. The AP’s certificate is signed by Aruba Certification Authority (trusted by all Aruba controllers) and the AP’s RSA private key is stored in non-volatile memory. Refer to the “Configuring Control Plane Security” section in the ArubaOS User Manual for details on the steps.
4. Enable FIPS mode on the controller. This is accomplished by going to the **Configuration > Network > Controller > System Settings** page (this is the default page when you click the **Configuration** tab), and clicking the **FIPS Mode for Mobility Controller Enable** checkbox.
5. Enable FIPS mode on the AP. This accomplished by going to the **Configuration > Wireless > AP Configuration > AP Group** page. There, you click the **Edit** button for the appropriate AP group, and then select **AP > AP System Profile**. Then, check the “FIPS Enable” box, check “Apply”, and save the configuration.
6. If the staging controller does not provide PoE, either ensure the presence of a PoE injector for the LAN connection between the module and the controller, or ensure the presence of a DC power supply appropriate to the particular model of the module
7. Connect the module via an Ethernet cable to the staging controller; note that this should be a direct connection, with no intervening network or devices; if PoE is being supplied by an injector, this

represents the only exception. That is, nothing other than a PoE injector should be present between the module and the staging controller.

8. Once the module is connected to the controller by the Ethernet cable, navigate to the **Configuration > Wireless > AP Installation page**, where you should see an entry for the AP. Select that AP, click the “Provision” button, which will open the provisioning window. Now provision the CPsec Mode by filling in the form appropriately. Detailed steps are listed in Section “Provisioning an Individual AP” of Chapter “The Basic User-Centric Networks” of the Aruba OS User Guide. Click “Apply and Reboot” to complete the provisioning process.
 - a. For CPsec AP mode, the AP always uses certificate based authentication to establish IPSec connection with controller. AP uses the RSA key pair assigned to it at manufacturing to authenticate itself to controller during IPSec. Refer to “Configuring Control Plane Security” Section in Aruba OS User Manual for details on the steps to provision an AP with CPsec enabled on controller.
9. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration
10. Terminate the administrative session
11. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network.

8.1.3 Configuring Remote Mesh Portal FIPS Mode

1. Apply TELs according to the directions in section 3.2
2. Log into the administrative console of the staging controller
3. Deploying the AP in Remote Mesh Portal mode, create the corresponding Mesh Profiles on the controller as described in detail in Section “Mesh Profiles” of Chapter “Secure Enterprise Mesh” of the Aruba OS User Manual.
 - a. For mesh configurations, configure a WPA2 PSK which is 8-63 ASCII characters or 64 hexadecimal digits in length; generation of such keys is outside the scope of this policy.
4. Enable FIPS mode on the controller. This is accomplished by going to the **Configuration > Network > Controller > System Settings** page (this is the default page when you click the **Configuration** tab), and clicking the **FIPS Mode for Mobility Controller Enable** checkbox.
5. Enable FIPS mode on the AP. This accomplished by going to the **Configuration > Wireless > AP Configuration > AP Group** page. There, you click the **Edit** button for the appropriate AP group, and then select AP > **AP System Profile**. Then, check the “FIPS Enable” box, check “Apply”, and save the configuration.
6. If the staging controller does not provide PoE, either ensure the presence of a PoE injector for the LAN connection between the module and the controller, or ensure the presence of a DC power supply appropriate to the particular model of the module.
7. Connect the module via an Ethernet cable to the staging controller; note that this should be a direct connection, with no intervening network or devices; if PoE is being supplied by an injector, this represents the only exception. That is, nothing other than a PoE injector should be present between the module and the staging controller.
8. Once the module is connected to the controller by the Ethernet cable, navigate to the **Configuration > Wireless > AP Installation page**, where you should see an entry for the AP. Select that AP, click the “Provision” button, which will open the provisioning window. Now provision the AP as Remote Mesh Portal by filling in the form appropriately. Detailed steps are listed in Section “Provisioning an Individual AP” of Chapter “The Basic User-Centric Networks” of the Aruba OS User Guide. Click “Apply and Reboot” to complete the provisioning process.

- a. During the provisioning process as Remote Mesh Portal, if Pre-shared key is selected to be the Remote IP Authentication Method, the IKE pre-shared key (which is at least 8 characters in length) is input to the module during provisioning. Generation of this key is outside the scope of this policy. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPSec session. If certificate based authentication is chosen, AP's RSA key pair is used to authenticate AP to controller during IPSec. AP's RSA private key is contained in the AP's non volatile memory and is generated at manufacturing time in factory.
 - b. During the provisioning process as Remote Mesh Portal, the WPA2 PSK is input to the module via the corresponding Mesh cluster profile. This key is stored on flash encrypted.
9. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration
 10. Terminate the administrative session
 11. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network.

To verify that the module is in FIPS mode, do the following:

1. Log into the administrative console of the Aruba Mobility Controller
2. Verify that the module is connected to the Mobility Controller
3. Verify that the module has FIPS mode enabled by issuing command "show ap ap-name <ap-name> config"
4. Terminate the administrative session

8.1.4 Configuring Remote Mesh Point FIPS Mode

1. Apply TELs according to the directions in section 3.2
2. Log into the administrative console of the staging controller
3. Deploying the AP in Remote Mesh Point mode, create the corresponding Mesh Profiles on the controller as described in detail in Section "Mesh Points" of Chapter "Secure Enterprise Mesh" of the Aruba OS User Manual.
 - a. For mesh configurations, configure a WPA2 PSK which is 8-63 ASCII characters or 64 hexadecimal digits in length; generation of such keys is outside the scope of this policy.
4. Enable FIPS mode on the controller. This is accomplished by going to the **Configuration > Network > Controller > System Settings** page (this is the default page when you click the **Configuration** tab), and clicking the **FIPS Mode for Mobility Controller Enable** checkbox.
5. Enable FIPS mode on the AP. This accomplished by going to the **Configuration > Wireless > AP Configuration > AP Group** page. There, you click the **Edit** button for the appropriate AP group, and then select **AP > AP System Profile**. Then, check the "Fips Enable" box, check "Apply", and save the configuration.
6. If the staging controller does not provide PoE, either ensure the presence of a PoE injector for the LAN connection between the module and the controller, or ensure the presence of a DC power supply appropriate to the particular model of the module.
7. Connect the module via an Ethernet cable to the staging controller; note that this should be a direct connection, with no intervening network or devices; if PoE is being supplied by an injector, this represents the only exception. That is, nothing other than a PoE injector should be present between the module and the staging controller.
8. Once the module is connected to the controller by the Ethernet cable, navigate to the **Configuration > Wireless > AP Installation page**, where you should see an entry for the AP.

Select that AP, click the “Provision” button, which will open the provisioning window. Now provision the AP as Remote Mesh Portal by filling in the form appropriately. Detailed steps are listed in Section “Provisioning an Individual AP” of Chapter “The Basic User-Centric Networks” of the Aruba OS User Guide. Click “Apply and Reboot” to complete the provisioning process.

- a. During the provisioning process as Remote Mesh Point, if Pre-shared key is selected to be the Remote IP Authentication Method, the IKE pre-shared key (which is 8 – 64 ASCII characters or 64 HEX characters in length) is input to the module during provisioning. Generation of this key is outside the scope of this policy. In the initial provisioning of an AP, this key will be entered in plaintext; subsequently, during provisioning, it will be entered encrypted over the secure IPSec session. If certificate based authentication is chosen, AP’s RSA key pair is used to authenticate AP to controller during IPSec. AP’s RSA private key is contained in the AP’s nonvolatile memory and is generated at manufacturing time in factory.
 - b. During the provisioning process as Mesh Point, the WPA2 PSK is input to the module via the corresponding Mesh cluster profile. This key is stored on flash encrypted.
9. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration
 10. Terminate the administrative session
 11. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network.

8.1.5 Verifying the FIPS mode

For all the approved modes of operations , follow the steps below to verify the FIPS mode:

1. Log into the administrative console of the Aruba Mobility Controller.
2. Verify that the module is connected to the Mobility Controller
3. Verify that the module has FIPS mode enabled by issuing command “show ap ap-name <ap-name> config”
4. Terminate the administrative session

8.1.6 Full Documentation

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=23054>