FIPS 140-2 Non-Proprietary Security Policy
for Aruba AP-120 Series Wireless Access Points

Version 1.5
Jan. 2013

Aruba Networks™
1322 Crossman Ave.
Sunnyvale, CA 94089-1113
Copyright
© 2013 Aruba Networks, Inc. Aruba Networks 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®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Aruba 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 Networks, Inc. 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 Networks, Inc. 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.
1 INTRODUCTION ......................................................................................................................................... 4
1.1 ACRONYMS AND ABBREVIATIONS ........................................................................................................ 4
2 PRODUCT OVERVIEW ............................................................................................................................ 5
  2.1 ARUBA AP-120 SERIES .......................................................................................................................... 5
    2.1.1 Physical Description ..................................................................................................................... 5
      2.1.1.1 Dimensions/Weight ............................................................................................................... 5
      2.1.1.2 Interfaces .............................................................................................................................. 6
      2.1.1.3 Indicator LEDs ................................................................................................................... 6
3 MODULE OBJECTIVES ............................................................................................................................... 8
  3.1 SECURITY LEVELS ................................................................................................................................ 8
  3.2 PHYSICAL SECURITY ............................................................................................................................ 8
    3.2.1 Aruba AP-124 TEL Placement ..................................................................................................... 9
    3.2.2 Aruba AP-125 TEL Placement ..................................................................................................... 10
    3.2.3 Inspection/Testing of Physical Security Mechanisms ................................................................... 10
  3.3 MODES OF OPERATION ..................................................................................................................... 11
  3.4 OPERATIONAL ENVIRONMENT ......................................................................................................... 12
  3.5 LOGICAL INTERFACES ...................................................................................................................... 13
4 ROLES, AUTHENTICATION, AND SERVICES.......................................................................................... 14
  4.1 ROLES .................................................................................................................................................. 14
    4.1.1 Crypto Officer Authentication ...................................................................................................... 14
    4.1.2 User Authentication ..................................................................................................................... 15
    4.1.3 Wireless Client Authentication ................................................................................................... 15
    4.1.4 Strength of Authentication Mechanisms ..................................................................................... 15
  4.2 SERVICES ......................................................................................................................................... 17
    4.2.1 Crypto Officer Services .............................................................................................................. 17
    4.2.2 User Services ............................................................................................................................. 18
    4.2.3 Wireless Client Services ............................................................................................................ 19
    4.2.4 Unauthenticated Services .......................................................................................................... 20
5 CRYPTOGRAPHIC KEY MANAGEMENT .................................................................................................. 21
  5.1 IMPLEMENTED ALGORITHMS ............................................................................................................ 21
6 CRITICAL SECURITY PARAMETERS ...................................................................................................... 22
7 SELF TESTS ............................................................................................................................................. 25
1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the AP-120 series 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.

1.1 Acronyms and Abbreviations

AES  Advanced Encryption Standard
AP  Access Point
CBC  Cipher Block Chaining
CLI  Command Line Interface
CO  Crypto Officer
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.

2.1 Aruba AP-120 Series Series

This section introduces the Aruba AP-120 series Wireless Access Points (APs) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

![Figure 1 – Aruba AP-120 Series Wireless Access Points](image)

The Aruba AP-124 and AP are high-performance 802.11n (3x3) MIMO, dual-radio (concurrent 802.11a/n + b/g/n) indoor wireless access points capable of delivering combined wireless data rates of up to 600Mbps. 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-120 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 IEEE 802.11a, 802.11b, 802.11g, and 802.11n transceivers, and up to 3 integrated or external omni-directional multi-band dipole antenna elements may be attached to the module.

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

The evaluated hardware versions are designated as

- AP-124-F1: Rev 01
- AP-125-F1: Rev 01

The evaluated firmware versions are designated as ArubaOS 3.3.2.18-FIPS, 3.3.2.19-FIPS, 3.3.2.20-FIPS, 3.3.2.21-FIPS, 3.4.2.3-FIPS, 3.4.4.0-FIPS and 3.4.5.1-FIPS.

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 4.9” x 5.13” x 2.0” (124mm x 130mm x 51mm)
2.1.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Auto-sensing link speed and MDI/MDX
- Antenna (model Aruba AP-124 only)
  - 3 x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x RJ-45 console interface

The module provides the following power interfaces:

- 48V DC 802.3af or 802.3at or PoE + interoperable Power-over-Ethernet (PoE) with intelli-source PSE sourcing intelligence
- 5V DC for external AC supplied power (adapter sold separately)

2.1.1.3 Indicator LEDs

There are 5 bicolor (power, ENET 0, 1, and WLAN) LEDs which operate as follows:

<table>
<thead>
<tr>
<th>Label</th>
<th>Function</th>
<th>Action</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>AP power / ready status</td>
<td>Off</td>
<td>No power to AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Power applied, bootloader starting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flashing - Green</td>
<td>Device booting, not ready</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Green</td>
<td>Device ready</td>
</tr>
<tr>
<td>ENET 0</td>
<td>Ethernet Network Link Status / Activity</td>
<td>Off</td>
<td>Ethernet link unavailable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Amber</td>
<td>10/100Mbs Ethernet link negotiated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Green</td>
<td>1000Mbs Ethernet link negotiated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flashing</td>
<td>Ethernet link activity</td>
</tr>
<tr>
<td>ENET 1</td>
<td>Ethernet Network Link Status / Activity</td>
<td>Off</td>
<td>Ethernet link unavailable</td>
</tr>
<tr>
<td>(Dual radio only)</td>
<td></td>
<td>On - Amber</td>
<td>10/100Mbs Ethernet link negotiated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Green</td>
<td>1000Mbs Ethernet link negotiated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flashing</td>
<td>Ethernet link activity</td>
</tr>
<tr>
<td>WLAN 2.4Ghz</td>
<td>2.4GHz Radio Status</td>
<td>Off</td>
<td>2.4GHz radio disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Amber</td>
<td>2.4GHz radio enabled in WLAN mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On – Green</td>
<td>2.4GHz radio enabled in 802.11n mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flashing</td>
<td>2.4GHz Air monitor</td>
</tr>
<tr>
<td>WLAN 5Ghz</td>
<td>5GHz Radio Status</td>
<td>Off</td>
<td>5GHz radio disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On - Amber</td>
<td>5GHz radio enabled in WLAN mode</td>
</tr>
<tr>
<td>Label</td>
<td>Function</td>
<td>Action</td>
<td>Status</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>--------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>On – Green</td>
<td>5GHz radio enabled in 802.11n mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flashing</td>
<td>2.4GHz Air monitor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard. In addition, it provides information on placing the module in a FIPS 140-2 approved configuration.

3.1 Security Levels

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

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 tested 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.

For physical security, the AP requires Tamper-Evident Labels (TELS) to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:
3.2.1 Aruba AP-124 TEL Placement

Following is the TEL placement for the Aruba AP-124:
3.2.2 Aruba AP-125 TEL Placement

Following is the TEL placement for the Aruba AP-125:

3.2.3 Inspection/Testing of Physical Security Mechanisms

<table>
<thead>
<tr>
<th>Physical Security Mechanism</th>
<th>Recommended Test Frequency</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper-evident labels (TELs)</td>
<td>Once per month</td>
<td>Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELs</td>
</tr>
<tr>
<td>Opaque module enclosure</td>
<td>Once per month</td>
<td>Examine module enclosure for any evidence of new openings or other access to the module internals.</td>
</tr>
</tbody>
</table>
3.3 Modes of Operation

The module supports multiple FIPS approved modes of operation, including the Mesh Point mode, Remote Mesh Portal mode, Remote AP mode and Control Plane Security protected AP (CPSec AP) mode, as well as a non-approved mode. This section explains how to place the module in FIPS mode, and how to verify that it is in this mode.

The access point is managed by an Aruba Mobility Controller, 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.

After setting up the Access Point by following the basic installation instructions in the module User Manual, the Crypto Officer performs the following steps:

1. Apply TELs according to the directions in section 3.2
2. Log into the administrative console of the staging controller
4. If deploying the AP in Remote Mesh Portal/Point 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 16 ASCII characters or 64 hexadecimal digits in length; generation of such keys is outside the scope of this policy
5. If deploying the AP in CPSec AP mode, configure the staging controller with CPSec under Configuration > Controller > Control Plane Security tab. AP will authenticate to the controller using certificate based authentication to establish IPSec. AP is configured with RSA key pair at manufacturing. AP’s certificate is signed by Aruba Certification Authority (trusted by all Aruba controller’s) and AP’s RSA private key is protected by AP’s TPM. Refer to “Configuring Control Plane Security” Section in ArubaOS User Manual for details on the steps.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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/Mesh Point/Remote Mesh Portal/CPSec AP 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 AP or 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 AP’s TPM and is generated at manufacturing time in factory.

b. During the provisioning process as Mesh Point or Remote Mesh Portal, the WPA2 PSK is input to the module via the corresponding Mesh cluster profile. This key is stored on flash encrypted.

c. 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.

11. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration

12. Terminate the administrative session

13. 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 using IPsec.

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

### 3.4 Operational Environment

The operational environment is non-modifiable. The Operating System (OS) is Linuz, a real-time multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly. Only Aruba-provided Crypto Officer interfaces are used. There is no user interface provided.
3.5 Logical Interfaces

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

Table 2 - FIPS 140-2 Logical Interfaces

<table>
<thead>
<tr>
<th>FIPS 140-2 Logical Interface</th>
<th>Module Physical Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Input Interface</td>
<td>10/100/1000 Ethernet Ports</td>
</tr>
<tr>
<td></td>
<td>802.11a/b/g/n Radio Transceiver</td>
</tr>
<tr>
<td>Data Output Interface</td>
<td>10/100/1000 Ethernet Ports</td>
</tr>
<tr>
<td></td>
<td>802.11a/b/g/n Radio Transceiver</td>
</tr>
<tr>
<td>Control Input Interface</td>
<td>10/100/1000 Ethernet Ports (PoE)</td>
</tr>
<tr>
<td></td>
<td>5V power input jack</td>
</tr>
<tr>
<td>Status Output Interface</td>
<td>10/100/1000 Ethernet Ports</td>
</tr>
<tr>
<td></td>
<td>802.11a/b/g/n Radio Transceiver</td>
</tr>
<tr>
<td></td>
<td>RJ-45 Serial Console Interface</td>
</tr>
<tr>
<td></td>
<td>LEDs</td>
</tr>
<tr>
<td>Power Interface</td>
<td>Power Supply</td>
</tr>
<tr>
<td></td>
<td>PoE</td>
</tr>
</tbody>
</table>

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 (5V DC or PoE). It also consists of all of the data that is entered into the access point while using the management interfaces.
- 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 may be 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.

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 a Remote AP, CPSec AP or as a Mesh AP:

- **Remote AP:**
  - 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 standard 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 configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access/bridging services. In advanced Remote AP configuration, when Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2-PSK only.

- **CPSec AP:**
  - 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 standard configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
  - Wireless Client role: in CPSec AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

- **Mesh AP (Mesh Point or Remote Mesh Portal configuration):**
  - 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.
  - User role: the second (or third, or nth) AP in a given mesh cluster
  - Wireless Client role: in Mesh 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

The Aruba Mobility Controller implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPsec. Crypto Officer authentication is accomplished via either proof of possession of the IKE preshared key or AP’s RSA key pair, which occurs during the IKE key exchange. In CPSec AP mode, AP can only authenticate using RSA key (stored in TPM).
4.1.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured as a Mesh AP, the User role is authenticated via the WPA2 preshared key. When the module is configured as a Remote AP, the User role is authenticated via the same IKE pre-shared key/RSA key pair that is used by the Crypto Officer. In CPSec AP mode, User authentication is accomplished via same RSA key pair that is used by the Crypto Officer.

4.1.3 Wireless Client Authentication

The wireless client role, in the Remote AP, Mesh AP or CPSec AP configuration authenticates to the module via WPA2. WEP and/or Open System configurations are not permitted in FIPS mode. In advanced Remote AP configuration, when Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via WPA2-PSK only.

4.1.4 Strength of Authentication Mechanisms

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

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Mechanism Strength</th>
</tr>
</thead>
</table>
| IKE shared secret (CO role) | For IKE, there are a $95^8 (=6.63 \times 10^{15})$ possible preshared keys. In order to test the guessed key, the attacker must complete an IKE aggressive mode exchange with the module. IKE aggressive mode consists of a 3 packet exchange, but for simplicity, let’s ignore the final packet sent from the AP to the attacker.

An IKE aggressive mode initiator packet with a single transform, using Diffie-Hellman group 2, and having an eight character group name has an IKE packet size of 256 bytes. Adding the eight byte UDP header and 20 byte IP header gives a total size of 284 bytes (2272 bits).

The response packet is very similar in size, except that it also contains the HASH_R payload (an additional 16 bytes), so the total size of the second packet is 300 bytes (2400 bits).

Assuming a link speed of 1Gbits/sec (this is the maximum rate supported by the module), this gives a maximum idealized guessing rate of $60,000,000,000 / 4,672 = 12,842,466$ guesses per minute. This means the odds of guessing a correct key in one minute is less than $12,842,466/(6.63\times10^{15}) = 1.94 \times 10^{-9}$, which is much less than $1$ in $10^5$. |
<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Mechanism Strength</th>
</tr>
</thead>
</table>
| Wireless Client WPA2-PSK (Wireless Client Role) | For WPA2-PSK there are at least $95^{16} (=4.4 \times 10^{31})$ possible combinations. In order to test a guessed key, the attacker must complete the 4-way handshake with the AP. Prior to completing the 4-way handshake, the attacker must complete the 802.11 association process. That process involves the following packet exchange:
  - Attacker sends Authentication request (at least 34 bytes)
  - AP sends Authentication response (at least 34 bytes)
  - Attacker sends Associate Request (at least 36 bytes)
  - AP sends Associate Response (at least 36 bytes)
  Total bytes sent: at least 140. Note that since we do not include the actual 4-way handshake, this is less than half the bytes that would actually be sent, so the numbers we derive will absolutely bound the answer.
  The theoretical bandwidth limit for IEEE 802.11n is 300Mbit, which is 37,500,000 bytes/sec. In the real world, actual throughput is significantly less than this, but we will use this idealized number to ensure that our estimate is very conservative.
  This means that the maximum number of associations (assume no delays, no inter-frame gaps) that could be completed is less than $37,500,000/214 = 267,857$ per second, or $16,071,429$ associations per minute. This means that an attacker could certainly not try more than this many keys per second (it would actually be MUCH less, due to the added overhead of the 4-way handshake in each case), and the probability of a successful attack in any 60 second interval MUST be less than $16,071,429/(4.4 \times 10^{31})$, or roughly $1$ in $10^{25}$, which is much less than $1$ in $10^5$. |
| Mesh AP WPA2 PSK (User role) | Same as Wireless Client WPA2-PSK above |
| Certificate based authentication –RSA key pair (CO role) | The module supports RSA 2048-bit keys, which has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than $1/1,000,000$. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{112})$, which is less than $1/100,000$. |
## 4.2 Services

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

### 4.2.1 Crypto Officer Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>CSPs Accessed (see section 6 below for complete description of CSPs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS mode enable/disable</td>
<td>The CO selects/de-selects FIPS mode as a configuration option.</td>
<td>None.</td>
</tr>
</tbody>
</table>
| Key Management                 | The CO can configure/modify the IKE shared secret (The RSA private key is protected by the TPM and cannot be modified) and the WPA2 PSK (used in advanced Remote AP configuration). Also, the CO/User implicitly uses the KEK to read/write configuration to non-volatile memory. | • IKE shared secret  
• WPA2 PSK  
• KEK |
<p>| Remotely reboot module         | The CO can remotely trigger a reboot                                        | KEK is accessed when configuration is read during reboot. The firmware verification key and firmware verification CA key are accessed to validate firmware prior to boot. |
| Self-test triggered by CO/User reboot | The CO can trigger a programmatic reset leading to self-test and initialization | KEK is accessed when configuration is read during reboot. The firmware verification key and firmware verification CA key are accessed to validate firmware prior to boot. |
| Update module firmware         | The CO can trigger a module firmware update                                 | The firmware verification key and firmware verification CA key are accessed to validate firmware prior to writing to flash. |
| Configure non-security related module parameters | CO can configure various operational parameters that do not relate to security | None. |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>CSPs Accessed (see section 6 below for complete description of CSPs)</th>
</tr>
</thead>
</table>
| Creation/use of secure management session between module and CO | The module supports use of IPsec for securing the management channel.        | • IKE Preshared Secret  
• DH Private Key  
• DH Public Key  
• IPsec session encryption keys  
• IPsec session authentication keys  
• RSA key pair |
| Creation/use of secure mesh channel                           | The module requires secure connections between mesh points using 802.11i.    | • WPA2-PSK  
• 802.11i PMK  
• 802.11i PTK  
• 802.11i EAPOL MIC Key  
• 802.11i EAPOL Encryption Key  
• 802.11i AES-CCM key  
• 802.11i GMK  
• 802.11i GTK  
• 802.11i AES-CCM key |
| System Status                                                 | CO may view system status information through the secured management channel | See creation/use of secure management session above.                  |

Note: CO role module services are same across all AP modes.

### 4.2.2 User Services

The following Module Services are provided for the User role in Mesh AP mode:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>CSPs Accessed (see section 6 below for complete description of CSPs)</th>
</tr>
</thead>
</table>
| Generation and use of 802.11i cryptographic keys              | When the module is in mesh configuration, the inter-module mesh links are secured with 802.11i. | • 802.11i PMK  
• 802.11i PTK  
• 802.11i EAPOL MIC Key  
• 802.11i EAPOL Encryption Key  
• 802.11i AES-CCM key |
### 4.2.3 Wireless Client Services

The following Module Services are provided for the Wireless Client role:

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>CSPs Accessed (see section 6 below for complete description of CSPs)</th>
</tr>
</thead>
</table>
| Use of WPA preshared key for establishment of IEEE 802.11i keys | When the module is in mesh configuration, the inter-module mesh links are secured with 802.11i. This is authenticated with a shared secret.                                                               | • 802.11i GMK  
• 802.11i GTK                                                                                           |
| Use of WPA preshared key 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.                                                                 | • WPA2 PSK                                                                  |
| Wireless bridging services                   | The module bridges traffic between the wireless client and the wired network.                                                                                                                               | None                                                                              |

For Remote AP and CPSec AP mode User services, please refer to Section 4.2.1, “Crypto Officer Services”
4.2.4 Unauthenticated Services

The module provides the following unauthenticated services, which are available regardless of role. No CSPs are accessed by these services.

- System status – SYSLOG and module LEDs
- 802.11 a/b/g/n
- FTP
- TFTP
- NTP
- GRE tunneling of 802.11 wireless user frames (when acting as a “Local AP”)
- Reboot module by removing/replacing power
- Self-test and initialization at power-on
5 Cryptographic Key Management

5.1 Implemented Algorithms
FIPS-approved cryptographic algorithms have been implemented in hardware and software. Some modules provide Cavium Octeon 5010 hardware encryption acceleration for bulk cryptographic operations for the following FIPS-approved algorithms:

- AES (Cert. #861) - CBC; 128, 192, 256 bits - CCM; 128 bits, Assoc. Data Len Range: 15 - 30, Payload Length Range: 0 - 32, Nonce Length(s): 13, Tag Length(s): 8
- TDES (Cert. #708) - CBC; 192 bits (168 used)/1,2,3 keys keying option
- SHA-1 (Cert. #856) - BYTE oriented
- HMAC SHA-1 (Cert. #478)

Hardware encryption is provided for the following non-FIPS-approved algorithms.
- MD5

The firmware implementation uses OpenSSL FIPS crypto library version 1.1.1, as well as the UBOOT bootloader. The firmware implements the following FIPS-approved algorithms:

- OpenSSL Module
  - AES (Cert. #900) - CBC: 128, 192, 256 bits
  - Triple-DES (Cert. #734) - CBC key options Keying Options 1,2,3 used
  - SHA-1 (Cert. #892) - BYTE oriented
  - HMAC SHA-1 (Cert. #503)
  - RSA (Cert. #436)
  - RNG (Cert. #516)

- UBOOT Bootloader cryptographic module
  - SHA-1 (Cert. #891) - BYTE oriented
  - RSA (Cert. #435)

The firmware implements the following non-FIPS-approved algorithms in firmware:
- MD5

The firmware implements the following non-approved but allowed algorithms in firmware:
- Diffie-Hellman

Diffie-Hellman key establishment methodology provides 80-bits of encryption strength.
## 6 Critical Security Parameters

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

<table>
<thead>
<tr>
<th>CSP</th>
<th>CSP TYPE</th>
<th>GENERATION</th>
<th>STORAGE And ZEROIZATION</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEK</td>
<td>TDES key</td>
<td>Hard-coded</td>
<td>Stored in flash, zeroized by the ‘ap wipe out flash’ command.</td>
<td>Encrypts IKE preshared keys and configuration parameters</td>
</tr>
<tr>
<td>IKE Pre-shared secret</td>
<td>64 character preshared key</td>
<td>Externally generated</td>
<td>Encrypted in flash using the KEK; zeroized by updating through administrative interface, or by the ‘ap wipe out flash’ command.</td>
<td>Module and crypto officer authentication during IKE; entered into the module in plaintext during initialization and encrypted over the IPSec session subsequently.</td>
</tr>
<tr>
<td>IPsec session encryption keys</td>
<td>168-bit TDES, 128/192/256 bit AES keys;</td>
<td>Established during Diffie-Hellman key agreement</td>
<td>Stored in plaintext in volatile memory; zeroized when session is closed or system powers off</td>
<td>Secure IPsec traffic</td>
</tr>
<tr>
<td>IPsec session authentication keys</td>
<td>HMAC SHA-1 keys</td>
<td>Established during Diffie-Hellman key agreement</td>
<td>Stored in plaintext in volatile memory; zeroized when session is closed or system powers off</td>
<td>Secure IPsec traffic</td>
</tr>
<tr>
<td>IKE Diffie-Hellman Private key</td>
<td>1024-bit Diffie-Hellman private key</td>
<td>Generated internally during IKE negotiation</td>
<td>Stored in plaintext in volatile memory; zeroized when session is closed or system is powered off</td>
<td>Used in establishing the session key for IPsec</td>
</tr>
<tr>
<td>IKE Diffie-Hellman public key</td>
<td>1024-bit Diffie-Hellman private key</td>
<td>Generated internally during IKE negotiation</td>
<td>Stored in plaintext in volatile memory</td>
<td>Used in establishing the session key for IPsec</td>
</tr>
<tr>
<td>PRNG seeds</td>
<td>PRNG Seed (8 bytes)</td>
<td>Generated by non-approved PRNG</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>Seed PRNG</td>
</tr>
<tr>
<td>PRNG Keys</td>
<td>PRNG Keys (16 bytes, TDES 2-keying option)</td>
<td>Generated by non-approved PRNG</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>PRNG operation</td>
</tr>
<tr>
<td>CSP</td>
<td>CSP TYPE</td>
<td>GENERATION</td>
<td>STORAGE And ZEROIZATION</td>
<td>USE</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>------------</td>
<td>-------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>WPA2 PSK</td>
<td>16-64 character shared secret used to authenticate mesh connections and in remote AP advanced configuration</td>
<td>Externally generated</td>
<td>Encrypted in flash using the KEK; zeroized by updating through administrative interface, or by the ‘ap wipe out flash’ command.</td>
<td>Used to derive the PMK for 802.11i mesh connections between APs and in advanced Remote AP connections; programmed into AP by the controller over the IPSec session.</td>
</tr>
<tr>
<td>802.11i Pairwise Master Key (PMK)</td>
<td>512-bit shared secret used to derive 802.11i session keys</td>
<td>Internally generated using WPA PSK</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>Used to derive 802.11i Pairwise Transient Key (PTK)</td>
</tr>
<tr>
<td>802.11i Pairwise Transient Key (PTK)</td>
<td>512-bit shared secret from which Temporal Keys (TKs) are derived</td>
<td>Derived during 802.11i 4-way handshake</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>All session encryption/decryption keys are derived from the PTK</td>
</tr>
<tr>
<td>802.11i EAPOL MIC Key</td>
<td>128-bit shared secret used to protect 4-way (key) handshake</td>
<td>Derived from PTK</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>Used for integrity validation in 4-way handshake</td>
</tr>
<tr>
<td>802.11i EAPOL Encr Key</td>
<td>128-bit shared secret used to protect 4-way handshakes</td>
<td>Derived from PTK</td>
<td>In volatile memory only; zeroized on reboot</td>
<td>Used for confidentiality in 4-way handshake</td>
</tr>
<tr>
<td>802.11i data AES-CCM encryption/mic key</td>
<td>128-bit AES-CCM key</td>
<td>Derived from PTK</td>
<td>Stored in plaintext in volatile memory; zeroized on reboot</td>
<td>Used for 802.11i packet encryption and integrity verification (this is the CCMP or AES-CCM key)</td>
</tr>
<tr>
<td>802.11i Group Master Key (GMK)</td>
<td>256-bit secret used to derive GTK</td>
<td>Internally generated from approved RNG</td>
<td>Stored in plaintext in volatile memory; zeroized on reboot</td>
<td>Used to derive Group Transient Key (GTK)</td>
</tr>
<tr>
<td>802.11i Group Transient Key (GTK)</td>
<td>256-bit shared secret used to derive group (multicast) encryption and integrity keys</td>
<td>Internally derived by AP which assumes “authenticator” role in handshake</td>
<td>Stored in plaintext in volatile memory; zeroized on reboot</td>
<td>Used to derive multicast cryptographic keys</td>
</tr>
<tr>
<td>CSP</td>
<td>CSP TYPE</td>
<td>GENERATION</td>
<td>STORAGE And ZEROIZATION</td>
<td>USE</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>802.11i Group AES-CCM Data Encryption/MIC Key</td>
<td>128-bit AES-CCM key derived from GTK</td>
<td>Derived from 802.11 group key handshake</td>
<td>Stored in plaintext in volatile memory; zeroized on reboot</td>
<td>Used to protect multicast message confidentiality and integrity (AES-CCM)</td>
</tr>
<tr>
<td>Firmware verification key</td>
<td>2048-bit RSA public key</td>
<td>Externally generated</td>
<td>Stored in plaintext in bootloader image</td>
<td>Used to validate the signature on firmware image</td>
</tr>
<tr>
<td>Firmware CA key</td>
<td>2048-bit RSA public key</td>
<td>Externally generated</td>
<td>Stored in plaintext in bootloader image</td>
<td>Used to validate certificate containing Firmware verification key</td>
</tr>
<tr>
<td>RSA private Key</td>
<td>2048-bit RSA private key</td>
<td>Generated on the AP (remains in AP at all times)</td>
<td>Stored in and protected by AP’s TPM</td>
<td>Used for IKE authentication when AP is authenticating using certificate based authentication</td>
</tr>
<tr>
<td>RSA public Key</td>
<td>2048-bit RSA public key</td>
<td>Generated on the AP</td>
<td>Stored in plaintext in flash.</td>
<td>Used for IKE authentication when AP is authenticating using certificate based authentication</td>
</tr>
</tbody>
</table>
7 Self Tests
The module performs both power-up and conditional self-tests. 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-up self-tests:

- Software Integrity Test–The module checks the integrity of its firmware by validating a 2048-bit RSA digital signature over the same image to ensure its authenticity.
- Cryptographic Algorithm Tests – These tests are run at power-up for the TDES encryption/decryption, AES and AES-CCM encryption/decryption, SHA-1 known answer test, HMAC SHA-1 known answer test, RSA signature verification, and the PRNG random data generation.

The following Conditional Self-tests are performed in the module:

- Continuous Random Number Generator Test–This test is run upon generation of random data by the module's random number generators to detect failure to a constant value.

These self-tests are run for the Cavium hardware cryptographic implementation as well as for the OpenSSL implementation.

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

For an AES cavium hardware POST failure:
Starting HW SHA1 KAT ...Completed HW SHA1 KAT
Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT
Starting HW DES KAT ...Completed HW DES KAT
Starting HW AES KAT ...Restarting system.