



**Hewlett Packard  
Enterprise**

# Aruba Crypto Module

Firmware Version 1.0

Non-Proprietary Security Policy

FIPS 140-3 Level 1

Document Version 1.0

January 2025

## Copyright

© 2024 Hewlett Packard Enterprise Company. Hewlett Packard Enterprise Company trademarks include



, HPE Networks®, HPE Wireless Networks®, HPE Networking, the registered HPE Networking the Mobile Edge Company logo, HPE Networking 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. HPE Networking, is a Hewlett Packard Enterprise company.

The resource assets in this firmware may include abbreviated and/or legacy terminology for HPE Networking products. See <https://www.hpe.com/us/en/networking/> for current and complete HPE Networking product lines and names.

## 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:

<https://myenterpriselicense.hpe.com/cwp-ui/software>

## Legal Notice

The use of Hewlett Packard Enterprise Company switching platforms and software or firmware, 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, Hewlett Packard Enterprise Company, from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.



# Hewlett Packard Enterprise

<https://www.hpe.com/us/en/networking/>

1701 E Mossy Oaks Rd,  
Spring, TX, USA 77389  
Phone: 1-888-342-2156

## Contents

1	General.....	5
1.1	Purpose of this Document.....	5
1.2	Additional Hewlett Packard Enterprise Product Information.....	5
1.3	Acronyms and Abbreviations.....	6
1.4	Security Levels.....	7
2	Cryptographic Module Specification.....	8
2.1	Description.....	8
2.1.1	Cryptographic Module Boundary.....	8
2.2	Version Information.....	9
2.3	Operating Environments.....	9
2.4	Excluded Components.....	10
2.5	Modes of Operation.....	10
2.5.1	Approved Mode.....	10
2.5.2	Non-Approved Mode.....	10
2.6	Approved Algorithms.....	11
2.7	Non-Approved Cryptographic Algorithms Allowed in the Approved Mode of Operation.....	13
2.8	Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed.....	13
2.9	Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.....	13
3	Cryptographic Module Interfaces.....	14
4	Roles, Services, and Authentication.....	14
4.1	Authentication.....	14
4.2	Roles.....	14
4.3	Services.....	16
4.3.1	Approved Services.....	16
4.3.2	Non-Approved Services.....	18
5	Software / Firmware Security.....	19
6	Operational Environment.....	19
7	Physical Security.....	19
8	Non-Invasive Security.....	19
9	Sensitive Security Parameter (SSP) Management.....	20
9.1	Non-Deterministic Random Number Generation Specification.....	25
10	Self-Tests.....	26
11	Life-Cycle Assurance.....	29
11.1	Start-up Procedures.....	29
11.1.1	Setting Up the Hewlett Packard Enterprise Controller, Gateway, Conductor, or Controller-managed Access Point (AP) and Running Hewlett Packard Enterprise Aruba Crypto Module Automatically.....	29
11.2	Full Documentation.....	30
11.2.1	Related Hewlett Packard Enterprise Documents.....	30
11.2.2	Administrator Guidance.....	30
11.2.3	Non-Administrator Guidance.....	30
11.2.4	Maintenance Requirements.....	30
11.3	End of Life.....	31
12	Mitigation of Other Attacks.....	31

## Figures

Figure 1 – Functional Block Diagram of Cryptographic Boundary for Aruba Crypto Module.....	8
--	---

## Tables

Table 1 – Document Revision History .....	4
Table 2 – Security Levels .....	7
Table 3 – Version Information .....	9
Table 4 – Tested Operational Environments.....	9
Table 5 – Vender Affirmed Operational Environments.....	10
Table 6 – Approved Algorithms .....	11
Table 7 –Approved Algorithms Provided by the Bound OpenSSL Module .....	12
Table 8 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation .....	13
Table 9 – Ports and Interfaces .....	14
Table 10 – Roles and Authentication .....	14
Table 11 – Roles, Service Commands, Input, Output.....	15
Table 12 – Approved Services .....	16
Table 13 – Approved Services Not Using Any Approved Security Functions .....	17
Table 14 – Non-Approved Services .....	18
Table 15 – SSPs/Keys Used in the Module .....	20
Table 16 – Non-Deterministic Random Number Generation Specification .....	25
Table 17 – Pre-Operational Self-Tests.....	26
Table 18 – Conditional Cryptographic Algorithm Tests.....	26
Table 19 – Conditional Pairwise Consistency Tests.....	27

## Preface

This document may be freely reproduced and distributed whole and intact including the copyright notice. Products identified herein contain confidential commercial firmware. Valid license required.

## Document Revision History

The following table lists the history of the revisions of this document by version number and date of revision.

**Table 1 – Document Revision History**

Version	Date	Description
1.0	November 2024	Initial FIPS 140-3 release for Hewlett Packard Enterprise <i>Aruba Crypto Module</i> firmware version 1.0 used by ArubaOS firmware versions running on Hewlett Packard Enterprise hardware and virtual appliances

# 1 General

This section describes:

- The purpose of this document.
- Hewlett Packard Enterprise documents related to this document contents.
- Where to go for additional Hewlett Packard Enterprise product information.
- Acronyms and abbreviations.
- The assurance security levels for each of the areas described in the FIPS 140-3 Standard.

## 1.1 Purpose of this Document

This release supplement provides information regarding the Hewlett Packard Enterprise *Aruba Crypto Module* firmware version 1.0 FIPS 140-3 Level 1 validation from Hewlett Packard Enterprise (HPE). Throughout this document, references to HPE Networking are to the Hewlett Packard Enterprise division. The material in this supplement modifies the general Hewlett Packard Enterprise firmware documentation included with this product and should be kept with your Hewlett Packard Enterprise product documentation.

This supplement primarily covers the non-proprietary Cryptographic Module Security Policy for the Hewlett Packard Enterprise *Aruba Crypto Module* firmware version 1.0. This security policy describes how the module meets the security requirements of FIPS 140-3 Level 1 and how to place and maintain the module in the secure Approved mode. This policy was prepared as part of the FIPS 140-3 Level 1 validation of the product.

FIPS 140-3 (Federal Information Processing Standards Publication 140-3, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. FIPS 140-3 aligns with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the Cryptographic Module Validation Program (CMVP), as a validation authority. The testing for these requirements will be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) website at:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program>

In addition, in this document, the Hewlett Packard Enterprise *Aruba Crypto Module* is referred to as the module, the cryptographic module, and Aruba Crypto module.

## 1.2 Additional Hewlett Packard Enterprise Product Information

More information is available from the following sources:

- See the Hewlett Packard Enterprise web site for the full line of products from HPE Networking:  
<https://www.hpe.com/us/en/networking/>
- The NIST Validated Modules web site contains contact information for answers to technical or sales-related questions for the product:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>

Enter **Hewlett Packard Enterprise** in the Vendor field then select Search to see a list of FIPS validated Hewlett Packard Enterprise cryptographic modules.

Select the Certificate Number for the Module Name 'Aruba Crypto Module'.

### 1.3 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security, a branch of CSE
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPSec	Control Plane Security protected
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DF	Derivation Function
EAP	Extensible Authentication Protocol
ECO	External Crypto Officer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESV	Entropy Source Validation
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 Tunnelling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PCT	Pairwise Consistency Test
PSP	Public Security Parameter
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSP	Sensitive Security Parameter
SPOE	Serial & Power Over Ethernet
TEL	Tamper-Evident Label
TFTP	Trivial File Transfer Protocol
TPM	Trusted Platform Module
WLAN	Wireless Local Area Network

## 1.4 Security Levels

The Hewlett Packard Enterprise *Aruba Crypto Module* is intended to meet overall FIPS 140-3 Level 1 requirements as shown in the following table.

**Table 2 – Security Levels**

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A
<b>Overall</b>	<b>Overall Security Rating of the Module</b>	<b>1</b>

## 2 Cryptographic Module Specification

### 2.1 Description

#### Purpose and Use:

The Hewlett Packard Enterprise *Aruba Crypto Module* version 1.0 (also referred to as ‘the module’) is a firmware type cryptographic module and was validated under FIPS 140-3 Level 1 requirements and meets the claims made in this document. ArubaOS is the operating system for Hewlett Packard Enterprise Mobility Conductors, Mobility Controllers/Gateways, and controller-managed Hewlett Packard Enterprise Access Points (APs). The Hewlett Packard Enterprise *Aruba Crypto Module* (firmware) is an Hewlett Packard Enterprise cryptographic module that provides cryptographic services for the ArubaOS operating system running on the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances.

The Hewlett Packard Enterprise *Aruba Crypto Module* uses the Hewlett Packard Enterprise *Aruba OpenSSL Module* as a bound module (also referred to as ‘the bound OpenSSL module’) to provide the underlying cryptographic algorithms necessary for the Random Number Generation (RNG) service. The Hewlett Packard Enterprise *Aruba OpenSSL Module* version 1.0 is a validated cryptographic module with CMVP certificate #4929. Both the Hewlett Packard Enterprise *Aruba Crypto Module* and *Aruba OpenSSL Module* were validated under and met FIPS 140-3 Level 1 requirements.

**Module Type:** Firmware

**Module Embodiment:** Multiple-chip Standalone

#### 2.1.1 Cryptographic Module Boundary

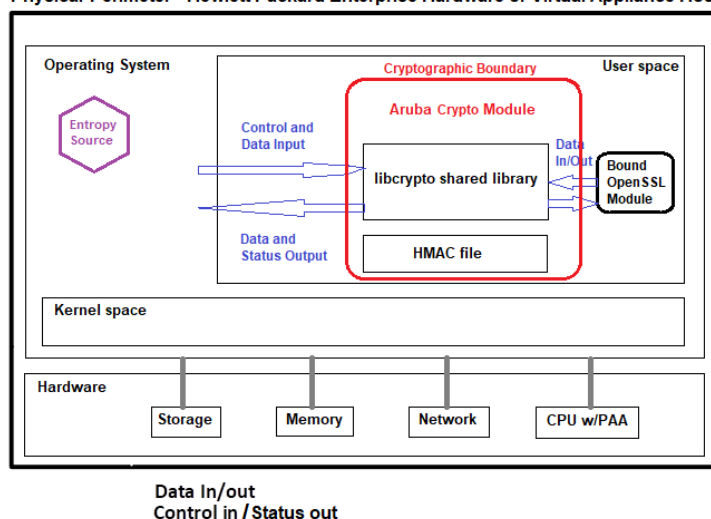
The Hewlett Packard Enterprise *Aruba Crypto Module* (firmware) is an Hewlett Packard Enterprise cryptographic module that provides cryptographic services for the ArubaOS operating system.

The cryptographic boundary for the Hewlett Packard Enterprise *Aruba Crypto Module* is defined as the module component within the Linux-based User Space. The physical perimeter is the production-grade enclosure of the hardware chassis of the Hewlett Packard Enterprise hardware device or Hewlett Packard Enterprise virtual appliance host.

The module is one of the components within the ArubaOS firmware package in electronic form and is installed automatically when a trusted and verified ArubaOS is booted on an Hewlett Packard Enterprise device. The Hewlett Packard Enterprise *Aruba Crypto Module* component includes the module shared library and the associated integrity check file (used for integrity tests):

- libcrypto.so
- libcrypto.so.hmac

Physical Perimeter - Hewlett Packard Enterprise Hardware or Virtual Appliance Host



**Figure 1 – Functional Block Diagram of Cryptographic Boundary for Aruba Crypto Module**



## 2.2 Version Information

Hewlett Packard Enterprise *Aruba Crypto Module* version 1.0 was validated against FIPS 140-3 Level 1 requirements. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating a version that is not listed on the validation certificate.

**Table 3 – Version Information**

Type	Versions	'show ver' Output
Firmware	Aruba Crypto Module version 1.0	Aruba Crypto Module 1.0

## 2.3 Operating Environments

The module operates in a limited operational environment. The module runs on the ArubaOS operating system and related hardware or virtual platform and provides cryptographic services for the ArubaOS operating system. See the following tables of Tested Operational Environments and Vendor Affirmed Operational Environments for details.

**Table 4 – Tested Operational Environments**

#	Operating System	Hardware / Virtual Platform	Processor	PAA / Acceleration
1	ArubaOS 8.10	7220 Mobility Controller	Broadcom XLP432 (MIPS64)	None
2	ArubaOS 8.10	9012 Gateway	Intel Atom C3508 (Denverton)	None
3	ArubaOS 8.10	AP-515 Wireless Access Point	Broadcom BCM (64-bit ARMv8)	None
4	ArubaOS 8.10	AP-535 Wireless Access Point	Qualcomm IPQ (64-bit ARM Cortex A53)	None
5	ArubaOS 8.10	AP-635 Wireless Access Point	Qualcomm IPQ (64-bit ARM Cortex A53)	None
6	ArubaOS 8.10	AP-655 Wireless Access Point	Qualcomm IPQ (64-bit ARM Cortex A53)	None
7	ArubaOS 8.10	MCR-HW-5K Mobility Conductor Hardware Appliance	Intel Xeon E5-2620v4 (Broadwell)	with PAA
8	ArubaOS 8.10 on VMWare ESXi 7.0	MC-VA-50 Mobility Controller Virtual Appliance on HPE ProLiant ML110 Gen10	Intel Xeon Silver 4210 (Cascade Lake)	with / without PAA

**Table 5 – Vender Affirmed Operational Environments**

#	Operating System	Hardware / Virtual Platform
1	ArubaOS 8.10	70xx Mobility Controllers
2	ArubaOS 8.10	72xx Mobility Controllers
3	ArubaOS 8.10	90xx Gateways
4	ArubaOS 8.10	92xx Gateways
5	ArubaOS 8.10	AP-51x and AP-57x Wireless Access Points
6	ArubaOS 8.10	AP-50x and AP-56x Wireless Access Points
7	ArubaOS 8.10	AP-53x, AP-55x, AP-58x, and AP-63x Wireless Access Points
8	ArubaOS 8.10	MCR-HW-xxx Mobility Conductor Hardware Appliances
9	ArubaOS 8.10 on VMWare ESXi 7.0	MC-VA-xxx Mobility Controller Virtual Appliances on HPE ProLiant ML110 Gen10
10	ArubaOS 8.10 on VMWare ESXi 7.0	MCR-VA-xxx Mobility Conductor Virtual Appliances on HPE ProLiant ML110 Gen10
11	ArubaOS 8.10 on VMWare ESXi 7.0	Virtual Appliances on HPE EdgeLine 20
12	ArubaOS 8.10 on VMWare ESXi 7.0	Virtual Appliances on PacStar PS451-1258 Series
13	ArubaOS 8.10 on VMWare ESXi 7.0	Virtual Appliances on device running an equivalent Intel processor (Intel Atom, i5, i7, or Xeon)

## 2.4 Excluded Components

There are no excluded components for the module.

## 2.5 Modes of Operation

The Hewlett Packard Enterprise *Aruba Crypto Module* (firmware) is one of the Hewlett Packard Enterprise cryptographic modules that provide cryptographic services for the host ArubaOS operating system, and is installed automatically when a trusted and verified ArubaOS is booted on an Hewlett Packard Enterprise host device.

### 2.5.1 Approved Mode

When the module starts up successfully, after passing all the Cryptographic Algorithm Self-Tests (CASTs) and Pre-Operational Self-Tests (POSTs), and following the guidance in [section 11.1, Start-up Procedures](#), the module is operating in the Approved mode of operation, provided that the guidelines on services, algorithms, and key management found in this Security Policy are followed.

### 2.5.2 Non-Approved Mode

When the module starts up but FIPS Settings are not enabled as per the guidance in [section 11.1, Start-up Procedures](#), then the module is operating in non-Approved mode of operation.

## 2.6 Approved Algorithms

The firmware in the Hewlett Packard Enterprise *Aruba Crypto Module* contains the following cryptographic algorithm implementations that will be used for the corresponding security services supported by the module in the Approved mode.

**Table 6 – Approved Algorithms**

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
<a href="#">A2689</a>	AES [FIPS 197] [SP 800-38A] [SP 800-38D]	CBC, CTR, GCM <sup>1</sup>	128, 192, 256	Data Encryption/Decryption
<a href="#">A2689</a>	CVL IKEv2 <sup>2</sup> [SP 800-135 Rev1]	IKEv2	IKEv2: DH 2048-bit; SHA2-256, SHA2-384	Key Derivation
<a href="#">A2689</a>	DSA <sup>3</sup> [FIPS 186-4]	keyGen, pqgGen	L=2048, N=256, SHA2-256	Key Generation, Domain Parameter Generation
<a href="#">A2689</a>	ECDSA [FIPS 186-4]	KeyGen, KeyVer, SigGen, SigVer	KeyGen: P-256, P-384 KeyVer: P-256, P-384 SigGen: P-256, P-384 with SHA2-256, SHA2-384, SHA2-512 SigVer: P-256, P-384 with SHA-1, SHA2-256, SHA2-384, SHA2-512	Key Generation and Verification, Digital Signature Generation and Verification
<a href="#">A2689</a>	HMAC [FIPS 198-1]	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	(minimum 112 bits)	Message Authentication
<a href="#">A2689</a>	KAS-SSC [SP 800-56A Rev3]	FFC: dhEphem, ECC: Ephemeral Unified	FFC: FC with SHA2-256, MODP-2048 with SHA2-256 ECC: P-256 with SHA2-256, P-384 with SHA2-384 KAS Roles - initiator, responder	Key Agreement Scheme – Shared Secret Computation
<a href="#">A2689</a>	RSA [FIPS 186-2]	SigVer: SHA-1 <sup>4</sup> , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	1024 (for legacy SigVer only), 2048	Digital Signature Verification

<sup>1</sup> AES GCM IV generation is performed in compliance with IG C.H, Scenario 2. The IV is generated internally and randomly using the Approved DRBG that is internal to the module's boundary and has a length of 96 bits.

<sup>2</sup> No parts of the IKEv2 protocols, other than the approved cryptographic algorithms and KDF, have been tested by the CAVP and CMVP.

<sup>3</sup> DSA was CAVP tested but is only used as a pre-requisite for DH.

<sup>4</sup> SHA-1 is only Approved for use with Signature Verification.

<a href="#">A2689</a>	RSA [FIPS 186-4]	KeyGen, SigGen: SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5 SigVer: SHA-1 <sup>5</sup> , SHA2-256, SHA2-384, SHA2-512 PKCS1 v1.5	KeyGen: 2048 SigGen: 2048 SigVer: 1024 (for legacy SigVer only), 2048	Key Generation, Digital Signature Generation and Verification
<a href="#">A2689</a>	Safe Primes [SP 800-56A Rev3]	KeyGen, KeyVer	Safe Prime Groups: MODP-2048	Safe Primes Key Generation and Key Verification
<a href="#">A2689</a>	SHS [FIPS 180-4]	SHA-1, SHA2-256, SHA2-384, SHA2-512 Byte Only	160, 256, 384, 512	Message Digest
AES <a href="#">A2689</a>	KTS [SP 800-38F]	AES-GCM <sup>6</sup>	128, 256	Key Wrapping / Key Transport via IKE/IPSec
AES <a href="#">A2689</a> HMAC <a href="#">A2689</a>	KTS [SP 800-38F] [FIPS 198-1]	AES-CBC <sup>7</sup> HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	128, 192, 256	Key Wrapping / Key Transport via IKE/IPSec

The Hewlett Packard Enterprise *Aruba Crypto Module* does not implement a random number generator. Instead, it uses the Random Number Generation (RNG) service provided by the bound Hewlett Packard Enterprise *Aruba OpenSSL Module* cryptographic module, which implements a Deterministic Random Bit Generator (DRBG) compliant to [SP800-90A]. Data input and output between the Hewlett Packard Enterprise *Aruba Crypto Module* and the bound OpenSSL module are via API parameters.

**Table 7 –Approved Algorithms Provided by the Bound OpenSSL Module**

CAVP Cert.	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
<a href="#">A2690</a>	DRBG <sup>8</sup> [SP 800-90A Rev1]	AES CTR	256	Deterministic Random Bit Generation

<sup>5</sup> SHA-1 is only Approved for use with Signature Verification.

<sup>6</sup> AES-GCM is an authenticated encryption algorithm that is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides 128 or 256 bits of encryption strength.

<sup>7</sup> AES-CBC combined with HMAC is approved for use in key transport per FIPS 140-3 IG D.G. This key establishment methodology provides between 128 and 256 bits of encryption strength.

<sup>8</sup> Refer to [section 9.1, Non-Deterministic Random Number Generation Specification](#) for details of the validated entropy source used by the RNG service provided by the bound OpenSSL module.

## 2.7 Non-Approved Cryptographic Algorithms Allowed in the Approved Mode of Operation

The cryptographic module implements no non-Approved algorithms allowed for use in the Approved mode of operation.

## 2.8 Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The cryptographic module implements no non-Approved algorithms allowed in the Approved mode of operation with no security claimed.

## 2.9 Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

The cryptographic module implements the following non-Approved algorithms that are not permitted for use in the Approved mode of operations. The module does not use any non-Approved algorithms implemented in the bound OpenSSL module.

**Table 8 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation**

Algorithm	Use / Function
DES	Used for older versions of WEP in non-Approved mode
HMAC-MD5	Used for older versions of WEP in non-Approved mode
MD5	Used for older versions of WEP in non-Approved mode
RC4	Used for older versions of WEP in non-Approved mode
Null Encryption	Used for older versions of WEP in non-Approved mode
RSA	Non-compliant less than 112 bits, or when used with SHA-1 for signature generation, or when other than 2048-bit modulus sizes are used
Diffie-Hellman	key agreement; non-compliant less than 112 bits of encryption strength
EC Diffie-Hellman	key agreement; non-compliant less than 112 bits of encryption strength
ECDSA	non-compliant when using 186-2 signature generation
Triple-DES-CBC	As used in IKE/IPSec

### 3 Cryptographic Module Interfaces

As a firmware module, the module interfaces are defined as Software or Firmware Module Interfaces (SFMI), and there are no physical ports. The logical interfaces are defined as the API of the cryptographic module. The interfaces are listed in the table below.

All data output via data output interface is inhibited when the module is performing pre-operational tests or zeroization or when the module enters error state.

**Table 9 – Ports and Interfaces**

Physical Port	Logical Interface	Data That Passes Over the Interface
N/A	Data Input	API input parameters for data (includes input data received from the bound OpenSSL module)
N/A	Data Output	API output parameters for data (includes output data sent to the bound OpenSSL module)
N/A	Control Input	API function calls
N/A	Status Output	API return codes, status information, error messages
N/A	Power	None

**Notes:**

- Module API return codes to calling application: 0 = success, 1 = failure.
- The module does not implement a control output interface.

### 4 Roles, Services, and Authentication

The following section lists the roles supported by the module, authentication mechanisms used by the module, and services (both security and non-security, Approved and non-Approved) available from the module.

#### 4.1 Authentication

The Hewlett Packard Enterprise *Aruba Crypto Module* does not provide any identification or authentication methods of its own. The CO and the User roles are implicitly identified by the service requested.

#### 4.2 Roles

The module supports two distinct operator roles: the Crypto Officer role and the User role. These roles are implicitly assumed by the operator of the module when performing a service. The module does not support multiple concurrent operators, a maintenance role, nor bypass capability.

**Table 10 – Roles and Authentication**

Role	Authentication Methods	Authentication Strength
Crypto Officer	N/A – Authentication not required for Level 1	N/A
User	N/A – Authentication not required for Level 1	N/A

The table below lists descriptions of the services available to the roles, with input and output.

**Table 11 – Roles, Service Commands, Input, Output**

Role	Service	Input	Output
User	Data encryption, decryption	Plaintext or ciphertext, key	Ciphertext or plaintext
User	Key derivation function	Shared secrets, inputs (IKEv2)	Derived keys
User	Digital signature	RSA or ECDSA public and private keys	RSA or ECDSA digital signature generated or verified
User	Message authentication	Message, HMAC key	Message authentication code
User	Key agreement	DH (FFC), ECDH key agreement primitives	Derived keys
User	Safe Primes key generation and verification	DH (FFC) domain parameters	DH (FFC) private key
User	Key pair generation	Key size or curve size	RSA, DSA (FFC), or ECDSA key pairs
User	Key wrapping / Key transport	AES key	Wrapped keys
User	Message digest	Message	Digest of the message
Crypto Officer	Zeroization	Command	Progress information
Crypto Officer	Status function	Commands and configuration data	Status of commands and configurations
User	Show Version	Command	Name and version of the module
Crypto Officer	Reboot Module	Command	Progress information
Crypto Officer	Self-Test triggered by Crypto Officer reboot	Module reboot	Progress information
Crypto Officer	Approved mode enable/disable	Command	Progress information

**Note:** The Crypto Officer must ensure that the module is kept in the Approved mode of operation, following the guidance in [section 11.1, Start-up Procedures](#), and provided that the guidelines on services, algorithms, and key management found in this Security Policy are followed.

### 4.3 Services

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

The meaning of the letters used to describe the 'Access Rights to Keys and/or SSPs' are:

- **G – Generate** The module generates or derives the Key/SSP.
- **R – Read** The Key/SSP is read from the module (e.g. the Key/SSP is output).
- **W – Write** The Key/SSP is updated, imported, or written to the module.
- **E – Execute** The module uses the Key/SSP in performing a cryptographic operation.
- **Z – Zeroize** The module zeroizes the Key/SSP.

#### 4.3.1 Approved Services

See the tables below for descriptions of the services, Approved security functions, keys and/or SSPs available to the module's roles.

The Hewlett Packard Enterprise *Aruba Crypto Module* is one of the components within the ArubaOS firmware package that runs on the host device. ArubaOS includes CLI commands, some of which interact with the module via APIs. Successful completion of a security service (via API return code for success) when the module is in Approved mode (see [section 11.1, Start-up Procedures](#)) denotes use of approved security service.

**Note:**

The module does not implement a random number generator. Instead, it uses the Random Number Generation (RNG) service provided by the bound Hewlett Packard Enterprise *Aruba OpenSSL Module* cryptographic module, which implements a Deterministic Random Bit Generator (DRBG) compliant to [SP800-90A]. Data input and output between the Hewlett Packard Enterprise *Aruba Crypto Module* and the bound OpenSSL module are via API parameters.

**Table 12 – Approved Services**

Service	Description	Approved Security Functions	Keys and/or SSPs [row # in SSPs/Keys Used table]	Roles	Access Rights to Keys and/or SSPs	Indicator
Data encryption, decryption	Encrypt or decrypt data	AES-CBC AES-GCM  (A2689)	[15] IKE Session Encryption Key [16] IPSec Session Encryption Key	User	W/E  W/E	API return code for success
Key derivation function	Key derivation through SP800-135rev1-KDF (IKEv2-KDF), SP800-108rev1-KDF (KBKDF)	KBKDF IKEv2-KDF  (A2689)	[4] DH Shared Secret [7] ECDH Shared Secret [12] IKE Pre-Shared Key [13] SKEYSEED [14] IKE Session Authentication Key [15] IKE Session Encryption Key [16] IPSec Session Encryption Key [17] IPSec Session Authentication Key	User	W/E W/E W/E G/R G/R  G/R G/R G/R	API return code for success
Digital signature	Generate or verify RSA or ECDSA digital signatures	RSA SigGen RSA SigVer ECDSA SigGen ECDSA SigVer  (A2689)	[8] RSA Private Key [9] RSA Public Key [10] ECDSA Private Key [11] ECDSA Public Key	User	R/W/E R/W/E R/W/E R/W/E	API return code for success



Message authentication	Generate or verify data integrity with HMAC key	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512  (A2689)	[14] IKE Session Authentication Key [17] IPSec Session Authentication Key	User	W/E  W/E	API return code for success
Key agreement	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	KAS-ECC-SSC KAS-FFC-SSC  (A2689)	[2] DH Private Key [3] DH Public Key [4] DH Shared Secret [5] ECDH Private Key [6] ECDH Public Key [7] ECDH Shared Secret	User	W/E W/E G/R W/E W/E G/R	API return code for success
Safe Primes key generation and verification	Diffie-Hellman key generation and verification using safe primes	Safe Primes KeyGen Safe Primes KeyVer  (A2689)	[2] DH Private Key [3] DH Public Key	User	G/R G/R	API return code for success
Key pair generation	Generate RSA, FFC, or ECDSA key pairs	DSA/FFC keyGen DSA/FFC pggGen Safe Primes KeyGen Safe Primes KeyVer ECDSA/ECC KeyGen ECDSA/ECC KeyVer RSA KeyGen RSA KeyVer  (A2689)	[1] Random Data Input [2] DH Private Key [3] DH Public Key [5] ECDH Private Key [6] ECDH Public Key [8] RSA Private Key [9] RSA Public Key [10] ECDSA Private Key [11] ECDSA Public Key	User	W/E G/R G/R G/R G/R G/R G/R G/R G/R	API return code for success
Key wrapping / Key transport	AES key wrapping	AES-GCM AES-CBC with HMAC  (A2689)	[15] IKE Session Encryption Key [16] IPSec Session Encryption Key	User	W/E  W/E	API return code for success
Message digest	Generate a SHA-1 or SHA2 message digest	SHA-1 SHA2-256 SHA2-384 SHA2-512  (A2689)	None	User	None	API return code for success

**Table 13 – Approved Services Not Using Any Approved Security Functions**

Service	Description	Approved Security Functions	Keys and/or SSPs [row # in SSPs/Keys Used table]	Roles	Access Rights to Keys and/or SSPs	Indicator
Approved mode enable/disable	The Crypto Officer enables the Approved mode by following the procedures under section <a href="#">11.1, Start-up Procedures</a> , to ensure the Aruba host device is configured for Secure Operations.	None	None	Crypto Officer	None	API return code for success
Status Function	Crypto Officer may use ArubaOS CLI “show” commands on host to view logs and status. Please see ArubaOS CLI guide for details.	None	None	Crypto Officer	None	API return code for success

Show Version	User may use ArubaOS CLI “ <code>show ver</code> ” command on host to view module name and version in log.	None	None	User	None	API return code for success
Reboot module	The Crypto Officer may remotely trigger a reboot. The module can also reboot by removing/replacing power to the host device.	None	None	Crypto Officer	None	API return code for success
Self-Test triggered by Crypto Officer reboot	Perform pre-operational self-tests and conditional cryptographic algorithm tests (refer to section <a href="#">10. Self-Tests</a> ) on demand through module reboot.	None	None	Crypto Officer	None	API return code for success
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKE Pre-shared key and RSA/ECDSA Private/Public keys) stored in the host flash can be zeroized by using the ArubaOS command ‘ <code>wipe out flash</code> ’ on the host or by overwriting with a new secret. Please see ArubaOS CLI guide for details.	None	All SSPs will be destroyed.	Crypto Officer	Z	API return code for success

### 4.3.2 Non-Approved Services

The non-Approved services listed in the table below are available in the non-Approved mode but are not available in the Approved mode (see [section 11.1, Start-up Procedures](#)). The module does not support a degraded mode of operation.

**Table 14 – Non-Approved Services**

Service	Description	Algorithms Accessed	Roles
IPSec/IKE using Triple-DES	IPSec/IKE key management using Triple-DES. This is a non-Approved service not available in the Approved mode.	Triple-DES	User
Use of non-Approved algorithms and/or sizes.	If the module has not been provisioned to operate in the Approved mode, then non-Approved algorithms and/or sizes are available for use – see above <a href="#">Table 8, Non-Approved Algorithms Not Allowed in the Approved Mode of Operation</a> . This is a non-Approved service not available in the Approved mode.	Non-Approved algorithms and/or sizes	User

**Note:** For additional information, please refer to the *ArubaOS 8.10 User Guide*.

## 5 Software / Firmware Security

The Hewlett Packard Enterprise *Aruba Crypto Module* (firmware version 1.0) is an Hewlett Packard Enterprise cryptographic module that provides cryptographic services for the ArubaOS operating system. The module is one of the components within the ArubaOS firmware package in electronic form and is installed automatically when a trusted and verified ArubaOS firmware package signed by Hewlett Packard Enterprise is booted on an Hewlett Packard Enterprise host device.

The module performs a firmware integrity test when powered on (refer to [Self-Tests](#) for details). All cryptographic algorithm self-tests are run at power-up, prior to the first operational use of the cryptographic algorithm. The firmware integrity test verifies the integrity of the module by comparing a calculated HMAC-SHA-1 value against the stored HMAC value.

The operator can initiate the firmware integrity test on demand by rebooting the host. Rebooting also zeroizes all SSPs stored in SDRAM memory. All data output via the data output interface is inhibited until the firmware integrity test has completed successfully. If the firmware integrity test fails, the module enters the error state (while in this state, the module provides no functionality). The temporary values generated during the firmware integrity test are zeroized upon completion of the integrity test. After the ArubaOS firmware boot, the operator can determine the version of the loaded module through reviewing the log and by using the show version ArubaOS CLI command on the host (use the link in the section [Full Documentation](#) to refer to *ArubaOS 8.10 Command-Line Interface Reference Guide* and *ArubaOS 8.10 User Guide*).

## 6 Operational Environment

The operational environment is limited.

The control plane Operating System (OS) is Linux, a multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly. Only Hewlett Packard Enterprise provided interfaces are used. The Hewlett Packard Enterprise *Aruba Crypto Module* is one of the components within the ArubaOS firmware package which runs on the host device. ArubaOS includes Command Line Interface (CLI) commands, some of which interact with the module via APIs. The ArubaOS CLI and the module APIs are restricted command sets. These operating control mechanisms protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data.

The module was tested on the platforms listed above in [section 2.3, Table 4, Tested Operational Environments](#).

## 7 Physical Security

The Hewlett Packard Enterprise *Aruba Crypto Module* is a firmware type module and obtains its physical security from the host platform. As per FIPS 140-3 for multiple-chip standalone cryptographic modules at Security Level 1, the host platform consists of production-grade components within a production-grade enclosure. All of the platforms listed above in [section 2.3](#) meet these requirements.

## 8 Non-Invasive Security

Since the module has not been purposely designed, built and publicly documented to include non-invasive mitigation techniques, the Non-Invasive Security requirements are not applicable.

## 9 Sensitive Security Parameter (SSP) Management

The following are the Sensitive Security Parameters (SSPs) used in the module. As specified in the Zeroization column of the following table, the majority of SSPs/Keys used in the module are zeroized implicitly by rebooting the module, indicated implicitly via the successful completion of the module reboot service. The Hewlett Packard Enterprise *Aruba Crypto Module* is one of the components within the ArubaOS firmware package that runs on the host device, thus the module is rebooted when the host device is rebooted. ArubaOS includes CLI commands. As specified in the Zeroization column of the following table, there are a minority of SSPs/Keys used in the module that are stored in the host flash. The host flash can be zeroized implicitly by using the ArubaOS CLI command 'wipe out flash' on the host device.

**Table 15 – SSPs/Keys Used in the Module**

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
<b>General Keys/SSPs</b>									
1	Random Data Input – CSP [EVM]	512 bits	SP800-90A Rev1 CTR_DRBG AES-256 Cert. # <a href="#">A2690</a>	64 bytes are retrieved by bound OpenSSL module DRBG on each call by any service that requires a random number.	Import: From bound OpenSSL module via API parameters. Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Random data inputs for key generation.
2	Diffie-Hellman Private Key – CSP	112 bits	Diffie-Hellman Group 14 Cert. # <a href="#">A2689</a>	Generated internally in compliance with Diffie-Hellman key agreement scheme by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> )	Import: From calling application Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used during the IPSec handshake to establish the Diffie-Hellman Shared Secret.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
3	Diffie-Hellman Public Key – PSP	112 bits	Diffie-Hellman Group 14 Cert. # <a href="#">A2689</a>	Generated internally in compliance with Diffie-Hellman key agreement scheme by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> )	Import: From calling application Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used during the IPSec handshake to establish the Diffie-Hellman Shared Secret.
4	Diffie-Hellman Shared Secret – CSP	112 bits	Diffie-Hellman Group 14 Cert. # <a href="#">A2689</a>	N/A	Import: N/A Export: To calling application	Established during Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for deriving IPSec/IKE cryptographic keys.
5	EC Diffie-Hellman Private Key – CSP	Curves: P-256 or P-384	EC Diffie-Hellman Cert. # <a href="#">A2689</a>	Generated internally by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ) during EC Diffie-Hellman Exchange.	Import: From calling application Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for establishing EC Diffie-Hellman Shared Secret.
6	EC Diffie-Hellman Public Key – PSP	Curves: P-256 or P-384	EC Diffie-Hellman Cert. # <a href="#">A2689</a>	Generated internally by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ) during EC Diffie-Hellman Exchange.	Import: From calling application Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for establishing EC Diffie-Hellman Shared Secret.
7	EC Diffie-Hellman Shared Secret – CSP	128 or 192 bits	EC Diffie-Hellman Cert. # <a href="#">A2689</a>	N/A	Import: N/A Export: To calling application	Established during EC Diffie-Hellman Exchange.	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	Used for deriving IPSec/IKE cryptographic keys.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
8	RSA Private Key – CSP	128 bits	RSA Private Key Cert. # <a href="#">A2689</a>	Generated by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ), in compliance with FIPS 186-4 RSA key pair generation method.	Import: From calling application Export: To calling application	N/A	Stored in host Flash memory (plaintext).	Zeroized by using ArubaOS command 'wipe out flash' on host.	Used for IKEv2 peers authentication.
9	RSA Public Key – PSP	128 bits	RSA Public Key Cert. # <a href="#">A2689</a>	Generated by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ), in compliance with FIPS 186-4 RSA key pair generation method.	Import: From calling application Export: To calling application	N/A	Stored in host Flash memory (plaintext).	Zeroized by using ArubaOS command 'wipe out flash' on host.	Used for IKEv2 peers authentication.
10	ECDSA Private Key – CSP	Curves: P-256 or P-384	ECDSA SigGen Cert. # <a href="#">A2689</a>	Generated by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ), in compliance with FIPS 186-4 ECDSA key pair generation method.	Import: From calling application Export: To calling application	N/A	Stored in host Flash memory (plaintext).	Zeroized by using ArubaOS command 'wipe out flash' on host.	Used for IKEv2 peers authentication.
11	ECDSA Public Key – PSP	Curves: P-256 or P-384	ECDSA SigGen Cert. # <a href="#">A2689</a>	Generated by calling bound OpenSSL module Approved DRBG (Cert. # <a href="#">A2690</a> ), in compliance with FIPS 186-4 ECDSA key pair generation method.	Import: From calling application Export: To calling application	N/A	Stored in host Flash memory (plaintext).	Zeroized by using ArubaOS command 'wipe out flash' on host.	Used for IKEv2 peers authentication.
<b>IPSec/IKE</b>									

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
12	IKE Pre-Shared Key – CSP	8 - 64 ASCII or 64 HEX characters	N/A	N/A	Import: From calling application Export: N/A	N/A	Stored in host Flash memory (plaintext).	Zeroized by using ArubaOS command 'wipe out flash' on host or by overwriting with a new secret.	Used for IKEv2 peers authentication.
13	SKEYSEED – CSP	160 / 256 / 384 bits	IKEv2 KDF Cert. # <a href="#">A2689</a>	Derived via key derivation function defined in SP800-135 Rev1 KDF (IKEv2).	Import: N/A Export: N/A	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	A shared secret known only to IKEv2 peers. Used for deriving other keys in IKEv2 protocol.
14	IKE Session Authentication Key – CSP	160 / 256 / 384 bits	HMAC-SHA-1/ HMAC-SHA2-256/384 Cert. # <a href="#">A2689</a>	Derived via key derivation function defined in SP800-135 Rev1 KDF (IKEv2).	Import: N/A Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IKE session (IKE Phase I) authentication key. Used for IKEv2 payload integrity verification.
15	IKE Session Encryption Key – CSP	128 / 192 / 256 bits	AES (CBC) Cert. # <a href="#">A2689</a>	Derived via key derivation function defined in SP800-135 Rev1 KDF (IKEv2).	Import: N/A Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IKE session (IKE Phase I) encrypt key. Used for IKE payload protection.

#	Key / SSP Name / Type	Security Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
16	IPSec Session Encryption Key – CSP	128 / 192 / 256 bits 128 / 256 bits	AES (CBC) and AES (GCM) Cert. # <a href="#">A2689</a>	Derived via key derivation function defined in SP800-135 Rev1 KDF (IKEv2).	Import: N/A Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IPSec (IKE phase II) encryption key. Used for IPSec traffics protection. IPSec session encryption keys can also be used for the Double Encrypt feature.
17	IPSec Session Authentication Key – CSP	160 bits	HMAC-SHA-1 Cert. # <a href="#">A2689</a>	Derived via key derivation function defined in SP800-135 Rev1 KDF (IKEv2).	Import: N/A Export: To calling application	N/A	Stored in SDRAM memory (plaintext).	Zeroized by rebooting the module.	The IPSec (IKE Phase II) authentication key. Used for IPSec traffics integrity verification.

**Notes:**

- AES GCM IV generation is performed in compliance with the Implementation Guidance C.H scenario 1 for IKEv2.
  - For IKEv2, the module is compliant with RFC 4106 and 7296. Specifically, the module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.
  - When the “nonce” (the IV in RFC 5282) for IKEv2 exhausts the maximum number of possible values for a given security association for IKEv2, either party to the security association for IKEv2 that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key.
- AES GCM IV is generated internally in compliance with the Implementation Guidance C.H scenario 3 and SP800-38D section 8.2.2.
- In case the module's power is lost and then restored, a new key for use with the AES-GCM encryption/decryption shall be established.
- The bound OpenSSL module's employed Approved DRBG (Cert. #[A2690](#)) generates a minimum of 256 bits of entropy for use in key generation.
- Sensitive Security Parameters (SSPs) can be Critical Security Parameters (CSPs) or Public Security Parameters (PSPs).
- Keys established while operating in the non-Approved mode cannot be used in the Approved mode, and vice versa.



## 9.1 Non-Deterministic Random Number Generation Specification

The module does not implement a random number generator. Instead, it uses the Random Number Generation (RNG) service provided by the bound Hewlett Packard Enterprise *Aruba OpenSSL Module* cryptographic module, which implements a Deterministic Random Bit Generator (DRBG) compliant to [SP800-90A]. The details of the validated entropy source used by the RNG service provided by the bound OpenSSL module are specified in the table below.

**Table 16 – Non-Deterministic Random Number Generation Specification**

Entropy Sources	Minimum Number of Bits of Entropy	Details
Aruba CPU Jitter Entropy Source (see <a href="#">NIST Entropy Source Validation (ESV) program certificate E7</a> )	Oversampling of 512 bits is performed to ensure that 256 bits of entropy is available to the DRBG.	The module employs a SP800-90Arev1-compliant Deterministic Random Bit Generator (DRBG) using an AES-256 CTR_DRBG mechanism with Derivation Function (DF) for random number generation ( <a href="#">Cert. #A2690</a> ). The employed DRBG uses a SP800-90B-compliant non-physical entropy source that uses CPU jitter provided by the operational environment as a noise source (Jitterentropy (JENT) with SHA-3 as the vetted conditioning component) which is within the module host's physical boundary but outside of the module's cryptographic boundary. The entropy source performs the SP800-90B Section 4.4 Approved Continuous Health Tests (RCT and APT).

## 10 Self-Tests

The Hewlett Packard Enterprise *Aruba Crypto Module* performs when powered on the Cryptographic Algorithm Self-Tests (CASTs) and Pre-Operational Self-Tests (POSTs). While the module is executing the cryptographic algorithm and pre-operational self-tests, services are not available, and input and output are inhibited. In addition, the module also performs Conditional self-tests. All cryptographic algorithm self-tests are run when the module is powered on, prior to the first operational use of the cryptographic algorithm. After the cryptographic algorithm, pre-operational, and conditional self-tests are passed successfully, the module transitions to the operational state.

When a cryptographic algorithm self-test or pre-operational self-test fails, or when a conditional self-test fails, the module enters the Critical Error state (while in this state, the module provides no functionality and inhibits data output), logs the error, and reboots automatically.

The Hewlett Packard Enterprise *Aruba Crypto Module* performs the following **Pre-Operational Self-Tests (POSTs)**:

**Table 17 – Pre-Operational Self-Tests**

Algorithm	Test Properties	Type	Details
Firmware Integrity Test	HMAC-SHA-1 with 117-bit key	KAT	The Firmware Integrity Test verifies the integrity of the module by comparing a calculated HMAC-SHA-1 value against the stored HMAC value. The KAT for the HMAC-SHA-1 is executed before the Firmware Integrity Test.

The Hewlett Packard Enterprise Crypto Module performs the following **Conditional Tests**:

**Table 18 – Conditional Cryptographic Algorithm Tests**

Algorithm	Test Properties	Type	Details	Condition
AES CBC	AES-CBC-256	KAT	Encrypt, Decrypt	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
AES GCM	AES-GCM-256	KAT	Encrypt, Decrypt	
ECDSA	P-256	KAT	Sign, Verify	
HMAC	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	KAT		
KAS-SSC-ECC	Primitive 'Z' computation with P-256 curve	KAT	Ephemeral Unified SP 800-56A Rev3 based	

Algorithm	Test Properties	Type	Details	Condition
KAS-SSC-FFC	Shared secret computation, p=2048, q=256	KAT	dhEphem SP 800-56A Rev3 based	Each run when module powered on, which is prior to the first operational use of the cryptographic algorithms
KDF135	Key derivation	KAT	SP 800-135 Rev1 based: IKEv2	
RSA	2048, PKCS#1-v1.5	KAT	Sign, Verify	
SHS	SHA-1, SHA-256, SHA-384, SHA-512	KAT		

**Table 19 – Conditional Pairwise Consistency Tests**

Algorithm	Test Properties	Type	Details	Condition
ECC key pairs	P-256, P-384	PCT	Sign, Verify	Each run on key pair generation
FFC key pairs	DH key pair generation	PCT	SP800-56A Rev3 assurances as per SP 800-56A Rev3 Section 5.6.2.1.4 for PCT	
RSA key pairs	2048, PKCS#1-v1.5	PCT	Sign, Verify	

**Self-Test Types:**

**KAT** = Known Answer Test, **PCT** = Pairwise Consistency Test

To see the results of the self-tests run by the module, use the ArubaOS CLI command on the host device:

```
show log crypto all
```

Upon successful completion of the power-up self-tests, the module displays results on the host device console:

```
Completed FIPS Aruba Cryptographic KAT test successfully.
```

In the event any self-test fails, the module will enter a Critical Error state (while in this state, the module provides no functionality and inhibits data output), logs the error, and reboots automatically. After a self-test failure, the module displays results on the host device console :

KATs:

```
FIPS Aruba Cryptographic KAT failure
```

PCTs:

```
FIPS Aruba Cryptographic asymmetric key KAT failure.
```

```
FIPS POST: FAIL
```

```
Rebooting...
```

When the firmware integrity test fails at power-up, the module enters the Critical Error state, where the invalid host ArubaOS firmware file is deleted to clear the error. The host device will automatically reboot from the backup ArubaOS image on the secondary partition. The module displays on the host device console:

```
FIPS Aruba Mocana Integrity test failure
```

```
Aruba Crypto FIPS KAT test FAILED!! Restarting System.
```

## 11 Life-Cycle Assurance

The Hewlett Packard Enterprise *Aruba Crypto Module* is a firmware type module, and must run on an Hewlett Packard Enterprise hardware unit (e.g., Controller, Gateway, Conductor, or Access Point) or virtual appliance (e.g., VMWare ESXi or open source KVM hypervisor running on a hardware server unit (e.g., HPE ProLiant ML110 Gen10 or HPE EdgeLine 20)).

ArubaOS is the operating system for Hewlett Packard Enterprise Mobility Conductors, Mobility Controllers/Gateways, and controller-managed Hewlett Packard Enterprise Access Points (APs). The Hewlett Packard Enterprise *Aruba Crypto Module* is one of the Hewlett Packard Enterprise cryptographic modules that provide cryptographic services for the host ArubaOS operating system running on the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances.

### 11.1 Start-up Procedures

The Hewlett Packard Enterprise *Aruba Crypto Module* is one of the components within the ArubaOS firmware package in electronic form and is installed automatically when a trusted and verified ArubaOS is booted on an Hewlett Packard Enterprise host device. ArubaOS firmware in electronic form is installed by Hewlett Packard Enterprise technical support personnel or downloaded from the HPE Networking Support Portal (NSP) by authenticated licensed customer personnel.

#### 11.1.1 Setting Up the Hewlett Packard Enterprise Controller, Gateway, Conductor, or Controller-managed Access Point (AP) and Running Hewlett Packard Enterprise Aruba Crypto Module Automatically

The Crypto Officer shall perform the following steps to set-up your Hewlett Packard Enterprise Controller, Gateway, Conductor, or controller-managed Access Point (AP) either as a host hardware unit or a virtual appliance:

1. Since the Hewlett Packard Enterprise *Aruba Crypto Module* firmware is a component of ArubaOS and is installed automatically when a trusted and verified ArubaOS firmware image is booted successfully on the Hewlett Packard Enterprise host device, the Crypto Officer (CO) shall review the *ArubaOS 8.10 Getting Started Guide*, *ArubaOS 8.10.0.x AP Software Quick Start Guide*, and *ArubaOS 8.10 Virtual Appliance Installation Guide*. Select the Hewlett Packard Enterprise host device running ArubaOS deployment scenario that best fits your installation and follow the scenario's deployment procedures.
2. Connect your PC or workstation to a line port (or virtual port mapped to the module interface) on the Hewlett Packard Enterprise Controller, Gateway, Conductor, or controller-managed Access Point (AP).
3. Enable power to the Hewlett Packard Enterprise Controller, Gateway, Conductor, or controller-managed Access Point (AP).
4. Monitor the Hewlett Packard Enterprise host device boot progress messages on the console.
5. Once ArubaOS is loaded successfully and operating normally on the Hewlett Packard Enterprise host device, check the console messages to make sure that all the power-up self-tests passed.
  - a. Check that the following console message is displayed:
 

```
Completed FIPS Aruba Cryptographic KAT test successfully.
```
  - b. As specified in the [Self-Tests](#) section, if any of the checks fail, error messages will be displayed on the console. If the errors persist after the Hewlett Packard Enterprise device is rebooted, contact Hewlett Packard Enterprise.
6. Enable the Approved mode with the ArubaOS CLI on the host.
  - a. Login to the Hewlett Packard Enterprise Controller, Gateway, or Conductor following the guidance from step 1. above (a controller-managed Access Point (AP) is placed in the Approved mode using a Staging Controller in the Approved mode as per the *Aruba AP Software Quick Start Guide*).

- b. Enable the Approved mode using the following ArubaOS CLI commands on the host:

```
#configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(config) #fips enable
(config) #exit
#write memory
Saving Configuration...
Configuration Saved.
```

- c. To verify the Approved mode has been enabled, issue the ArubaOS CLI command on the host:

```
show fips    to see:    FIPS Settings:
                          Mode Enabled
```

## 11.2 Full Documentation

Documentation for any Hewlett Packard Enterprise product can be found on the HPE Networking Support Portal (NSP). Filters can be used to limit the displayed results by Product(s), Product Series, Version(s), and File Category.

For example,

- Full ArubaOS version 8.10 documentation for Hewlett Packard Enterprise Mobility Controllers, Virtual Mobility Controllers, Gateways, Mobility Conductors, and Access Points can be found at the link provided below after authentication.

<https://networkingsupport.hpe.com/downloads;pageSize=100;fileTypes=DOCUMENT;products=Aruba%20Access%20Points,Aruba%20Mobility%20Gateways;softwareGroups=ArubaOS;softwareMajorVersions=8.10>

### 11.2.1 Related Hewlett Packard Enterprise Documents

The following Hewlett Packard Enterprise documents can be referenced to ensure that ArubaOS and the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances that run ArubaOS are installed and operated correctly in the Approved mode:

- Aruba Access Points Installation Guides*
- ArubaOS 8.10.0.x AP Software Quick Start Guide*
- ArubaOS 8.10.0.0 Virtual Appliance Installation Guide*
- ArubaOS 8.10.0.0 User Guide*
- ArubaOS 8.10.0.x CLI Reference Guide*
- ArubaOS 8.10.0.0 API Guide*
- ArubaOS 8.10.0.0 Getting Started Guide*
- ArubaOS 8.10.0.0 Syslog Reference Guide*

### 11.2.2 Administrator Guidance

The Crypto Officer must ensure that the module is kept in the Approved mode of operation. To keep the module in the Approved mode, abide by [section 11.1, Start-up Procedures](#), [section 2.9, Non-Approved Algorithms Not Allowed in the Approved Mode of Operation](#), and [section 4.3.2, Non-Approved Services](#).

### 11.2.3 Non-Administrator Guidance

None

### 11.2.4 Maintenance Requirements

Not Applicable (N/A)

### 11.3 End of Life

To determine if an Hewlett Packard Enterprise product is considered end of life, refer to the Hewlett Packard Enterprise end-of life information at <https://networkingsupport.hpe.com/end-of-life>. If an Hewlett Packard Enterprise product is deemed end-of-life, the CO should work with their Hewlett Packard Enterprise representative to determine the appropriate Hewlett Packard Enterprise product upgrade path to use a newer Approved version.

For secure sanitization and zeroization of SSP values, follow the guidance in the Zeroization service entry above in [Table 13, in section Approved Services](#) to wipe out host flash and reboot the module. Since the module is a component of ArubaOS, if the module is deprecated, the module will be upgraded to a newer Approved validated version by loading and booting the newer validated version of ArubaOS with the help of an Hewlett Packard Enterprise-Certified Mobility Professional (ACMP).

## 12 Mitigation of Other Attacks

The module has not been purposely designed, built and publicly documented to mitigate one or more specific attacks. The Mitigation of Other Attacks requirements are not applicable, per FIPS 140-3 IG 12.A.