Hewlett Packard Enterprise

Bootloader Module

Firmware Version 1.0

Non-Proprietary Security Policy

FIPS 140-3 Level 1

Document Version 1.0

November 2024

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.

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

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

Contents

Figures

Tables

Preface

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 *Bootloader Module* firmware version 1.0 that boots verified ArubaOS firmware versions 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 *Bootloader 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 *Bootloader 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 FIPS 140-3 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 *Bootloader Module* is referred to as the module, the cryptographic module, or the bootloader.

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 products.

  Select the Certificate Number for the Module Name ‘Bootloader Module’.

1.3 Acronyms and Abbreviations

AES	**Advanced Encryption Standard**
AP	**Access Point**
BIOS	**Basic Input/Output System**
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**
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**
UEFI	**Unified Extensible Firmware Interface**
WLAN	**Wireless Local Area Network**

1.4 Security Levels

The Hewlett Packard Enterprise *Bootloader 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
Overall	**Overall Security Rating of the Module**	**1**

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Hewlett Packard Enterprise *Bootloader Module* (also referred to as 'the module') is a firmware type cryptographic module and was validated under FIPS 140-3 Level 1 requirements. The Hewlett Packard Enterprise *Bootloader Module* (firmware) is booted by the hardware BIOS process (out of the scope of this validation) and provides basic cryptographic services before booting the ArubaOS operating system on the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances. ArubaOS is the operating system for Hewlett Packard Enterprise Mobility Conductors, Mobility Controllers/Gateways, and controller-managed Hewlett Packard Enterprise Access Points (APs) – ArubaOS is out of the scope of this validation. Once ArubaOS is booted, control of the Hewlett Packard Enterprise device passes to ArubaOS and the module is not executed again until the next hardware boot of the Hewlett Packard Enterprise device.

Module Type: Firmware

Module Embodiment: Multiple-chip Standalone

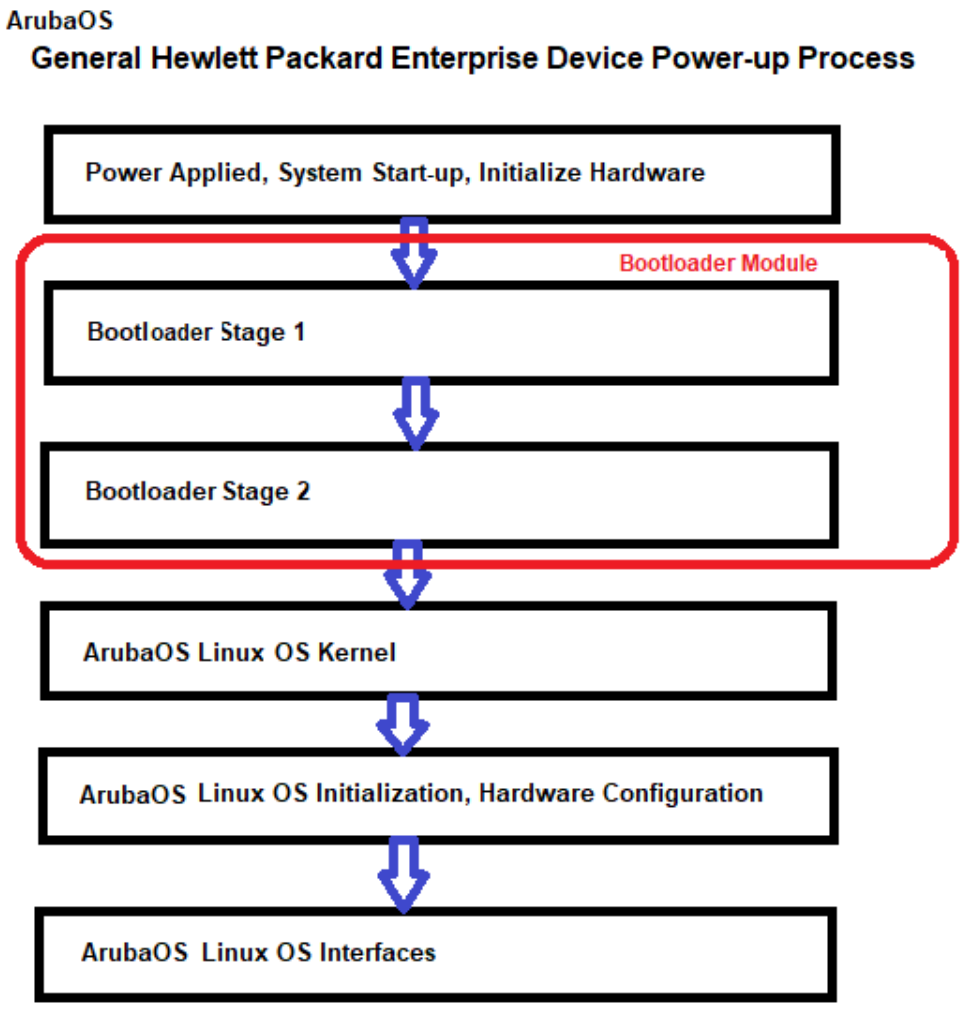

Figure 1 – General Hewlett Packard Enterprise Device Power-up Process with Bootloader Module and ArubaOS

2.1.1 Cryptographic Module Boundary

The Hewlett Packard Enterprise *Bootloader Module* (firmware) is preloaded during Hewlett Packard Enterprise device manufacturing with the appropriate Hewlett Packard Enterprise bootloader image for the Hewlett Packard Enterprise device, the Factory CA Public Key, and the ArubaOS image (both the Factory CA Public Key and ArubaOS are out of scope of this validation). Refer to Figure 2 block diagram below and the following section 2.2, Version Information.

Once booted by the hardware BIOS process (out of the scope of this validation) from the bootloader partition storage, the Hewlett Packard Enterprise *Bootloader Module* (firmware) boots the ArubaOS operating system from the ArubaOS image partition after confirming the OS has been properly signed and performing the firmware integrity test (see section 5, Software/Firmware Security).

The cryptographic boundary for the module firmware is defined as the preloaded Hewlett Packard Enterprise *Bootloader Module* (see Figure 2).

The **Tested Operational Environment's Physical Perimeter (TOEPP)** is the production-grade enclosure of the hardware chassis of the Hewlett Packard Enterprise hardware device or Hewlett Packard Enterprise virtual appliance host (see Figure 2).

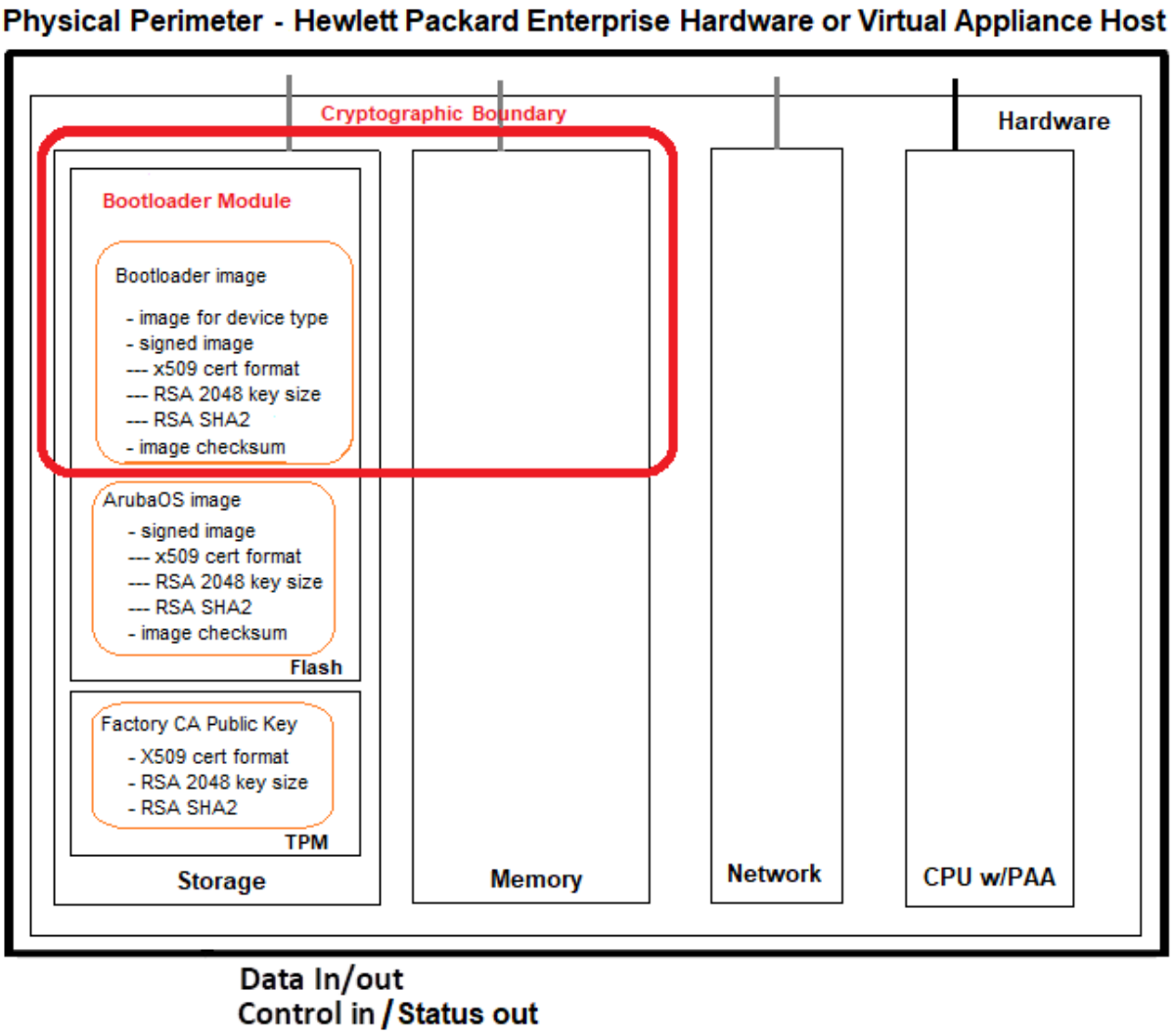

Figure 2 – Functional Block Diagram of Cryptographic Boundary for Bootloader Module

2.2 Version Information

The Hewlett Packard Enterprise *Bootloader Module* (firmware) 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 when operating a version that is not listed on the validation certificate.

Table 3 – Version Information

Type	Versions
Firmware	Bootloader Module version 1.0

To aid the module administrator to correlate the output of the module current name and versioning information with the corresponding Hewlett Packard Enterprise *Bootloader Module* version 1.0 FIPS 140-3 Level 1 validation record, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.

2.3 Operating Environments

Hewlett Packard Enterprise *Bootloader Module* version 1.0 is preloaded during Hewlett Packard Enterprise device manufacturing with the appropriate Hewlett Packard Enterprise bootloader image for the Hewlett Packard Enterprise device (see section 2.2, Version Information, in the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document).

The module operates in a limited operational environment. The module runs on the host hardware and boots the verified and integrity tested ArubaOS firmware. See the following tables of Tested Operational Environments and Vendor Affirmed Operational Environments for details.

Table 4 – Tested Operational Environments

#	Operating System (firmware version booted by bootloader)	Hardware / Virtual Platform	Processor	PAA / Acceleration
1	ArubaOS 8.10	7220 Mobility Controller	Broadcom XLP432 (MIPS64)	None
2	ArubaOS 8.10	9004 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 (firmware version booted by bootloader)	Hardware / Virtual Platform
1	ArubaOS 8.10	70xx Mobility Controllers
2	ArubaOS 8.10	72xx Mobility Controllers
3	ArubaOS 8.10	9012 Gateways
4	ArubaOS 8.10	9240 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

Table 6 – Modes List and Description

Name	Description	Approved FIPS Mode	Status Indicator
FIPS Mode	Single Approved Mode, the module always operates in the Approved mode and all services are available when the host has power	Yes	Status messages showing the bootloader FIPS POSTs and Conditional tests passed and the ArubaOS version being booted

When the module starts up successfully, after passing all the Cryptographic Algorithm Self-Tests (CASTs), Pre-Operational Self-Tests (POSTs), and Conditional self-tests, and following the guidance in section 11.1, Start-up Procedures, the module is operating in the Approved mode of operation. The module cannot be transitioned into any other mode. Section 4.3, Services, provides details on the service indicator implemented by the module.

2.6 Approved Algorithms

The firmware in the Hewlett Packard Enterprise *Bootloader 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 7 – Approved Algorithms

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2688	RSA [FIPS 186-4]	SigVer: SHA2-256 PKCS1 v1.5	SigVer: 2048	Digital Signature Verification (only)
A2688	SHS [FIPS 180-4]	SHA2-256 Byte Only	256	Message Digest

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

The cryptographic module does not implement any non-Approved algorithms that are 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 does not implement any non-Approved algorithms 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 does not implement any non-Approved algorithms that are not permitted for use in the Approved mode of operations.

2.10 Cryptographic Bypass

Cryptographic bypass is not supported by the Hewlett Packard Enterprise *Bootloader Module*.

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 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 8 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over the Interface
N/A	Data Input	Input parameters for data
N/A	Data Output	None
N/A	Control Input	Function calls
N/A	Status Output	Return codes, status information, error messages
N/A	Power	None

Note:

- 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) available from the module.

4.1 Authentication

The Hewlett Packard Enterprise *Bootloader Module* does not provide any identification or authentication methods.

4.2 Roles

The module supports the Crypto Officer role only. This sole role is 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 9 – Roles and Authentication

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

Table 10 – Roles, Service Commands, Input, Output

Role	Service	Input	Output
Crypto Officer	Load the OS (boot)	Commands and configuration data	Status of commands and configuration data
Crypto Officer	Configure the module	Commands and configuration data	Status of commands and configuration data
Crypto Officer	Status Function	Commands and configuration data	Status of commands and configurations
Crypto Officer	Self-Test triggered by CO reboot	Module reboot	Progress information
Crypto Officer	Validate Firmware[1] Integrity	Commands and configuration data	Status of commands and configuration data
Crypto Officer	Update Firmware[1]	Commands and configuration data	Status of commands and configuration data

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:

- **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.

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.

Table 11 – 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
Load the OS (boot)	Load the OS and boot the device.	RSA SigVer SHA2-256	[1] Factory CA Public Key	Crypto Officer	E	Status messages showing module booted ArubaOS OS.
Validate Firmware[1] Integrity	Validate firmware on the module.	RSA SigVer SHA2-256	[1] Factory CA Public Key	Crypto Officer	E	Status of command to show firmware version.
Update Firmware[1]	Update firmware on the module.	RSA SigVer SHA2-256	[1] Factory CA Public Key	Crypto Officer	E	Status of command to show firmware version.

[1] Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-3 validation.

Table 12 – 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
Configure the module	Select boot partition specifics used by the module if not using the default partition specifics.	None	None	Crypto Officer	None	Status of configuration commands.
Status Function	Cryptographic officer may use CLI "show" commands including show version.	None	None	Crypto Officer (N/A for system status via host LEDs)	None	Status of "show" commands.
Self-Test triggered by CO reboot	Perform FIPS start-up tests on demand through module reboot.	None	None	Crypto Officer (N/A if host power is cycled manually)	None	Status of self-tests in log.

Note:

The module does not implement a zeroization service. The only key used by the module is the Factory CA Public Key, used for Firmware verification. This key is stored and protected in the TPM during Hewlett Packard Enterprise device manufacturing, so it is not possible to modify and is exempt from zeroization requirements.

4.3.2 Non-Approved Services

Since the module always operates in the Approved mode, there are no non-approved services.

5 Software / Firmware Security

The Hewlett Packard Enterprise *Bootloader Module* (firmware version 1.0) is an Hewlett Packard Enterprise cryptographic module that provides basic cryptographic services for the Hewlett Packard Enterprise bootloader function. The module is preloaded and shipped with each Hewlett Packard Enterprise device and is booted by the hardware BIOS process (out of the scope of this validation) when power is applied to the device. After the cryptographic algorithm, pre-operational firmware integrity test, and conditional self-tests are successfully passed, the module will boot the ArubaOS operating system from the image partition. The module only allows the booting of trusted and verified firmware that is signed by Hewlett Packard Enterprise.

The module performs a firmware integrity test when powered on and conditionally whenever a firmware load request is received (refer to Self-Tests for details). All cryptographic algorithm self-tests are run when the module is powered on, prior to the first operational use of the cryptographic algorithm. Both the Firmware Integrity Test and Firmware Load Test use RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA2-256.

The operator can initiate the firmware integrity test on demand by rebooting the host. All data output via the data output interface is inhibited until the cryptographic algorithm self-tests and firmware integrity test have 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 firmware through reviewing the log and by using the show status ArubaOS CLI command (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 Hewlett Packard Enterprise *Bootloader Module* (firmware) is booted by the hardware BIOS process and provides basic cryptographic services before booting the ArubaOS operating system on the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances. ArubaOS, Hewlett Packard Enterprise devices, and the hardware BIOS process are out of scope of this validation. Once ArubaOS is booted, control of the Hewlett Packard Enterprise device passes to ArubaOS and the module is not executed again until the next hardware boot of the Hewlett Packard Enterprise device.

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 *Bootloader 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 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) and Keys used in the module.

Table 13 – 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
Factory Key									
1	Factory CA Public Key -PSP	2048 bits	RSA Public Key Cert. #A2688	N/A Loaded into the TPM during manufacturing (i.e. out of scope of module).	Import: from TPM Export: N/A	N/A	Stored in TPM	Since this public key is stored and protected in the TPM, the zeroization requirements do not apply.	This is a RSA public key. Used for Hewlett Packard Enterprise firmware verification.

Note:

- The module does not generate keys and does not include nor need an entropy source.

10 Self-Tests

The module performs at power-on the Cryptographic Algorithm Self-Tests (CASTs) and Pre-Operational Self-Tests (POSTs). After the cryptographic algorithm, pre-operational, and conditional self-tests are successfully passed, the module automatically transitions to the operational state and is operating in the Approved mode of operation by default. 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.

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

Table 14 – Pre-Operational Self-Tests

Algorithm	Test Properties	Type	Details
RSA Firmware Integrity Test	2048-bit public key, PKCS#1-v1.5, signature verification with SHA2-256 message digest	SigVer	The Hewlett Packard Enterprise *Bootloader Module* performs the firmware integrity test when module powered on, before booting the ArubaOS operating system

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

Table 15 – Conditional Cryptographic Algorithm Tests

Algorithm	Test Properties	Type	Details	Condition
RSA	2048, PKCS#1-v1.5	KAT	Verify	Each run when module powered on, prior to the first operational use of the cryptographic algorithms
SHS	SHA-256	KAT		

Table 16 – Conditional Software/Firmware Load Tests

Algorithm	Test Properties	Type	Details	Condition
RSA Firmware Load Test	2048, PKCS#1-v1.5, signature verification with SHA2-256	SigVer		Test is applied by the Hewlett Packard Enterprise *Bootloader Module* on request to load firmware

Self-Test Types:

KAT = Known Answer Test, **SigVer** = Signature Verification

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

- Conditional Cryptographic Algorithm Test:

```
Secure Boot Enabled on the Processor
CPBoot 1.2.9.0-FIPS (build 85048)
Built: 2022-09-06 at 11:11:56
FIPS POST: PASS
```

- Pre-Operational self-tests – Firmware Integrity Test:

```
Loading image 0:0################################
Image is signed; verifying checksum...passed
SHA2 Signature available
Signer Cert OK
Policy Cert OK
RSA signature verified using SHA2.
Aruba Networks
ArubaOS Version 8.10.0.2-FIPS
```

For more details, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.

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.

If cryptographic algorithm test fails, the module will display on the host device console:

```
FIPS POST: FAIL
Rebooting…
```

If image checksum verification fails, the module will display on host device the console:

```
Image is signed; verifying checksum...failed!
Rebooting…
```

If RSA Firmware Integrity Test or RSA Firmware Load Test fails, the module will not load the image and the invalid firmware file is deleted to clear the error. The module displays on the host device console:

```
Integrity test fail.
Contact Aruba support.
```

11 Life-Cycle Assurance

The Hewlett Packard Enterprise *Bootloader 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 *Bootloader Module* (firmware) is an Hewlett Packard Enterprise cryptographic module that provides basic cryptographic services for the Hewlett Packard Enterprise bootloader function that boots the ArubaOS operating system running on the Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances.

The Hewlett Packard Enterprise *Bootloader Module* is preloaded on shipped Hewlett Packard Enterprise equipment. The module boots the ArubaOS operating system (for either Hewlett Packard Enterprise hardware-based equipment or Hewlett Packard Enterprise virtual appliances) from the image partition after performing the firmware integrity test. The module performs a firmware integrity test when powered on and conditionally whenever a firmware load request is received (refer to Software / Firmware Security and Self-Tests for details). Once ArubaOS is booted, control of the Hewlett Packard Enterprise device passes to ArubaOS and the module is not executed again until the next hardware boot of the Hewlett Packard Enterprise device. ArubaOS and Hewlett Packard Enterprise devices are out of scope of this validation.

11.1 Start-up Procedures

The Hewlett Packard Enterprise *Bootloader Module* firmware is preloaded into the Hewlett Packard Enterprise equipment that is ordered by the Crypto Officer. The Hewlett Packard Enterprise equipment is shipped to the Crypto Officer in factory-sealed boxes using trusted commercial carrier shipping companies.

The Crypto Officer should examine the carton for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging. Inform your supplier if there are any incorrect, missing, or damaged parts. If possible, retain the carton, including the original packing materials. Use these materials to repack and return the Hewlett Packard Enterprise unit to the supplier if needed.

All Hewlett Packard Enterprise hardware units and virtual appliances should be professionally installed by an Hewlett Packard Enterprise-Certified Mobility Professional (ACMP). Do not disassemble Hewlett Packard Enterprise hardware unit chassis or components. They have no internal user-serviceable parts. When service or repair is needed, contact Hewlett Packard Enterprise.

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

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

1. Since the Hewlett Packard Enterprise *Bootloader Module* firmware's purpose is to boot a trusted and verified ArubaOS firmware image on the Hewlett Packard Enterprise 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 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 device boot progress messages on the console.

a. Refer to the appropriate boot console messages listed above in the Self-Tests section. For more details, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.

b. Successful boot sequences automatically include:

i. Cryptographic Algorithm Self-Tests (CASTs) and Pre-Operational Self-Tests (POSTs) are performed at power-up (refer to the Self-Tests section above).
ii. The verification of the Hewlett Packard Enterprise bootloader image with a checksum operation is performed.
iii. A bootloader firmware integrity check with RSA verify is completed to ensure the bootloader firmware is signed by Hewlett Packard Enterprise.
iv. The Hewlett Packard Enterprise bootloader function appropriate for the Hewlett Packard Enterprise device is executed. For more details, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.
v. The Hewlett Packard Enterprise bootloader name, firmware version, and build information is displayed on the host device console.
vi. When the Hewlett Packard Enterprise *Bootloader Module* starts up successfully, after passing all the cryptographic algorithm self-tests, pre-operational self-tests and power-on conditional tests, the module is operating in the Approved mode of operation by default.
vii. A verification of the ArubaOS image with a checksum operation is performed.
viii. An ArubaOS firmware load integrity check with RSA verify is completed to ensure the ArubaOS firmware is signed by Hewlett Packard Enterprise.
ix. ArubaOS is booted on the Hewlett Packard Enterprise device from the default image partition.
x. Cryptographic Algorithm Self-Tests (CASTs) and Pre-Operational Self-Tests (POSTs) are performed for the ArubaOS components at start-up.
xi. ArubaOS is loaded successfully and operating normally on the Hewlett Packard Enterprise device.
xii. Once ArubaOS is booted successfully, control of the Hewlett Packard Enterprise device passes to ArubaOS and the module is not executed again until the next hardware boot of the Hewlett Packard Enterprise device or host.
xiii. Follow the procedures as described in 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*, as appropriate to the Hewlett Packard Enterprise device's deployment.
xiv. As specified in the Self-Tests section, if any of the checks fail, error messages will be displayed on the host device console. If the errors persist after the Hewlett Packard Enterprise device is rebooted, contact Hewlett Packard Enterprise. For more details, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.

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 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

To keep the module in Approved mode, abide by section 11.1, Start-up Procedures.
Also, refer to the Hewlett Packard Enterprise *Bootloader Module* version 1.0 Administrator Guidance document.

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.

The Hewlett Packard Enterprise *Bootloader Module* does not implement a zeroization service. The only key used by the module is the Factory CA Public Key which is stored and protected in the TPM during Hewlett Packard Enterprise device manufacturing, so it is not possible to modify and is exempt from zeroization requirements. For secure sanitization, reboot the module.

If the module is deprecated, the CO should work with an Hewlett Packard Enterprise representative to determine the appropriate Hewlett Packard Enterprise product upgrade path to a newer Approved version. With the help of an Hewlett Packard Enterprise-Certified Mobility Professional (ACMP), they can assist in the loading and booting of a newer approved version of the module on the Hewlett Packard Enterprise device.

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.